Problems in logic for computer science students

Lorenzo Clemente   Jerzy Tyszkiewicz

May 2020

(289 problems, 283 solutions)

Contents

List of Problems

Part I

Problems

Chapter 1

Propositional logic

Preliminaries

The formulas φ of propositional logic are described by the following abstract syntax:

$$\varphi, \psi \ ::\equiv \ p \mid \bot \mid \top \mid \neg\varphi \mid \varphi \to \psi \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \leftrightarrow \psi,$$

where p belongs to a countably infinite set of *propositional variables* Z. We consider $\varphi \to \psi$ as an abbreviation for $\neg\varphi \vee \psi$ and $\varphi \leftrightarrow \psi$ as an abbreviation for $(\varphi \to \psi) \wedge (\psi \to \varphi)$. When writing formulas, we reduce the use of parentheses by assuming the following order of binding strength (priority) of the connectives, from highest to lowest: $\neg, \wedge, \vee, \to, \leftrightarrow$. For example, $\neg p \wedge q \vee r \leftrightarrow p \vee q$ is parsed as $(((\neg p) \wedge q) \vee r) \leftrightarrow (p \vee q)$.

The notation $\bigvee_{i \in I} \varphi_i$ denotes the disjunction of all formulas in $\{\varphi_i \mid i \in I\}$, and similarly for $\bigwedge_{i \in I} \varphi_i$.

$F_\wedge(x,y)$		
$x \setminus y$	0	1
0	0	0
1	0	1

$F_\vee(x,y)$		
$x \setminus y$	0	1
0	0	1
1	1	1

$F_\neg$	
x	
0	1
1	0

Figure 1.1: Semantic functions for classical logic

Definition (Semantics of propositional formulas)**.** A *propositional valuation* (or *truth assignment*) is a function

$$\varrho : Z \to \{0,1\}.$$

A valuation ϱ extends to a semantic function of propositional formulas $[\![\varphi]\!]_\varrho \in \{0,1\}$ (also written $\varrho(\varphi)$) by structural induction as

- $[\![p]\!]_\varrho = \varrho(p)$, if p is a propositional variable;
- $[\![\varphi \vee \psi]\!]_\varrho = F_\vee([\![\varphi]\!]_\varrho, [\![\psi]\!]_\varrho)$;
- $[\![\varphi \wedge \psi]\!]_\varrho = F_\wedge([\![\varphi]\!]_\varrho, [\![\psi]\!]_\varrho)$;
- $[\![\neg\varphi]\!]_\varrho = F_\neg([\![\varphi]\!]_\varrho)$.

The semantic functions $F_\vee, F_\wedge : \{0,1\} \times \{0,1\} \to \{0,1\}$ and $F_\neg : \{0,1\} \to \{0,1\}$ are defined by the truth table in Figure 1.1.

A formula φ is *satisfied* by ϱ, written $\varrho \vDash \varphi$, if $[\![\varphi]\!]_\varrho = 1$, and it is *satisfiable* if $\varrho \vDash \varphi$ holds for at least one valuation ϱ. We write $[\![\varphi]\!]$ for the set of valuations $\{\varrho \mid \varrho \vDash \varphi\}$ satisfying φ. If Γ is a (possibly infinite) set of propositional formulas, and $\varrho \vDash \varphi$ for all $\varphi \in \Gamma$, then we write $\varrho \vDash \Gamma$. We say that φ is a *logical consequence* of Γ, written $\Gamma \vDash \varphi$, if every valuation which satisfies all formulas from Γ satisfies φ as well. If $\Gamma = \{\psi\}$ consists of a single formula, then we just write $\psi \vDash \varphi$. If $\Gamma = \varnothing$ is empty, then we just write $\varnothing \vDash \varphi$ and we say that φ is a *tautology*.

1.1 Logical consequence

Problem 1.1.1. Consider the following statements about formulas of classical propositional logic. For each of them, establish whether it holds or not, giving a proof in the positive cases and a counterexample in the negative ones.

1. If φ and $\varphi \leftrightarrow \psi$ are tautologies, then so is ψ.
2. If φ and $\varphi \leftrightarrow \psi$ are satisfiable, then so is ψ.
3. If φ is satisfiable and $\varphi \leftrightarrow \psi$ is a tautology, then ψ is satisfiable.
4. If φ is a tautology and $\varphi \leftrightarrow \psi$ is satisfiable, then ψ is a tautology.
5. If φ is a tautology and $\varphi \leftrightarrow \psi$ is satisfiable, then ψ is satisfiable. [solution]

Problem 1.1.2 (Transitivity of "$\vDash$")**.** Show that the logical consequence relation is *transitive*, in the sense that:

$$\Gamma \vDash \Delta \quad \text{and} \quad \Delta \vDash \Xi \qquad \text{implies} \qquad \Gamma \vDash \Xi.$$ [solution]

Problem 1.1.3 (Semantic deduction theorem)**.** Prove that for classical propositional logic,

$$\Gamma \cup \{\varphi\} \vDash \psi \quad \text{if, and only if,} \quad \Gamma \vDash \varphi \to \psi.$$ [solution]

Problem 1.1.4 (Weak soundness of modus ponens)**.** Prove that $\vDash \varphi$ and $\vDash \varphi \to \psi$ imply $\vDash \psi$. [solution]

Problem 1.1.5 (Strong soundness of modus ponens)**.** Show that modus ponens is *strongly sound*, in the sense that

$$\varphi, \varphi \to \psi \vDash \psi.$$ [solution]

Problem 1.1.6. Let S be a function mapping propositional variables to propositional formulas. Show that if $\Gamma \vDash \varphi$ holds, then $S(\Gamma) \vDash S(\varphi)$ holds, too. In particular, if φ is a tautology, then so is $S(\varphi)$. [solution]

Problem 1.1.7. A logic is called *monotone*, if $\Delta \vDash \varphi$ and $\Gamma \supseteq \Delta$ imply $\Gamma \vDash \varphi$. Prove that classical propositional logic is monotone. [solution]

Problem 1.1.8. Consider formulas built only from conjunction $\wedge$ and disjunction $\vee$. For such a formula φ, its *dualisation* $\hat{\varphi}$ is the formula obtained by replacing every occurrence of $\vee$ by $\wedge$, and vice-versa.

1. Prove that φ is a classical tautology if, and only if, $\neg\hat{\varphi}$ is a classical tautology.

2. Prove that $\varphi \leftrightarrow \psi$ is a tautology if, and only if, $\hat{\varphi} \leftrightarrow \hat{\psi}$ is a tautology.

3. Propose a method to dualise formulas additionally containing the logical constants $\bot$ and $\top$, such that the above equivalences remain valid. [solution]

Problem 1.1.9. Let φ, ψ be two formulas without common propositional variables. Assume that $\not\models \neg\varphi$ and $\not\models \psi$. Is it possible that $\models \varphi \to \psi$? [solution]

Problem 1.1.10. Let $G = (V, E)$ be a finite directed graph with vertices $V = \{v_1, \ldots, v_n\}$ and consider the set of propositional formulas over variables $\{p_1, \ldots, p_n\}$

$$\Delta = \{p_i \to p_j \mid (v_i, v_j) \in E\}.$$

1. Let $\Gamma_{ij} = \Delta \cup \{\neg(p_i \to p_j)\}$. Which property of G does satisfiability of Γ_{ij} expresses?

2. Provide a propositional formula φ_n, depending only on n, s.t. $\Delta \models \varphi_n$ if, and only if, G is strongly connected. [solution]

1.2 Normal forms

Definition 1.2.1 (Normal forms)**.** A *positive literal* is a propositional variable $p \in Z$, a *negative literal* is the negation of a propositional variable $\neg p$, and a *literal* ℓ is either a positive p or a negative literal $\neg p$. A formula φ is in *conjunctive normal form* (CNF) if it is a finite conjunction of disjunctions of literals, i.e., of the form

$$\varphi \equiv (\ell_1^1 \vee \cdots \vee \ell_1^{k_1}) \wedge \cdots \wedge (\ell_r^1 \vee \cdots \vee \ell_r^{k_r}),$$

and in *disjunctive normal form* (DNF) if it is a finite disjunction of conjunctions of literals, i.e., of the form

$$\varphi \equiv (\ell_1^1 \wedge \cdots \wedge \ell_1^{k_1}) \vee \cdots \vee (\ell_r^1 \wedge \cdots \wedge \ell_r^{k_r})$$

A formula φ is in *negation normal form* (NNF) if negation is applied only in front of propositional variables.

Problem 1.2.2 (Normal forms)**.** Prove that for each propositional formula φ, there exists a propositional formula ψ in each of the following normal forms, s.t. ψ is logically equivalent to φ, i.e., $\varphi \leftrightarrow \psi$ is a tautology:

1. Negation normal form (NNF).
2. Disjunctive normal form (DNF).
3. Conjunctive normal form (CNF). *Hint: Apply point 2.*

In each case, how large is ψ in terms of the size of φ? [solution]

Problem 1.2.3. A formula φ using propositional variables from the set $\{p_1, \ldots, p_k\}$ *defines* the function $f : \{0,1\}^k \to \{0,1\}$ if, for any valuation ϱ,

$$[\![\varphi]\!]_\varrho = f(\varrho(p_1), \ldots, \varrho(p_k)).$$

We say that a set of logical connectives is *functionally complete* if *any* function $f : \{0,1\}^k \to \{0,1\}$ can be defined by a formula using only the connectives from the set. Show that:

1. $\{\wedge, \vee, \neg\}$ is functionally complete;
2. $\{\wedge, \neg\}$ and $\{\vee, \neg\}$ are functionally complete;

3. $\{\to, \bot\}$ is functionally complete;

4. $\{\wedge, \vee\}$ is functionally complete for all monotonic functions (w.r.t. the natural order $0 \le 1$);

5. $\{\wedge, \vee, \to, \top\}$ is not functionally complete;

6. $\{\uparrow\}$ is functionally complete, where "$\uparrow$" is the so-called *Sheffer stroke* (a.k.a. *nand* function), which is defined as

$$\varphi \uparrow \psi \equiv \neg(\varphi \wedge \psi).$$

[solution]

We have seen that a propositional formula can always be transformed into a logically equivalent formula in CNF and DNF, however the complexity of such translations is exponential. If we content ourselves with preserving only equisatisfiability, then a method by Tseitin [33] allows us to do it with linear complexity.

Problem 1.2.4 (Equisatisfiable 3CNF)**.** Show that for each propositional formula φ there exists a propositional formula ψ in 3CNF such that 1) ψ is satisfiable if, and only if, φ is satisfiable, and 2) ψ has size linear in the size of φ. *Hint: Introduce new propositional variables.* [solution]

Note. Problem 1.4.3 demonstrates that it is impossible to construct equivalent 3-CNF formulas (or even CNF formulas of polynomial length) for every propositional formula.

The following problem has been proposed by Bartek Klin and Szymon Toruńczyk.

(*) Problem 1.2.5. Fix a $k \in \mathbb{N}$. Does there exist an infinite sequence of formulas $\varphi_0, \varphi_1, \ldots$ in k-CNF giving rise to an infinite strictly increasing chain of valuations

$$[\![\varphi_0]\!] \subsetneq [\![\varphi_1]\!] \subsetneq \cdots ?$$

What about k-DNF formulas? And CNF formulas? [solution]

1.3 Satisfiability

In this section we assume familiarity with standard computational complexity classes such as

$$\mathsf{LOGSPACE} \subseteq \mathsf{NLOGSPACE} \subseteq \mathsf{PTIME} \subseteq \mathsf{NPTIME},$$

and their complements (c.f. [24, 2, 28] for background).

Problem 1.3.1. Show that the satisfiability problem for DNF formulas is in NLOGSPACE. [solution]

Problem 1.3.2. Show that the satisfiability problem for 2-CNF formulas is in NLOGSPACE. [solution]

Problem 1.3.3. A formula is in XOR-CNF if it is a conjunction of *xor clauses* of the form

$$\ell_1 \oplus \cdots \oplus \ell_n,$$

where $p \oplus q$ is defined as $p \wedge \neg q \vee \neg p \wedge q$. Show that the satisfiability problem xor-formulas in CNF is in PTIME. [solution]

Problem 1.3.4. A *Horn clause* is an implication of the form either

$$p_1 \wedge \cdots \wedge p_n \to q, \quad (n \geq 0)$$

or

$$p_1 \wedge \cdots \wedge p_n \to \bot, \quad (n \geq 0)$$

and a *Horn formula* is a conjunction of Horn clauses. Show that the satisfiability problem for Horn formulas is in PTIME. [solution]

Problem 1.3.5 (Self-reducibility of SAT)**.** Assume an oracle that solves the SAT problem and let φ be a satisfiable formula. Show how to construct a satisfying assignment for φ using polynomially many invocations of the oracle. [solution]

1.4 Complexity

Problem 1.4.1. Construct a sequence of formulas $(\varphi_n)_{n\in\mathbb{N}}$ s.t. φ is of size $O(n)$ and admits n^2 different satisfying valuations. [solution]

Problem 1.4.2. Prove that there are Boolean functions of n variables $p_1, \ldots, p_n$ s.t. any propositional formula defining them has size $\Omega(2^n/\log n)$. [solution]

Problem 1.4.3. In this problem we show an exponential blowup when converting a formula to an equivalent one in CNF. We proceed in two steps.

1. Prove that there is no $k \in \mathbb{N}$ s.t. every formula of classical propositional logic is equivalent to a k-CNF formula.

2. Prove that there is no polynomial $p(n)$ s.t. every formula of classical propositional logic with n variables is equivalent to a CNF formula with $O(p(n))$ clauses. [solution]

Problem 1.4.4. Consider formulas of n variables, where we allow all possible $(n-1)$-ary Boolean functions $\{0,1\}^{n-1} \to \{0,1\}$ as connectives.

1. Prove that there is a formula which is not logically equivalent to one in which every propositional variable is used only once.

2. Assume now that we allow only all possible unary $\{0,1\} \to \{0,1\}$ and binary $\{0,1\}^2 \to \{0,1\}$ Boolean functions as connectives. Prove that there is no polynomial $p(n)$ s.t. every classical propositional formula of n variables is equivalent to one in which every variable is used at most $p(n)$ times. [solution]

Problem 1.4.5. Consider a *simple graph* $G = (V, E)$ with vertices in $V = \{v_1, \ldots, v_n\}$, i.e., an undirected graph without loops $(v, v) \in E$. Let us introduce a propositional variable p_i for every vertex v_i. Given two propositional formulas $\varphi(x, y)$ and $\psi(x, y)$ over two variables x, y, consider the set of formulas

$$\Delta_{\varphi,\psi}(G) = \{\varphi(p_i, p_j) \mid (v_i, v_j) \in E\} \cup \{\psi(p_i, p_j) \mid (v_i, v_j) \notin E\}. \tag{1.1}$$

For which values of $k \in \mathbb{N}$ there are formulas φ, ψ such that for every simple graph G, the set $\Delta_{\varphi,\psi}(G)$ is satisfiable if, and only if, G is k-colourable? [solution]

1.5 Compactness

Problem 1.5.1 (Compactness theorem for propositional logic)**.** Let Γ be an infinite set of formulas of propositional logic. Show that if every finite subset of Γ is satisfiable, then Γ is satisfiable. *Hint: Use König's lemma.*
[solution]

Problem 1.5.2. Prove that Problem 1.5.1 "Compactness theorem for propositional logic" implies the following alternative reformulation: If $\Gamma \vDash \varphi$, then there exists a finite subset $\Delta \subseteq_{\text{fin}} \Gamma$ s.t. $\Delta \vDash \varphi$.

Proof. Assume $\Gamma \vDash \varphi$. By way of contradiction, assume $\Delta \nvDash \varphi$, for every $\Delta \subseteq_{\text{fin}} \Gamma$. Consequently, $\Gamma \cup \{\neg\varphi\}$ is finitely satisfiable, and thus by Problem 1.5.1 "Compactness theorem for propositional logic" $\Gamma \cup \{\neg\varphi\}$ is satisfiable, which is a contradiction. [solution]

[solution]

Problem 1.5.3 (Compactness implies König's lemma)**.** Use the compactness theorem for propositional logic to prove König's lemma.
[solution]

Problem 1.5.4 (De Bruijn–Erdős theorem)**.** Let k be a fixed natural number. Prove, using the compactness theorem, that if every finite subgraph of an infinite graph $G = (V, E)$ is k-colourable, then G is k-colourable as well. [solution]

Problem 1.5.5. Consider an infinite set of people with the property that 1) each man has a *finite* number of girlfriends, and 2) any $k \in \mathbb{N}$ men collectively have at least k girlfriends. Demonstrate that each man can marry one of his girlfriends without committing polygamy, i.e., no man marries two or more women (polygyny) and no woman marries two or more men (polyandry). Are the two assumptions necessary? [solution]

Problem 1.5.6. The following equivalence holds, for any truth assignment ϱ:

$$\varrho \vDash r \leftrightarrow (p_0 \vee p_1) \quad \text{if, and only if,} \quad \varrho(r) = \max(\varrho(p_0), \varrho(p_1)).$$

Does there exist a (possibly infinite) set of formulas Γ over propositional variables $\{r, p_0, p_1, \dots\}$ s.t., for every ϱ,

$$\varrho \vDash \Gamma \quad \text{if, and only if,} \quad \varrho(r) = \max_{n \in \mathbb{N}}(\varrho(p_n))?$$ [solution]

Problem 1.5.7. Does there exist a set Γ of sentences over propositional variables $\{p_0, p_1, \dots\}$ s.t. the valuations ϱ satisfying Γ are exactly those s.t. $\{i \in \mathbb{N} \mid \varrho(p_i) = 1\}$ is finite? [solution]

Definition 1.5.8. A *topological space* is a pair (X, τ), where X is a non-empty set and $\tau \subseteq 2^X$ is a family of subsets of X containing the empty set $\varnothing \in \tau$ and closed under arbitrary unions and finite intersections. A set $Y \in \tau$ is called *open* and a set $Z \subseteq X$ is *closed* if it is the complement $X \setminus Y$ of some open set $Y \in \tau$. A topological space is *countably compact* if every countable collection of closed sets $\mathcal{C} \subseteq 2^X$ has non-empty intersection $\bigcap \mathcal{C} \neq \varnothing$ if, and only if, every finite subcollection thereof $\mathcal{D} \subseteq_{\text{fin}} \mathcal{C}$ has non-empty intersection $\bigcap \mathcal{D} \neq \varnothing$.

Problem 1.5.9 (The name of the game)**.** Let Z be a countable set of propositional variables and for a set of sentences Γ let

$$[\![\Gamma]\!] = \{\varrho : Z \to \{0,1\} \mid \varrho \vDash \Gamma\}.$$

Consider the topological space (X, τ), where X is the set of all valuations $[\![\top]\!]$ and τ is the topology generated by basic open sets of the form $[\![\varphi]\!]$. Show, using the compactness theorem for propositional logic, that (X, τ) is a countably compact topological space. [solution]

Problem 1.5.10 (Compactness with infinitary conjunction)**.** Show that the compactness theorem still holds for infinite CNF formulas with infinitary conjunction

$$\bigwedge_{i=1}^{\infty} \bigvee_{j=1}^{n_i} l_{ij},$$

where l_{ij} is a literal (a propositional variable or a negation thereof). [solution]

Problem 1.5.11 (No compactness with infinitary disjunction)**.** Show that the compactness fails infinite DNF formulas with infinitary disjunction

$$\bigvee_{i=1}^{\infty} \bigwedge_{j=1}^{n_i} l_{ij}.$$ [solution]

1.6 Resolution

Let Γ be a set of formulas. The following inference rule is called *Robinson's resolution* principle:

$$\frac{\Gamma \vdash p \vee \varphi \quad \Gamma \vdash \neg p \vee \psi}{\Gamma \vdash \varphi \vee \psi} \tag{R}$$

A set of inference rules is *sound* if it preserves logical entailment:

$$\Gamma \vdash \varphi \quad \text{implies} \quad \Gamma \vDash \varphi.$$

Problem 1.6.1 (Resolution is sound)**.** Show that the resolution rule (1.3) is sound. *Hint: Proceed by induction on the length of derivations.* [solution]

A set of inference rules is *complete* if it can prove all logical entailments,

$$\Gamma \vDash \varphi \quad \text{implies} \quad \Gamma \vdash \varphi,$$

and *refutation complete* if it can derive a contradiction from any unsatisfiable set of formulas:

$$\Gamma \vDash \bot \quad \text{implies} \quad \Gamma \vdash \bot.$$

Problem 1.6.2 (Resolution is refutation complete)**.** Show that resolution (1.3) is refutation complete when Γ is a set of clauses. Is it complete? *Hint: Proceed by induction on the number of propositional variables.* [solution]

(*) Problem 1.6.3 (Pigeonhole formulas [15])**.** Let there be m pigeons and n holes, and for every $1 \le i \le m$ and $1 \le j \le n$, let $p_{i,j}$ be a propositional variable encoding that pigeon i is in hole j. Consider the following CNF family of *pigeonhole formulas*

$$\varphi_{m,n} \equiv \bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} p_{ij} \wedge \bigwedge_{j=1}^{n} \bigwedge_{i=1}^{m} \bigwedge_{k=i+1}^{m} \neg p_{ij} \vee \neg p_{kj},$$

stating that 1) each pigeon is inside some hole, and 2) no hole contains two pigeons. Show that $\varphi_{n+1,n}$ has only resolution refutation trees of size exponential in n. [solution]

1.7 Interpolation

Definition 1.7.1. An *interpolant* of two propositional formulas φ, ψ satisfying $\vDash \varphi \to \psi$ is a formula ξ containing only propositional variables occurring both in φ and in ψ s.t. $\vDash \varphi \to \xi$ and $\vDash \xi \to \psi$.

Problem 1.7.2 (Propositional interpolation)**.** Let φ and ψ be two formulas of classical propositional logic s.t. $\vDash \varphi \to \psi$. Show that there exists a formula ξ interpolating φ, ψ. [solution]

The following problem presents a simplified version of Beth's definability theorem [4] in the context of propositional logic.

Problem 1.7.3 (Beth's definability theorem)**.** Let φ be a formula of propositional logic and let p, q be two propositional variables s.t. p occurs in φ, q does not occur in φ, and

$$\varphi, \varphi[p \mapsto q] \vDash p \leftrightarrow q. \qquad \text{(implicit definability of } p\text{)}$$

Prove that there exists a formula ψ not containing p, q s.t.

$$\varphi \vDash p \leftrightarrow \psi. \qquad \text{(explicit definability } p\text{)}$$

Hint: Use interpolation. [solution]

Problem 1.7.4. Prove the following infinite extension of the interpolation theorem for propositional logic: If Δ, Γ are two sets of formulas satisfying $\Gamma \vDash \Delta$, then there is a set of formulas Θ containing only propositional variables occurring both in (some formula of) Γ and in (some formula of) Δ s.t. $\Gamma \vDash \Theta$ and $\Theta \vDash \Delta$. [solution]

(*) Problem 1.7.5 (Interpolants and circuit complexity [23])**.** Show that if one could bound the circuit size of an interpolant by a polynomial in the size of the input formulas, then any disjoint pair of NPTIME languages would be separable by a circuit of polynomial size. Deduce that $\mathsf{NPTIME} \cap \mathsf{coNPTIME}$ would have polynomial size circuits in this case. [solution]

The following result appeared in [18, Theorem 6.1], [26, Theorem 1], and [21, Theorem 2].

(*) Problem 1.7.6 (Resolution has polynomial interpolation)**.** A proof system has the *polynomial interpolation property* if, whenever $\neg(\varphi \to \psi)$ has a proof of size n, there exists an interpolant ξ of size polynomial in n. Show that resolution has the polynomial interpolation property. [solution]

1.8 Hilbert's proof system

We consider a Hilbert-style deduction system for the minimal set of connectives "$\to$" and "$\bot$" (which is functionally complete; c.f. Problem 1.2.3). We define $\neg\varphi \equiv \varphi \to \bot$, and we consider the following three axioms and one deduction rule.

$$\varphi \to \psi \to \varphi, \tag{A1}$$

$$(\varphi \to \psi \to \theta) \to (\varphi \to \psi) \to \varphi \to \theta, \tag{A2}$$

$$\neg\neg\varphi \to \varphi, \tag{A3}$$

$$\frac{\varphi \to \psi \quad \varphi}{\psi}. \tag{MP}$$

(The connective "$\to$" associates to the right, e.g., $\varphi \to \psi \to \varphi$ is to be read as $\varphi \to (\psi \to \varphi)$.) The axiom (A1) is projection, the axiom (A2) is transitivity, the axiom (A3) is one of the equivalent forms of the law of double negation, and the inference rule (MP) is *modus ponens*. For a set of formulas Δ and a formula φ we write $\Delta \vdash \varphi$ if there exists a *proof* of φ from Δ, i.e., a sequence of formulas $\varphi_0, \ldots, \varphi_n$ s.t. every φ_i's is either an axiom, an assumption in Δ, or it follows from applying (MP) to some previous formulas φ_j, φ_k with $j, k \in \{0, \ldots, i-1\}$, and the last formula is $\varphi_n \equiv \varphi$.

Problem 1.8.1. As an example, provide a formal proof in Hilbert's system of the following tautology:

$$\varphi \to \varphi. \tag{B0}$$

[solution]

By definition, the deduction (or provability) relation "$\vdash$" is monotonic in the following sense.

Lemma 1.8.2 (Monotonicity)**.** *If $\Delta \vdash \varphi$ and $\Delta \subseteq \Gamma$, then $\Gamma \vdash \varphi$.*

The first important property of the provability relation is that it preserves logical consequence.

Problem 1.8.3 (Soundness)**.** Let φ be a formula. Then,

$$\Delta \vdash \varphi \quad \text{implies} \quad \Delta \vDash \varphi.$$

Hint: Proceed by complete induction on the length of proofs. [solution]

Problem 1.8.4 (Deduction theorem)**.** Show that $\Delta \vdash \varphi \to \psi$ if, and only if, $\Delta \cup \{\varphi\} \vdash \psi$. [solution]

Problem 1.8.5 (Derived theorems)**.** Show how to derive the following tautologies in Hilbert's deduction system.

$$\bot \to \varphi, \tag{B1}$$

$$\varphi \to \neg\neg\varphi, \tag{B2}$$

$$\neg\varphi \to \varphi \to \psi, \tag{B3}$$

$$(\varphi \to \psi) \to (\neg\varphi \to \psi) \to \psi. \tag{B4}$$

$$\varphi \to \neg\psi \to \neg(\varphi \to \psi). \tag{B5}$$

Hint: Do use Problem 1.8.4 "Deduction theorem". [solution]

Definition 1.8.6. Let ϱ be a truth valuation and φ a formula. Then we define φ^ϱ as

$$\varphi^\varrho \equiv \begin{cases} \varphi & \text{if } \varrho(\varphi) = \top, \\ \neg\varphi & \text{otherwise.} \end{cases}$$

The following is the main technical step leading to the completeness theorem

Problem 1.8.7 (Core lemma)**.** Let φ be a formula and let $\bar{q} = (q_1, \ldots, q_n)$ be its variables. For every truth valuation $\varrho : \bar{q} \to \{\top, \bot\}$,

$$\bar{q}^\varrho \vdash \varphi^\varrho.$$

Hint: Proceed by structural induction on φ. [solution]

Problem 1.8.8 (Weak completeness theorem)**.** Let φ be a formula. Then,

$$\vDash \varphi \quad \text{implies} \quad \vdash \varphi.$$

[solution]

Problem 1.8.9 (Strong completeness theorem)**.** Let φ be a formula and let Δ be a set of formulas (possibly infinite). Then,

$$\Delta \vDash \varphi \quad \text{implies} \quad \Delta \vdash \varphi.$$

Hint: Use Problem 1.8.8 "Weak completeness theorem" and Problem 1.5.2. [solution]

1.9 Intuitionistic propositional logic

1.9.1 Gentzen's natural deduction

The syntax of intuitionistic propositional logic is the same as that of its classical counterpart. However, the interpretation of the logical connectives is not given in terms of functions acting on truth values (i.e., truth tables), but in terms of how they act on *proofs*. Negation "$\neg$" is defined via the following shorthand:

$$\neg\varphi \;\equiv\; \varphi \to \bot.$$

A *sequent* is a pair, written $\Gamma \vdash \varphi$, where Γ is a set of propositional formulas. Thus, a sequent is just a data structure, and "$\vdash$" in this context should not be confused with the provability relation in Hilbert's proof system (the symbol is overloaded). New sequents can be derived from other sequents according to the following rules for *Gentzen's natural deduction*. We have a single axiom (rule with no premises) which allows to use an assumption

$$\frac{}{\Gamma, \varphi \vdash \varphi}\ (\mathrm{A})$$

The interpretation of connectives $\to, \wedge, \vee, \bot$ is given by two group of rules. The introduction rules allow the connective to be introduced, and the elimination rules explain how the connective can be eliminated.

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to \mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \to \psi \quad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ (\to \mathrm{E})$$

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge \mathrm{I}) \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ (\wedge \mathrm{E_L}) \quad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ (\wedge \mathrm{E_R})$$

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee \mathrm{I_R}) \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ (\vee \mathrm{I_L}) \qquad \frac{\Gamma \vdash \varphi \vee \psi \quad \Gamma, \varphi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma \vdash \theta}\ (\vee \mathrm{E})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ (\bot \mathrm{E})$$

A *proof tree* is a tree where every node is labelled with a sequent $\Gamma \vdash \varphi$ with the property that the label of every node is obtained by applying a natural deduction rule to its children. We write $\Gamma \vdash_{\mathrm{ND}} \varphi$ if there is a proof tree whose root is labelled by the sequent $\Gamma \vdash \varphi$.

Problem 1.9.1. As a warm-up, prove the following intuitionistic tautologies using natural deduction:

$$
\begin{aligned}
&p \to \neg\neg p,\\
&\neg(p \vee q) \to \neg p \wedge \neg q,\\
&\neg p \wedge \neg q \to \neg(p \vee q),\\
&\neg p \vee \neg q \to \neg(p \wedge q).
\end{aligned}
$$

[solution]

Problem 1.9.2. Is intuitionistic propositional logic monotonic, in the sense that $\Delta \vdash_{\mathrm{ND}} \varphi$ and $\Gamma \supseteq \Delta$ imply $\Gamma \vdash_{\mathrm{ND}} \varphi$? [solution]

1.9.2 Kripke models

The semantics of intuitionistic propositional logic proposed by Samuel Kripke is the one that is the closest to models of classical logic [19]. Fix a finite set P of propositional variables. An *intuitionistic Kripke model* is a tuple $\mathcal{K} = (W, \leq, [\![\cdot]\!])$, where W is a set of *possible worlds*, $\leq \subseteq W \times W$ is a partial order on possible worlds, called *accessibility relation*, and $[\![\cdot]\!] : W \to 2^P$ is a function assigning to a possible world w the set of propositional variables $[\![w]\!] = \{p \in P \mid w \vDash p\}$ which are satisfied in w. The function $[\![\cdot]\!]$ is required to be *monotonic*, in the sense that $[\![w]\!] \subseteq [\![w']\!]$ whenever $w \leq w'$. The function $[\![\cdot]\!]$ uniquely induces the following *satisfaction relation* "$\vDash$" between possible worlds and formulas: For every world w, propositional variable p, and formulas φ, ψ:

$$
\begin{array}{lll}
w \vDash p & \text{if, and only if,} & p \in [\![w]\!],\\
w \vDash \varphi \to \psi & \text{if, and only if,} & \forall (w' \geq w)\,.\, w' \vDash \varphi \text{ implies } w' \vDash \psi,\\
w \vDash \varphi \wedge \psi & \text{if, and only if,} & w \vDash \varphi \text{ and } w \vDash \psi,\\
w \vDash \varphi \vee \psi & \text{if, and only if,} & w \vDash \varphi \text{ or } w \vDash \psi,\\
w \nvDash \bot. & &
\end{array}
$$

(The interpretation of the meta-logical connectives "and", "or", and "implies" on the r.h.s. is classical) We write $\mathcal{K} \vDash \varphi$ if $w \vDash \varphi$ holds for every possible world $w \in W$, $\mathcal{K} \vDash \Gamma$ if $\mathcal{K} \vDash \varphi$ for every $\varphi \in \Gamma$, and $\Gamma \vDash \varphi$ if $\mathcal{K} \vDash \varphi$ holds for every intuitionistic Kripke model $\mathcal{K}$ satisfying $\mathcal{K} \vDash \Gamma$. When $\Gamma = \varnothing$, we just write $\vDash \varphi$ and we say that φ is *intuitionistically valid* (alternatively, an *intuitionistic tautology*).

Intuitively, an intuitionistic Kripke model introduces a dynamic element into models, which are not static but evolve according to the accessibility relation "$\leq$". The monotonicity requirement says that if a propositional variable holds now, then it will hold in every possible future (this holds even for arbitrary formulas; c.f. Problem 1.9.4). The most interesting connective is implication "$\rightarrow$", whose semantics says that an implication $\varphi \rightarrow \psi$ holds in the present if, and only if, for every possible future, whenever φ holds, then ψ holds.

The next exercise shows that Kripke models are a generalisation of truth tables that evolve monotonically over time.

Problem 1.9.3. Show that φ is a classical tautology if, and only if, $\mathcal{K} \vDash \varphi$ holds for every Kripke model with just $|W| = 1$ possible world. [solution]

Problem 1.9.4. Show that the satisfiability relation "$\vDash$" is *monotonic* on all propositional formulas:

$$w \vDash \varphi \text{ and } w \leq w' \quad \text{implies} \quad w' \vDash \varphi.$$

Hint: Proceed by structural induction on formulas. [solution]

Problem 1.9.5 (Soundness of intuitionistic propositional logic)**.** Show that the rules of natural deduction are *sound* w.r.t. Kripke models, in the sense that, for every set of formulas Γ and formula φ of propositional logic,

$$\Gamma \vdash_{\mathrm{ND}} \varphi \quad \text{implies} \quad \Gamma \vDash \varphi.$$

Hint: Use induction on proof trees. [solution]

Problem 1.9.6 (Completeness of intuitionistic propositional logic)**.** Show that the rules of natural deduction are *complete* w.r.t. Kripke models, in the sense that, for every set of formulas Γ and formula φ of propositional logic,

$$\Gamma \vDash \varphi \quad \text{implies} \quad \Gamma \vdash_{\mathrm{ND}} \varphi.$$

[solution]

Problem 1.9.7. Show that the following formulas are not theorems of intuitionistic propositional logic by providing Kripke models as counterexamples:

1. The law of excluded middle: $\varphi_1 \equiv p \vee \neg p$.

2. *Peirce's formula*: $\varphi_2 \equiv ((p \to q) \to p) \to p$.

3. One of De Morgan's laws: $\varphi_3 \equiv \neg(p \wedge q) \to (\neg p \vee \neg q)$.

Can one find Kripke models *with one state* in which the formulas above are not enforced? [solution]

The following exercise explores the connection between restricted classes of Kripke models and validity of classical tautologies which are not intuitionistically valid.

Problem 1.9.8. In which class of Kripke models is the following formula φ satisfied?

$$\varphi \equiv (p \to q) \vee (q \to p).$$ [solution]

Problem 1.9.9 (Disjunction property)**.** Prove that natural deduction has the following *disjunction property*:

$$\vdash_{\mathrm{ND}} \varphi \vee \psi \quad \text{if, and only if,} \quad \vdash_{\mathrm{ND}} \varphi \text{ or } \vdash_{\mathrm{ND}} \psi.$$

Hint: Use Problem 1.9.6 "Completeness of intuitionistic propositional logic". [solution]

Chapter 2

First-order predicate logic

Preliminaries

Syntax. A *signature* is a set of pairs

$$\Sigma = \{f_1 : l_1, \ldots, f_m : l_m, R_1 : k_1, \ldots, R_n : k_n\}, \qquad \text{(signature)}$$

where each *functional symbol* f_i comes equipped with an *arity* $l_i \in \mathbb{N}$, and similarly for each *relational symbol* R_j. A formula of first-order logic is generated by the following abstract syntax

$$\begin{aligned} t, u, v &::\equiv x \mid f_i(t_1, \ldots, t_{l_i}), && \text{(terms)} \\ \varphi, \psi &::\equiv \bot \mid \top \mid R_j(t_1, \ldots, t_{k_j}) \mid t_1 = t_2 \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \neg\varphi \mid \forall x \,.\, \varphi \mid \exists x \,.\, \varphi. && \text{(formulas)} \end{aligned}$$

where x comes from a countable set of variables. Formulas of the form $R_j(t_1, \ldots, t_{k_j})$ and $t_1 = t_2$, as well as $\bot$ and $\top$ are called *atomic formulas*. We assume that the scope of quantifiers $\exists, \forall$ extends as far to the right as possible. For example, $\exists x \,.\, p(x) \vee q(x)$ stands for $\exists x \,.\, (p(x) \vee q(x))$. We write $u \neq v$ as an abbreviation for $\neg(u = v)$.

The *quantifier rank* of a formula φ, denoted $\mathsf{rank}(\varphi)$, is the maximal depth of nesting of its quantificators, as expressed by the following recurrence:

$$
\begin{aligned}
\mathsf{rank}(\bot) = \mathsf{rank}(\top) &= 0 \\
\mathsf{rank}(R_j(t_1,\dots,t_{k_j})) &= 0, \\
\mathsf{rank}(\varphi \wedge \psi) = \mathsf{rank}(\varphi \vee \psi) &= \max(\mathsf{rank}(\varphi), \mathsf{rank}(\psi)), \\
\mathsf{rank}(\neg\varphi) &= \mathsf{rank}(\varphi), \\
\mathsf{rank}(\forall x \,.\, \varphi) = \mathsf{rank}(\exists x \,.\, \varphi) &= 1 + \mathsf{rank}(\varphi).
\end{aligned}
$$

A formula φ is *quantifier-free* if $\mathsf{rank}(\varphi) = 0$, i.e., there are no quantifiers. A variable x is *free* in a formula φ if no occurrence of x falls under the scope of a quantifier $\exists x$ or $\forall x$. Let $\mathsf{fv}(t), \mathsf{fv}(\varphi), \mathsf{fv}(\Gamma)$ be the set of free variables occurring, resp., in the term t, in the formula φ, and in the set of formulas Γ. A *sentence* is a formula with no free variables. A sentence is *universal* if it is of the form $\forall x_1 \dots \forall x_n \,.\, \varphi$, where φ is quantifier-free; existential sentences are defined analogously. A formula is *positive* if it does not contain negations.

Let φ be a formula, let x be a variable, and let t be a term. By $\varphi[x \mapsto t]$ we denote the formula obtained from φ by replacing every free occurrence of x by t.

Semantics. Let Σ be a signature. A Σ-*structure* (or just *structure* when the signature is clear from the context) is a tuple

$$\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \dots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \dots, R_n^{\mathfrak{A}}), \qquad \text{(structure)}$$

where A is a domain, $f_i^{\mathfrak{A}}$ is a function $A^{l_i} \to A$ for every $1 \leq i \leq m$, and $R_j^{\mathfrak{A}}$ is a relation subset of A^{k_j} for every $1 \leq j \leq n$. To keep the notation light, we often write just f_i to denote its interpretation $f_i^{\mathfrak{A}}$, and similarly for R_j. A *relational structure* is a structure $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \dots, R_n^{\mathfrak{A}})$ with $m = 0$ function symbols; for a subset of the domain $B \subseteq A$, the *restriction* of $\mathfrak{A}$ to B (*the substructure of* $\mathfrak{A}$ *induced by* B) is defined as $\mathfrak{A}|_B = (B, R_1^{\mathfrak{A}}|_B, \dots, R_n^{\mathfrak{A}}|_B)$, where $R_j^{\mathfrak{A}}|_B = R_i^{\mathfrak{A}} \cap B^{k_j}$. Equality, $\bot$ and $\top$ are not subject to interpretation. For instance, if $\mathfrak{A} = (A, E^{\mathfrak{A}})$ is a graph, then $\mathfrak{A}|_B$ is the *subgraph induced by* B. A *valuation* is a mapping ϱ assigning a value $\varrho(x) \in A$ to every variable x. Let ϱ be a valuation, x be a variable, and let $a \in A$ be an element of the domain. We denote by $\varrho[x \mapsto a]$ the new valuation which evaluates to a on

x, and agrees with ϱ otherwise. Given a structure $\mathfrak{A}$, a valuation ϱ extends to terms by structural induction as

$$[\![x]\!]^{\mathfrak{A}}_{\varrho} = \varrho(x),$$
$$[\![f_i(t_1,\dots,t_{l_i})]\!]^{\mathfrak{A}}_{\varrho} = f_i^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{A}}_{\varrho},\dots,[\![t_{l_i}]\!]^{\mathfrak{A}}_{\varrho}).$$

The semantics of a first-order formula φ in a structure $\mathfrak{A}$ and valuation ϱ is defined by structural induction as

$$\begin{aligned}
&\mathfrak{A},\varrho \vDash \top \\
&\mathfrak{A},\varrho \nvDash \bot \\
&\mathfrak{A},\varrho \vDash R_j(t_1,\dots,t_{k_j}) &&\text{iff} \quad ([\![t_1]\!]^{\mathfrak{A}}_{\varrho},\dots,[\![t_{k_j}]\!]^{\mathfrak{A}}_{\varrho}) \in R_j^{\mathfrak{A}}, \\
&\mathfrak{A},\varrho \vDash t_1 = t_2 &&\text{iff} \quad [\![t_1]\!]^{\mathfrak{A}}_{\varrho} = [\![t_2]\!]^{\mathfrak{A}}_{\varrho}, \\
&\mathfrak{A},\varrho \vDash \varphi \wedge \psi &&\text{iff} \quad \mathfrak{A},\varrho \vDash \varphi \text{ and } \mathfrak{A},\varrho \vDash \psi, \\
&\mathfrak{A},\varrho \vDash \varphi \vee \psi &&\text{iff} \quad \mathfrak{A},\varrho \vDash \varphi \text{ or } \mathfrak{A},\varrho \vDash \psi, \\
&\mathfrak{A},\varrho \vDash \neg\varphi &&\text{iff} \quad \mathfrak{A},\varrho \nvDash \varphi, \\
&\mathfrak{A},\varrho \vDash \forall x\,.\,\varphi &&\text{iff} \quad \text{for every } a \in A,\ \mathfrak{A},\varrho[x \mapsto a] \vDash \varphi, \\
&\mathfrak{A},\varrho \vDash \exists x\,.\,\varphi &&\text{iff} \quad \text{for some } a \in A,\ \mathfrak{A},\varrho[x \mapsto a] \vDash \varphi.
\end{aligned}$$

We write $[\![\varphi]\!]^{\mathfrak{A}} = \{\varrho \mid \mathfrak{A},\varrho \vDash \varphi\}$ for the set of valuations satisfying φ; by fixing a total order on the k free variables of φ, we can equivalently interpret $[\![\varphi]\!]^{\mathfrak{A}}$ as a subset of A^k. When φ is a sentence, we sometimes omit the valuation and just write $\mathfrak{A} \vDash \varphi$. When Γ is a set of formulas over a signature Σ, we write $\mathfrak{A},\varrho \vDash \Gamma$ whenever $\mathfrak{A},\varrho \vDash \varphi$ for every $\varphi \in \Gamma$. For two sets of formulas Γ,Δ, we write $\Gamma \vDash \Delta$ whenever for every model $\mathfrak{A}$ and valuation ϱ, if $\mathfrak{A},\varrho \vDash \Gamma$, then $\mathfrak{A},\varrho \vDash \Delta$. When $\Gamma = \{\varphi\}$ or $\Delta = \{\psi\}$ contain only one formula, we omit the curly braces and write, e.g., $\Gamma \vDash \psi$ or $\varphi \vDash \psi$.

If Γ is a set of sentences, its set of *models* is denoted by

$$\mathsf{Mod}(\Gamma) = \{\mathfrak{A} \text{ over signature } \Sigma \mid \mathfrak{A} \vDash \Gamma\}.$$

Lemma 2.0.1 (Substitution lemma). *Let φ be a formula, x a variable, and t a term. Assume the following* capture-avoiding condition*:*

$$\begin{gathered}\textit{no free occurrence of } x \textit{ in } \varphi \\ \textit{falls under the scope of a quantifier } Qy \textit{ with } y \in \mathsf{fv}(t)\end{gathered} \tag{$\dagger$}$$

Then,

$$\mathfrak{A}, \varrho \vDash \varphi[x \mapsto t] \quad \textit{if, and only if,} \quad \mathfrak{A}, \varrho[x \mapsto a] \vDash \varphi, \tag{2.1}$$

where $a = [\![t]\!]^{\mathfrak{A}}_{\varrho}$.

Note that both directions of the lemma require the condition (†).

2.1 Definability

Definition 2.1.1. Let Σ be a signature. We say that an isomorphism-closed class of structures $\mathcal{A}$ over Σ is *definable* (equivalently, *expressible*) in first-order logic if there is a sentence φ s.t.

$$\mathfrak{A} \models \varphi \quad \text{if, and only if,} \quad \mathfrak{A} \in \mathcal{A}.$$

The theme of this section is expressing in first-order logic properties of commonly occurring mathematical structures. The counter-point is provided by the inexpressibility results in Sections 2.9 and 2.12.

2.1.1 Real numbers

In this section, consider the structure

$$\mathfrak{A} = (\mathbb{R}, +^{\mathfrak{A}}, *^{\mathfrak{A}}, 0^{\mathfrak{A}}, 1^{\mathfrak{A}}), \tag{2.2}$$

where $\mathbb{R}$ is a set of real numbers and the symbols $+, *, 0, 1$ are interpreted as the corresponding operations on real numbers.

Problem 2.1.2. Show that one can define the natural order "$\leq$" on $\mathbb{R}^2$ as a formula $\varphi(x, y)$ of first-order logic of two free variables x, y. [solution]

Problem 2.1.3 (Periodicity)**.** Extend the signature of the reals with an arbitrary function of one variable $f : \mathbb{R} \to \mathbb{R}$. Show that one can express as a first-order logic sentence φ that f is a periodic function whose smallest strictly positive period is 1. [solution]

Problem 2.1.4 (Continuity and uniform continuity)**.** Express that f is a continuous, resp., uniformly continuous function. [solution]

Problem 2.1.5 (Differentiability)**.** With the same setting as in Problem 2.1.3 "Periodicity", write a formula of first-order logic $\varphi(x)$ with one free variable x expressing that f is differentiable in x. [solution]

2.1.2 Cardinality constraints

Problem 2.1.6 (Cardinality constraints I)**.** For every n, construct a sentence $\varphi_{\geq n}$ of first-order logic with equality, s.t. the following holds for every model $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$:

$$\mathfrak{A} \vDash \varphi_{\geq n} \qquad \text{if, and only if,} \qquad |A| \geq n.$$

Can $\varphi_{\geq n}$ be a universal sentence? [solution]

Problem 2.1.7 (Cardinality constraints II)**.** This exercise is dual to Problem 2.1.6 "Cardinality constraints I". For every n, construct a sentence $\varphi_{\leq n}$ of first-order logic with equality, s.t. the following holds for every model $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$:

$$\mathfrak{A} \vDash \varphi_{\leq n} \qquad \text{if, and only if,} \qquad |A| \leq n.$$

Can $\varphi_{\leq n}$ be an existential sentence? [solution]

2.1.3 Characteristic sentences

Problem 2.1.8 (Characteristic sentences)**.** Show that for each *finite* structure $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$ there exists a first-order sentence $\delta_{\mathfrak{A}}$, called the *characteristic sentence* of $\mathfrak{A}$, s.t., for all structures $\mathfrak{B}$,

$$\mathfrak{B} \vDash \delta_{\mathfrak{A}} \qquad \text{if, and only if,} \qquad \mathfrak{B} \cong \mathfrak{A}.$$

In other words, $\delta_{\mathfrak{A}}$ uniquely determines $\mathfrak{A}$ up to isomorphism. [solution]

2.1.4 Miscellanea

Problem 2.1.9 (Binary trees)**.** In this problem we consider finite trees $\mathfrak{T}$ where each vertex can have zero, one, or two children. The signature consists of two binary relational symbols L and R: $L(x, y)$ means that y is the left son of x, and $R(x, y)$ for the right son; there is always at most one left son, and at most one right son. Prove that, for any natural number $n \in \mathbb{N}$, one can express that $\mathfrak{T}$ is the complete binary tree of depth n (i.e., one where all leaves are at depth n and all other nodes have exactly two children) as a first-order logic sentence φ_n of size $O(n)$ using only two variables x and y (which can be re-quantified as often as necessary). [solution]

Problem 2.1.10 (Conway's "Game of Life")**.** Conway's *game of life* is played on the bidimensional grid

$$\mathfrak{A} = (\mathbb{Z} \times \mathbb{Z}, \leq_1, \leq_2, U),$$

where $U \subseteq \mathbb{Z} \times \mathbb{Z}$ is a unary relation (on $\mathfrak{A}$) denoting the *alive* cells (cells in $(\mathbb{Z} \times \mathbb{Z}) \setminus U$ are *dead*), and $(x_1, x_2) \leq_i (y_1, y_2)$ holds iff $x_i \leq y_i$, for $i \in \{1, 2\}$. The neighbours of a cell (x, y) are the eight cells $(x', y') \neq (x, y)$ satisfying $|x - x'| \leq 1$ and $|y - y'| \leq 1$. At each discrete time step, the status of all cells in the grid changes simultaneously, according to the following rules:

- a dead cell with exactly three alive neighbours becomes alive;
- an alive cell with two or three living neighbours remains alive;
- all other cells remain or become dead.

Prove that, for any $k \in \mathbb{N}$, there is a formula $\varphi_k(x)$ of one free variable s.t. $\mathfrak{A}, x : a \vDash \varphi$ if cell a is alive after the k-th step of the game of life, starting from the position described by U. [solution]

2.2 Normal forms

Problem 2.2.1 (Negation normal form)**.** A formula φ is in *negation normal form* (NNF) if negation is only applied to atomic formulas, i.e., for every subformula of the form $\neg\psi$, $\psi \equiv R_j(\cdots)$ is atomic. Show that each first-order logic formula can be transformed into an equivalent one in NNF. [solution]

Problem 2.2.2 (Prenex normal form)**.** A formula φ is in *prenex normal form* (PNF) if it is of the form

$$\varphi \equiv Q_1 x_1 \cdots Q_n x_n \,.\, \psi$$

where $Q_i \in \{\forall, \exists\}$ and ψ is quantifier-free. Show that for each first-order logic formula there is an equivalent one in PNF. [solution]

Problem 2.2.3. Show that there exists a sentence of first-order logic φ s.t. for any logically equivalent sentence ψ in PNF, ψ has greater quantifier rank: $\mathsf{rank}(\psi) > \mathsf{rank}(\varphi)$. [solution]

Problem 2.2.4. Fix a finite signature Σ. Is there a $k \in \mathbb{N}$ s.t. every first-order sentence φ over Σ is logically equivalent to a sentence of rank k? [solution]

2.3 Satisfaction relation

Problem 2.3.1. In which structures is the following formula of one free variable $\varphi(x) \equiv \exists y \,.\, y \neq x$ satisfied? And the closed formula $\psi \equiv \exists y \,.\, y \neq y$ obtained by "naive" substitution of y in place of x? [solution]

Problem 2.3.2. Consider the formula

$$\varphi \equiv R(x, f(x)) \to \forall x \exists y \,.\, R(f(y), x).$$

Construct two structures $\mathfrak{A} = (A, f^{\mathfrak{A}}, R^{\mathfrak{A}})$ and $\mathfrak{B} = (B, f^{\mathfrak{B}}, R^{\mathfrak{B}})$ and valuations $\rho^{\mathfrak{A}}, \rho^{\mathfrak{B}}$ s.t. $\mathfrak{A}, \rho^{\mathfrak{A}} \models \varphi$ and $\mathfrak{B}, \rho^{\mathfrak{B}} \not\models \varphi$. [solution]

Problem 2.3.3. For each one of the following formulas, check whether it is 1) a tautology, and 2) satisfiable:

$$\begin{aligned}
\varphi_1 &\equiv (\forall x \,.\, P(x) \vee Q(f(x))) \to \forall x \exists y \,.\, P(x) \vee Q(y),\\
\varphi_2 &\equiv (\forall x \exists y \,.\, P(x) \vee Q(y)) \to \forall x \,.\, P(x) \vee Q(f(x)),\\
\varphi_3 &\equiv (\forall x \,.\, P(x) \vee Q(f(x))) \wedge \exists x \forall y \,.\, \neg P(x) \wedge \neg Q(y),\\
\varphi_4 &\equiv (\exists x \,.\, (\forall y \,.\, Q(y)) \to P(x)) \to \exists x \,.\, Q(x) \to P(x).
\end{aligned}$$

[solution]

Problem 2.3.4. Show that the following formula has only infinite models:

$$\varphi \equiv \forall x \,.\, \exists y \,.\, R(x, y) \wedge \forall x \,.\, \neg R(x, x) \wedge \forall x, y, z \,.\, R(x, y) \wedge R(y, z) \to R(x, z).$$

[solution]

Problem 2.3.5. For each of the following signatures, write a sentence that has only infinite models:

1. One unary functional symbol and no relational symbols.
2. One binary relation symbol and no function symbols. [solution]

Problem 2.3.6. Show that the following formula is not a tautology:

$$\varphi \equiv (\forall x \forall y \,.\, f(x) = f(y) \to x = y) \to \forall x \exists y \,.\, f(y) = x.$$

Does its negation have a finite model? [solution]

Problem 2.3.7. Show that the following formula is not a tautology:

$$\varphi \equiv \exists x \exists y \exists u \exists v \,.\, (\neg(x = u) \vee \neg(y = v)) \wedge f(x, y) = f(u, v).$$

1. How many non-isomorphic finite models does $\neg\varphi$ have?

2. Is $\psi \equiv \varphi \vee \forall x \forall y \, . \, x = y$ a tautology? [solution]

Problem 2.3.8. Consider the set Δ consisting of the sentences

$$\exists x \exists y \, . \, x \neq y,$$
$$\forall x \, . \, \neg E(x,x), \text{ and}$$
$$\forall x \forall y \, . \, x \neq y \to \exists z \, . \, E(x,z) \wedge E(y,z).$$

What is the smallest possible number of edges in a graph $\mathfrak{A} = (A, E^{\mathfrak{A}})$ which is a model of Δ? [solution]

Problem 2.3.9. Prove that each satisfiable *existential* sentence has both a finite and an infinite model. [solution]

Problem 2.3.10. Find two *universal* sentences φ_1, φ_2 s.t.

1. φ_1 has a finite model, but no infinite one.

2. φ_2 has an infinite model, but no finite one. [solution]

Problem 2.3.11 (Constructibility)**.** Is it the case, that if $\mathfrak{A} \models \exists x \, . \, \varphi$, then there exists a term t in the language of $\mathfrak{A}$ s.t. $\mathfrak{A} \models \varphi[x \mapsto t]$? In other words, are existential witnesses *constructible*? [solution]

2.4 Skolemisation

We would like to remove the existential quantifiers while preserving satisfiability. Intuitively, $\forall \bar{x} \,.\, \exists y \,.\, \varphi(\bar{x}, y)$ is logically equivalent to $\exists f \,.\, \forall \bar{x} \,.\, \varphi(\bar{x}, f(\bar{y}))$, however we cannot directly express second-order quantification in first-order logic. This difficulty disappears if we do not insist on logical equivalence but just on equisatisfiability, since we can use the implicit second-order quantification of the satisfiability problem. We demonstrate this in detail in the case of one quantifier alternation.

Problem 2.4.1. Let φ be a formula and f a unary function symbol s.t. 1) f is not used in φ, and 2) every free occurrence of variable y in φ is not under the scope of a quantifier binding variable x. Show that

$$\forall x \,.\, \exists y \,.\, \varphi \text{ is satisfiable} \quad \text{if, and only if,} \quad \forall x \,.\, \varphi[y \mapsto f(x)] \text{ is satisfiable.}$$

Is the first assumption necessary? And the second one? Find counterexamples in each case. [solution]

Problem 2.4.2 (Skolemisation)**.** Show that for every sentence φ there exists a *universal* sentence $\forall x_1, \dots, x_n \,.\, \psi$ (with ψ quantifier-free) s.t.

$$\varphi \text{ satisfiable} \quad \text{if, and only if,} \quad \vDash \forall x_1, \dots, x_n \,.\, \psi \text{ satisfiable.}$$

Hint: Generalise Problem 2.4.1. [solution]

Problem 2.4.3 (Herbrandisation)**.** Show that for every sentence φ there exists an *existential* sentence $\exists x_1, \dots, x_n \,.\, \psi$ (with ψ quantifier-free) s.t.

$$\vDash \varphi \quad \text{if, and only if,} \quad \exists x_1, \dots, x_n \,.\, \psi.$$

Hint: Use Problem 2.4.2 "Skolemisation". [solution]

2.5 Herbrand models

Definition 2.5.1. Let $\Sigma = \{f_1, \ldots, f_m, R_1, \ldots, R_n\}$ be a signature. A *Herbrand model* is a structure $\mathfrak{H} = (H, f_1^{\mathfrak{H}}, \ldots, f_m^{\mathfrak{H}}, R_1^{\mathfrak{H}}, \ldots, R_n^{\mathfrak{H}})$ over Σ s.t. the domain H (*Herbrand universe*) is the set of all ground terms constructible from Σ and every function symbol f_i is interpreted "as itself" $f_i^{\mathfrak{H}}(\bar{u}) = f_i(\bar{u})$. This is a model built from pure syntax.

Problem 2.5.2 (Herbrand's theorem)**.** Consider a universal sentence $\varphi \equiv \forall \bar{x} \,.\, \psi$, with ψ quantifier-free. Show that φ is satisfiable if, and only if, it has a Herbrand model. Does this hold for non-universal sentences? [solution]

Problem 2.5.3. Let Σ be a signature containing at least one constant symbol. Let Δ be a set of universal sentences over Σ of the form $\forall x_1, \ldots, x_n \,.\, \psi$ with ψ quantifier-free. Show that the following three conditions are equivalent:

1. Δ is satisfiable.
2. Δ has a Herbrand model.
3. The set following set of ground formulas is satisfiable in the sense of first-order logic:

   $$\Gamma = \{\psi[x_1 \mapsto u_1] \cdots [x_n \mapsto u_n] \mid (\forall x_1, \ldots, x_n \,.\, \psi) \in \Delta \text{ and } u_1 \in H, \ldots, u_n \in H\}. \tag{2.3}$$

4. Let p_ψ be a fresh propositional variable for every atomic formula ψ of the form $u_1 = u_2$ or $R(u_1, \ldots, u_n)$ with $R \in \Sigma$, and let φ^{p} be the formula of propositional logic obtained from φ by replacing every atomic formula ψ as above with p_ψ. The following set of formulas of propositional logic is satisfiable in the sense of propositional logic:

   $$\Gamma^{\mathrm{p}} = \{\varphi^{\mathrm{p}} \mid \varphi \in \Gamma\}. \tag{2.4}$$

[solution]

Problem 2.5.4. Consider a universal sentence of the form $\varphi \equiv \forall \bar{x} \,.\, \psi$, with ψ quantifier-free. Show that φ is unsatisfiable if, and only if, there exist tuples of ground terms $\bar{u}_1, \dots, \bar{u}_n$ s.t. the following is unsatisfiable:

$$\psi[\bar{x} \mapsto \bar{u}_1] \wedge \cdots \wedge \psi[\bar{x} \mapsto \bar{u}_n]. \tag{2.5}$$

Hint: Use Problem 2.5.3 and Problem 1.5.1 "Compactness theorem for propositional logic". [solution]

2.6 Logical consequence

Problem 2.6.1. Consider the following two sentences:

$$\varphi \equiv \forall x \forall y \,.\, y = f(g(x)) \to \exists u \,.\, u = f(x) \wedge y = g(u), \text{and}$$
$$\psi \equiv \forall x \,.\, f(g(f(x))) = g(f(f(x))).$$

Is it the case that φ logically implies ψ, in symbols $\varphi \vDash \psi$? [solution]

Problem 2.6.2. Let f be a unary function symbol and, for $n \in \mathbb{N}$, denote the n-fold application of f to x by

$$f^n(x) := \underbrace{f(\cdots(f(x))\cdots)}_{n}.$$

Does the following hold?

$$\{\forall x \,.\, f^n(x) = x \mid n = 2, 3, 5, 7\} \vDash \forall x \,.\, f^{11}(x) = x.$$ [solution]

2.6.1 Independence

Definition 2.6.3. A set of formulas Δ is *independent* if, for each $\varphi \in \Delta$, $\Delta \smallsetminus \{\varphi\} \nvDash \varphi$.

Independence of an axiom φ in set of axioms Δ is shown by providing a model of $\Delta \smallsetminus \{\varphi\}$ which is not a model of φ.

Problem 2.6.4. Show that the set of axioms of equivalence relations "$\approx$" are independent:

$$\begin{aligned} \Delta = \{ & \forall x \,.\, x \approx x, && \text{(reflexivity)} \\ & \forall x \forall y \,.\, x \approx y \to y \approx x, && \text{(symmetry)} \\ & \forall x \forall y \forall z \,.\, x \approx y \wedge y \approx z \to x \approx z \}. && \text{(transitivity)} \end{aligned}$$ [solution]

Problem 2.6.5. Show that the set of axioms of linear orders "$\leq$" are independent:

$$\begin{aligned} \Delta_{\text{lin}} = \{ & \forall x \forall y \,.\, x \leq y \wedge y \leq x \to x = y, && \text{(antisymmetry)} \\ & \forall x \forall y \forall z \,.\, x \leq y \wedge y \leq z \to x \leq z, && \text{(transitivity)} \\ & \forall x \forall y \,.\, x \leq y \vee y \leq x \}. && \text{(totality)} \end{aligned}$$ [solution]

Problem 2.6.6. Show that the set of axioms of groups with a binary operation "$*$" and unit element "1" are independent:

$$
\begin{aligned}
\Delta = \{&\forall x\,.\,1 * x = x \land x * 1 = x, && \text{(unit)}\\
&\forall x, y, z\,.\,(x * y) * z = x * (y * z), && \text{(associativity)}\\
&\forall x\,.\,\exists y\,.\,x * y = 1 \land y * x = 1\}. && \text{(inverses)}
\end{aligned}
$$

[solution]

Problem 2.6.7. Prove that every *finite* set of sentences Δ contains a subset $\Delta' \subseteq \Delta$ s.t. Δ' is independent and $\Delta' \vDash \Delta$. Is the finiteness assumption necessary? [solution]

We have seen in Problem 2.6.7 that in general infinite set of sentences do not have any equivalent independent *subset*. In the next exercise we look for an equivalent independent set of axioms (which is not necessarily a subset of the original set).

Problem 2.6.8. Prove that every class of structures over a finite signature which is axiomatised by a set of first-order sentences, can be axiomatised by an *independent* set of first-order sentences. [solution]

2.7 Axiomatisability

Definition 2.7.1. Let Σ be a signature. We say that a class of structures $\mathcal{A}$ over Σ is *axiomatisable* in first-order logic if there is a set of sentences Δ s.t.

$$\mathfrak{A} \models \Delta \quad \text{if, and only if,} \quad \mathfrak{A} \in \mathcal{A}.$$

The following problem shows a perhaps surprising property of countable classes of finite structures.

Problem 2.7.2 (Classes of finite structures are axiomatisable)**.** Fix a finite signature Σ. Show that any countable class $\mathcal{A}$ of *finite* structures over Σ is axiomatisable. *Hint: Use the characteristic sentences from Problem 2.1.8 "Characteristic sentences".* [solution]

Problem 2.7.3 (Universal axiomatisations)**.** Recall that $\mathfrak{B}$ is an induced substructure of $\mathfrak{A}$ if if can obtained from the latter by taking a subset of the domain, and restricting the relations to the new domain. Show that an isomorphism-closed class $\mathcal{A}$ of finite relational structures can be axiomatised by a set of *universal* sentences of first-order logic if, and only if, $\mathcal{A}$ is closed under induced substructures. [solution]

2.8 Spectrum

Definition 2.8.1. The *spectrum* of a sentence φ, denoted $\mathsf{Spec}(\varphi)$, is the set of all positive integers $n \in \mathbb{N}$ s.t. φ has a model of cardinality n:

$$\mathsf{Spec}(\varphi) = \{|A| \mid \mathfrak{A} = (A, \ldots), \mathfrak{A} \models \varphi, \ A \text{ finite}\} \subseteq \mathbb{N}.$$

The notion of spectrum pertains to which cardinalities can be represented by first-order sentences ("recognised" in the automata-theoretic jargon), and does not take into account the *multiplicity* of each cardinality, i.e., the number of non-isomorphic models of a given size.

2.8.1 Examples

In the following problems, in order to show that a set of natural numbers $N \subseteq \mathbb{N}_{>0}$ is a first-order spectrum, one must exhibit a first-order sentence φ over a chosen signature s.t. $\mathsf{Spec}(\varphi) = N$.

Problem 2.8.2 (Finite and cofinite sets are spectra)**.** Show that if $N \subseteq \mathbb{N}_{>0}$ is either finite or co-finite (i.e., its complement $\mathbb{N}_{>0} \setminus N$ is finite), then N is a first-order spectrum. [solution]

Problem 2.8.3 (Even numbers)**.** Show that the set of all positive even numbers $\{2 \cdot n \mid n \in \mathbb{N}_{>0}\}$ is a first-order spectrum. *Hint: Use a unary function symbol f.* [solution]

Problem 2.8.4. Show that the set of squares $\{n^2 \mid n \in \mathbb{N}_{>0}\}$ is a first-order spectrum. *Hint: Use a binary function symbol f and a unary relation symbol U.* [solution]

Problem 2.8.5. Show that the set $\{m \cdot n \mid m, n \in \mathbb{N}_{>0}\}$ of positive composite numbers is a first-order spectrum. *Hint: Use a binary function symbol f and two unary relation symbols U, V.* [solution]

Problem 2.8.6. Show that the set of powers of two $\{2^n \mid n \in \mathbb{N}\}$ is a first-order spectrum. *Hint: Axiomatise the membership relation "$\in$".* [solution]

Problem 2.8.7. Show that the set of self-powers $\{n^n \mid n \in \mathbb{N}_{>0}\}$ is a first-order spectrum. *Hint: Axiomatise the relation Apply(f, u, v), which holds iff "$f(u) = v$".* [solution]

Problem 2.8.8. Show that the set of factorials $\{n! \mid n \in \mathbb{N}\}$ is a first-order spectrum. *Hint: Axiomatise that the universe is the set of all linear orders on U.* [solution]

Problem 2.8.9. Find a first-order sentence φ s.t. its spectrum is precisely the powers of all prime numbers:

$$\mathsf{Spec}(\varphi) = \{p^n \mid p, n \in \mathbb{N}, p \text{ prime}\}.$$ [solution]

2.8.2 Closure properties

Problem 2.8.10 (Spectra are closed under union)**.** Show that spectra of first-order logic sentences are closed under finite union. [solution]

Problem 2.8.11 (Spectra are closed under intersection)**.** Show that spectra of first-order logic sentences are closed under finite intersection. [solution]

Note. The related problem of whether first-order spectra are closed under complementation has been posed in 1955 by Günter Asser [3] and it is still open to these days [10]. For spectra of second-order sentences, closure under complement is known and it is the subject of Problem 3.1.3 "Spectrum".

For two sets of natural numbers $M, N \subseteq \mathbb{N}$, we interpret $M + N$ and $M \cdot N$ "á la Minkowski" (i.e., pointwise) as

$$\begin{aligned} M + N &:= \{m + n \mid m \in M, n \in N\}, \text{ and} \\ M \cdot N &:= \{m \cdot n \mid m \in M, n \in N\}. \end{aligned}$$

Problem 2.8.12 (Spectra are closed under addition)**.** Show that spectra of first-order logic sentences are closed under addition "+". [solution]

Problem 2.8.13 (Spectra are closed under multiplication)**.** Show that spectra of first-order logic sentences are closed under multiplication "·". [solution]

Definition 2.8.14. A set of natural numbers $L \subseteq \mathbb{N}$ is *linear* if there is a base $b \in \mathbb{N}$ and finitely many periods $p_1, \dots, p_n \in \mathbb{N}$ s.t.

$$L = \{b + k_1 \cdot p_1 + k_2 \cdot p_2 + \cdots k_n \cdot p_n \mid \text{for some } k_1, k_2, \dots, k_n \in \mathbb{N}\}.$$

A *semilinear* set is a finite union of linear sets.

Problem 2.8.15 (Semilinear sets are spectra)**.** Show that any semilinear set not containing 0 is the spectrum of a sentence of first-order logic. [solution]

For a set of natural numbers $M \subseteq \mathbb{N}$, consider the following iteration operation “á la Kleene”

$$M^+ = M \cup (M + M) \cup \cdots.$$

Problem 2.8.16 (Spectra and Kleene iteration)**.** Are spectra of first-order logic sentences closed under the iteration operation “$(\_)^+$”?. [solution]

Problem 2.8.17 (Doubling)**.** Given a first-order logic sentence φ, construct a sentence ψ s.t.

$$\mathsf{Spec}(\psi) \;=\; \{2 \cdot n \mid n \in \mathsf{Spec}(\varphi)\}.$$ [solution]

2.8.3 Restricted formulas

Problem 2.8.18 (Spectra with only unary relations)**.** Consider a sentence φ containing only unary relational symbols. Prove that $\mathsf{Spec}(\varphi)$ is either finite or cofinite. [solution]

The problem above is optimal, in the sense that already with only one unary *function* symbol one can define spectra which are neither finite nor cofinite, as we show below[1].

Problem 2.8.19 (Spectra with a unary function)**.** Find a sentence φ with only one unary *function* symbol f s.t. neither $\mathsf{Spec}(\varphi)$ nor its complement is finite. [solution]

Problem 2.8.20. Give an example of a sentence of first-order logic φ s.t. $\mathsf{Spec}(\varphi) = \mathsf{Spec}(\neg\varphi)$ using only a single unary relation symbol U. Does such an example exists using only a unary function symbol f? [solution]

Problem 2.8.21 (Spectra of existential sentences)**.** Show that the spectrum of an existential first-order sentence φ is *upward closed*, in the sense that $m \in \mathsf{Spec}(\varphi)$ and $n \geq m$ imply $n \in \mathsf{Spec}(\varphi)$. *Hint: C.f. Problem 2.3.9, and also Problem 2.11.3 “Fundamental property” (point 3).* [solution]

[1] Spectra of sentences using only one unary function symbol are known to be precisely the ultimately periodic sets [9].

Problem 2.8.22 (Spectra of universal sentences)**.** Prove that for every first-order sentence φ there exists a universal first-order sentence ψ, perhaps over a larger signature, having the same spectrum $\mathsf{Spec}(\varphi) = \mathsf{Spec}(\psi)$. What if we require that ψ uses only relational symbols? *Hint: Use Problem 2.4.2 "Skolemisation".* [solution]

Problem 2.8.23 (Spectra of $\exists^*\forall^*$-sentences)**.** Show that the spectrum of a $\exists^*\forall^*$-sentence of first-order logic (i.e., in the so called *Bernays-Schönfinkel-Ramsey* class) using only relational symbols is either finite or cofinite. Does this hold for $\forall\exists^*$-sentences? *Hint: Use Problem 2.11.4 "Preservation for $\exists^*\forall^*$-sentences".* [solution]

2.8.4 Counting models

In this series of problems we study a refinement of the notion of spectrum.

Definition 2.8.24. Let the *counting spectrum* of φ be the ordered sequence of positive natural numbers $a_1 a_2 \cdots \in \mathbb{N}_{>0}^{\omega}$ s.t., for every n, there are precisely a_n nonisomorphic models of φ of cardinality n. This is a strict generalisation of the spectrum, which can be reconstructed as $\{n \mid a_n > 0\}$.

Problem 2.8.25. Show that the sequence $a_n = n$ is the counting spectrum of a sentence of first-order logic. [solution]

Problem 2.8.26. Show that the sequence $a_n = 2^n$ is the counting spectrum of a sentence of first-order logic. [solution]

Problem 2.8.27. Let k be a fixed constant. Show that the sequence a_n defined as $\binom{n}{k}$ for $n \geq k$ and 0 for $n < k$ is the counting spectrum of a sentence of first-order logic. [solution]

Problem 2.8.28. Show that the sequence $a_n = n!$ is the counting spectrum of a sentence of first-order logic. [solution]

2.8.5 Characterisation

The following problem shows a complexity upper bound for spectra of first-order logic.

Problem 2.8.29 (Spectra are in $\mathsf{NEXPTIME}$)**.** Show that the following decision problem is in the complexity class $\mathsf{NEXPTIME}$:

Spectrum membership.

Input: A sentence of first-order logic φ and a number $n \in \mathbb{N}$ encoded in binary.

Output: Is it the case that $n \in \mathsf{Spec}(\varphi)$? [solution]

Note. In fact, *every* set in NEXPTIME can be expressed as the spectrum of a sentence of first-order logic. This seminal result was independently proved in the 1970's by Jones and Selman [17] and by Fagin [12] .

2.9 Compactness

Problem 2.9.1 (Compactess theorem)**.** Prove that if $\Gamma \vDash \varphi$, then there exists a finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ s.t. $\Gamma_0 \vDash \varphi$. *Hint: Use Gödel's completeness theorem.* [solution]

Problem 2.9.2 (Compactness theorem (w.r.t. satisfiability))**.** Sometimes the compactness theorem is stated in the following form: If every finite subset of Γ is satisfiable, then Γ is also satisfiable. Show that this alternative form is equivalent to Problem 2.9.1 "Compactess theorem". [solution]

Problem 2.9.3 (Compactness in finite structures?)**.** Establish whether the following variant of compactness for finite structures holds: If every *finite* model of Γ is also a model of φ, then there is a finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ with the same property. [solution]

Problem 2.9.4. Prove that if a class $\mathcal{A}$ of structures over a signature Σ and its complement $\mathsf{Mod}(\Sigma) \setminus \mathcal{A}$ are both axiomatisable by a set of first-order sentences, then each of them is definable by a first-order sentence. [solution]

The previous exercise has the following natural generalisation in terms of separability.

Problem 2.9.5 (Definable separability of axiomatisable classes)**.** We say that two disjoint classes of structures $\mathcal{A}, \mathcal{B}$ are *separated* by a class $\mathcal{C}$ if $\mathcal{A} \subseteq \mathcal{C}$ and $\mathcal{C} \cap \mathcal{B} = \varnothing$. Show that two disjoint first-order axiomatisable classes are separable by a first-order definable class. Why does this generalise Problem 2.9.4? [solution]

2.9.1 Nonaxiomatisability

Problem 2.9.6 (Finiteness is not axiomatisable)**.** Show that there is no set of first-order sentences Δ s.t. $\mathfrak{A} \vDash \Delta$ if, and only if, $\mathfrak{A}$ is finite. [solution]

Problem 2.9.7 (Finite diameter is not axiomatisable)**.** The *diameter* of a graph is the smallest $n \in \mathbb{N} \cup \{\infty\}$ s.t. any two vertices are connected by a path of length at most n. Prove that the class of graphs of finite diameter is not axiomatisable by any set of first-order logic sentences. [solution]

Problem 2.9.8 (Finite colourability is not axiomatisable)**.** A *finite colouring* of a graph $\mathfrak{G} = (V, E)$ is a mapping $c : V \to C$, where C is a finite set of colours, s.t. every two vertices connected by an edge get a different colour: $(u, v) \in E$ implies $c(u) \neq c(v)$. Show that the class of finitely colourable graphs cannot be axiomatised by any set of sentences of first-order logic. [solution]

Problem 2.9.9 (Finitely many equivalence classes is not axiomatisable)**.** Show that the class of equivalence relations $\sim \subseteq A \times A$ containing finitely may equivalence classes (i.e., of finite index) is not axiomatisable. [solution]

Problem 2.9.10 (Finite equivalence classes is not axiomatisable)**.** We want to show that the class of equivalence relations $\sim \subseteq A \times A$ where every class is finite is not axiomatisable.

1. A standard way of reasoning is to extend a purported axiomatisation Δ as $\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \ldots\}$, where φ_n says that there is an equivalence class containing at least n elements:

   $$\varphi_n \ \equiv\ \exists x_1 \cdots \exists x_n \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge x_i \sim x_j .$$

   Do models of Γ have an infinite equivalence class?

2. If not, how can we amend the φ_n's in order to ensure that Γ has only models with an infinite equivalence class? [solution]

Problem 2.9.11 (Finitely generated monoids are not axiomatisable)**.** A *monoid* is a structure

$$\mathfrak{M} = (M, \circ, e),$$

where $\circ : M \times M \to M$ is an associative binary operation with neutral element $e \in M$. A monoid $\mathfrak{M}$ is *finitely generated* if there exist finitely many elements $a_1, \ldots, a_n \in M$ s.t. every $a \in M$ is a product of the a_i's. (For example, $(A^*, \cdot, \varepsilon)$ is finitely generated iff the alphabet A is finite.) Prove that the class of finitely generated monoids is not axiomatisable. [solution]

Problem 2.9.12 (Cycles are not axiomatisable)**.** Prove that the class $\mathcal{C}$ of graphs containing a cycle is not axiomatisable by any set of first-order logic sentences. [solution]

Problem 2.9.13 (Unions of cycles are not axiomatisable)**.** Prove that the class $\mathcal{C}$ of graphs where every vertex belongs to a cycle is not axiomatisable by any set of first-order logic sentences. [solution]

Problem 2.9.14 (The Church-Rosser property is not axiomatisable (via compactness))**.** A binary relation $\to \subseteq A \times A$ has the *Church-Rosser property* (CR) if, whenever $a \to^* b$ and $a \to^* c$, there exists d s.t. $b \to^* d$ and $c \to^* d$. Prove that CR is not axiomatisable by any set of first-order logic sentences. [solution]

Problem 2.9.15 (Strong normalisation is not axiomatisable (via compactness))**.** A binary relation $\to \subseteq A \times A$ is *strongly normalising* (SN) if there is no infinite path

$$a_1 \to a_2 \to \cdots \quad (a_1, a_2, \cdots \in A)$$

Prove that SN is not axiomatisable in first-order logic. [solution]

Problem 2.9.16 (Well-orders are not axiomatisable)**.** A *well-order* is a strict total order $<$ not containing an infinite descending chain $a_0 > a_1 > \cdots$. Prove that well-orders are not axiomatisable. [solution]

Problem 2.9.17. Consider the class $\mathcal{A}$ of partial orders $(A, \sqsubseteq)$ with infinitely many minimal elements s.t. every non-minimal element $a \in A$ is a supremum $a = \bigsqcup B$ of finitely many minimal elements $B = \{a_1, \ldots, a_n\}$. Prove that $\mathcal{A}$ is not axiomatisable by any set of sentences of first-order logic. [solution]

Problem 2.9.18. Prove that if Δ is a set of sentences s.t. $\mathsf{Spec}(\neg\varphi)$ is finite for every $\varphi \in \Delta$, and $\Delta \models \psi$, then $\mathsf{Spec}(\neg\psi)$ is also finite. [solution]

Problem 2.9.19. Consider structures $\mathfrak{A}$ over a signature consisting of binary operations $+, -, *$, constants $0, 1$, and an additional unary operation f. We say that f is *expressible* if there is a term $\tau(x)$ with one free variable x not containing f s.t.

$$\mathfrak{A} \models \forall x \,.\, \tau(x) = f(x).$$

(For example, if $A = \mathbb{R}$ with the usual interpretation of $+, -, *, 0, 1$, then f if expressible if it is a polynomial of one variable with integer coefficients.) Prove that the class of structures $\mathfrak{A}$ where f is expressible is not axiomatisable. [solution]

Problem 2.9.20. We say that a structure $\mathfrak{A}$ over signature Σ has *property F* if for any two terms s, t with one free variable x, the set of elements $a \in A$ satisfying the equation

$$\mathfrak{A}, x : a \models s = t$$

is either finite or the whole A. (For example, the field of real numbers $(F, +, *, 0, 1)$ has property F, since terms define polynomial functions, and the latter are either identically 0 or have finitely many roots.) Prove that:

1. If Σ contains only constant symbols and relation symbols, then property F is axiomatisable.

2. If Σ contains at least one unary function symbol, then property F is not axiomatisable. [solution]

Problem 2.9.21 (Periodicity is not axiomatisable)**.** Consider structures of the form $\mathfrak{A} = (A, +, s, f, 0)$, where $+$ is a binary operation, s and f are unary functions, and 0 is a constant. The function f is *periodic* if there exists $k \in A$, $k \neq 0$, s.t. $f(x + k) = f(x)$ for every $x \in A$, and *standard periodic* if k is additionally of the form $k = s^k(0)$. Consider the classes of structures where

1. f is periodic;

2. f is standard periodic;

3. f is *not* standard periodic.

For each of the classes above, determine whether it is a) definable by a single sentence; b) axiomatisable by a set of sentences, but not definable by a single sentence; c) not axiomatisable by any set of sentences. [solution]

Problem 2.9.22. Let f be a unary function symbol, and consider the class of structures

$$\mathcal{A} = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \mathsf{Mod}(\varphi_n),$$

where $\varphi_n \equiv \forall x \,.\, f^n(x) = x$ expresses that the n-th iterate of f, defined as $f^n(x) = \underbrace{f(\ldots f}_{n}(x)\ldots)$, is the identity function.

1. Prove that $\mathcal{A}$ cannot be axiomatised by any set of first-order sentences.
2. Can $\mathsf{Mod}(\{f\}) \setminus \mathcal{A}$ be axiomatised by *a set* of first-order sentences?
3. Prove that $\mathsf{Mod}(\{f\}) \setminus \mathcal{A}$ cannot be defined with *a single* first-order sentence. [solution]

2.9.2 Extensions

The following problems show that we can use compactness to build new models satisfying interesting limit properties.

Problem 2.9.23. Let A be an infinite set. Show using Problem 2.9.1 "Compactess theorem" that every partial order $\sqsubseteq \subseteq A \times A$ can be extended to a total order $\leq \subseteq A \times A$ (in the sense that $\sqsubseteq \subseteq \leq$). [solution]

In the next problem we explore a special property of the real numbers which is not first-order.

Problem 2.9.24 (Non-Archimedean reals)**.** Consider the first-order theory $\mathsf{Th}(\mathbb{R})$ of the real numbers $(\mathbb{R}, \Sigma)$ over the signature $\Sigma = \{0, 1, +, \cdot\}$ (i.e., the set of all first-order formulas φ s.t. $\mathbb{R} \models \varphi$). The reals satisfy the following important *Archimedean property*: For all positive real numbers $a, b > 0$, there is a natural number n s.t. $n \cdot a > b$.

1. Show that the real numbers can be conservatively extended to a non-Archimedean field $\mathbb{R}^*$ in the sense that $\mathsf{Th}(\mathcal{R}) \subseteq \mathsf{Th}(\mathbb{R}^*)$ (possibly enlarging the signature). *Hint: Force an arbitrarily large element.*
2. Is it possible that $\mathbb{R}^*$ satisfies a formula over the common signature Σ not satisfied by $\mathbb{R}$, i.e., that $\mathsf{Th}(\mathcal{R}) \neq \mathsf{Th}(\mathbb{R}^*) \cap \mathsf{Th}(\Sigma)$?

[solution]

Problem 2.9.25. The compactness theorem is a purely semantic statement. Its proof in Problem 2.9.1 "Compactess theorem" using completeness, and thus referring to proofs can be considered unsatisfactory. Prove the compactness theorem for first-order logic by using Problem 2.5.3 and Problem 1.5.1 "Compactness theorem for propositional logic". [solution]

2.10 Skolem-Löwenheim theorems

2.10.1 Going upwards

Theorem 2.10.1 (Upward Skolem-Löwenheim theorem). *If* Γ *is a set of sentences over a signature* Σ *with an infinite model, then it has a model* $\mathfrak{A} \models \Gamma$ *of every sufficiently large cardinality* $\kappa = |A| \geq |\Sigma|, |\Gamma|$.

Problem 2.10.2 (Hessenberg theorem). Show that for each infinite cardinal $\mathfrak{m}$, we have $\mathfrak{m}^2 = \mathfrak{m}$. *Hint: Express that the cardinality of the universe is not smaller than the cardinality of its Cartesian square. Show that the sentence has an infinite model and use Theorem 2.10.1 "Upward Skolem-Löwenheim theorem".* [solution]

Problem 2.10.3. Is there a set of first-order logic sentences over a finite signature, which has finite models of every even cardinality, but has no model of the continuum cardinality $\mathfrak{c}$? [solution]

Problem 2.10.4 (Infinite axiomatisability?). We want to extend Problem 2.1.8 "Characteristic sentences" to deal with countable structures over a countable signature

$$\mathfrak{A} = (\{a_1, a_2, \dots\}, R_1^{\mathfrak{A}}, R_2^{\mathfrak{A}}, \dots)$$

Is it possible to find a countable set of sentences $\Delta_{\mathfrak{A}}$ s.t., for every structure $\mathfrak{B}$,

$$\mathfrak{B} \models \Delta_{\mathfrak{A}} \qquad \text{if, and only if,} \qquad \mathfrak{B} \cong \mathfrak{A}?$$ [solution]

Problem 2.10.5 (Nowhere dense orders). A strict linear order $\mathfrak{A} = (A, <)$ is *nowhere dense* if for any two elements $x, y \in A$ with $x < y$, there are only finitely many elements $z \in A$ s.t. $x < z < y$. Show that nowhere dense linear orders cannot be axiomatised in first-order logic. [solution]

2.10.2 Going downwards

Theorem 2.10.6 (Downward Skolem-Löwenheim theorem). *If* Γ *is a satisfiable set of sentences over a signature* Σ*, then it has a model* $\mathfrak{A} \models \Gamma$ *of cardinality* $\kappa = |\mathfrak{A}| \leq |\Sigma|$.

Problem 2.10.7. Let $\mathcal{A}$ be an axiomatisable class of structures over a countable signature Σ. Show that if there is an infinite structure not in $\mathcal{A}$, then there is a countable structure not in $\mathcal{A}$. [solution]

Problem 2.10.8. Let A be a fixed set. Consider the class $\mathcal{A}$ of structures isomorphic to $(A^{\mathbb{N}}, R)$, where $A^{\mathbb{N}}$ is the set of all infinite sequences of elements of A and $R(x, y)$ holds if, and only if, the set of positions at which x and y differ is finite. Prove that $\mathcal{A}$ is axiomatisable in first-order logic if, and only if, $|A| = 1$. [solution]

Problem 2.10.9. Prove that the class of all algebras $\mathfrak{A} = (A, f)$, where f is a unary function symbol, s.t. $|f(A)| < |A|$ (the cardinality of the codomain of f is strictly smaller than the cardinality of the universe), is not axiomatisable in first-order logic. [solution]

Problem 2.10.10 (Function semigroups)**.** Consider a signature with a binary operation $\circ$ and a constant symbol id. A model $\mathfrak{F}$ over this signature is called a *function semigroup* if its carrier is the set of all functions $f : A \to A$ on some set A, $\circ$ is function composition, and id is the identity function. Prove that the class of function semigroups cannot be axiomatised in first-order logic. [solution]

Problem 2.10.11. Prove that the class of all structures isomorphic to $\mathfrak{A} = (\mathcal{P}(A), \cup, \cap, \subseteq)$, where $\cup, \cap$ are the binary operations of union, resp., intersection, and $\subseteq$ is the set containment relation, is not axiomatisable in first-order logic. [solution]

We have seen in Problem 2.9.15 "Strong normalisation is not axiomatisable (via compactness)" that strong normalisation is not axiomatisable, and in Problem 2.9.16 "Well-orders are not axiomatisable" that well-orders are not axiomatisable. Since a well-order R is in particular strongly normalising (up to reversal), one may wonder whether it was necessary to prove nonaxiomatisability twice. The following exercise answer this question positively, showing that nonaxiomatisability of a class of structures is not monotonic w.r.t. subset inclusion.

Problem 2.10.12. Prove that there are three isomorphism closed classes $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$ of structures over the same finite signature, such that:

- $\mathcal{B}$ is not axiomatisable even though $\mathcal{A}$ and $\mathcal{C}$ are.

- $\mathcal{B}$ is axiomatisable even though $\mathcal{A}$ and $\mathcal{C}$ are not. [solution]

2.11 Relating models

2.11.1 Relational homomorphisms

In this section we study preservation properties of structures.

Definition 2.11.1. Consider two over the same signature

$$\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \dots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \dots, R_n^{\mathfrak{A}}) \text{ and } \mathfrak{B} = (B, f_1^{\mathfrak{B}}, \dots, f_m^{\mathfrak{B}}, R_1^{\mathfrak{B}}, \dots, R_n^{\mathfrak{B}}).$$

A *relational homomorphism* between $\mathfrak{A}$ and $\mathfrak{B}$ is a relation $R \subseteq A \times B$ preserving the interpretation of function and relations: for every functional symbol f_i and tuples $\bar{a} \in A^{l_i}, \bar{b} \in B^{l_i}$, if $(\bar{a}, \bar{b}) \in R$, then $(f_i^{\mathfrak{A}}(\bar{a}), f_i^{\mathfrak{B}}(\bar{b})) \in R$[2], and for every relational symbol R_j and tuples $\bar{a} \in A^{k_j}, \bar{b} \in B^{k_j}$, if $(\bar{a}, \bar{b}) \in R$, then

$$\bar{a} \in R_j^{\mathfrak{A}} \quad \text{implies} \quad \bar{b} \in R_j^{\mathfrak{B}},$$

A relational homomorphism R is extended on variable valuations ϱ in $\mathfrak{A}$ and σ in $\mathfrak{B}$ as $(\varrho, \sigma) \in R$ if, for every variable x, we have $(\varrho(x), \sigma(x)) \in R$. The relational homomorphism R is *faithful* if we additionally have equivalence "iff" above. A formula $\varphi(x_1, \dots, x_n)$ is *preserved* by a relational homomorphism $R \subseteq A \times B$ if $(\varrho, \sigma) \in R$ implies

$$\mathfrak{A}, \varrho \vDash \varphi \quad \text{implies} \quad \mathfrak{B}, \sigma \vDash \varphi. \tag{2.6}$$

For example, if $\mathfrak{B}$ is an induced substructure of $\mathfrak{A}$, then there exists a relational homomorphism between $\mathfrak{A}$ and $\mathfrak{B}$ which is injective, surjective, and faithful.

Problem 2.11.2. Show that a relational homomorphism R preserves the meaning of terms, in the sense that, for any term t,

$$(\varrho, \sigma) \in R \quad \text{implies} \quad (\llbracket t \rrbracket_\varrho^{\mathfrak{A}}, \llbracket t \rrbracket_\sigma^{\mathfrak{B}}) \in R.$$

Additionally equality of terms is preserved when R is injective:

$$\llbracket u \rrbracket_\varrho^{\mathfrak{A}} = \llbracket v \rrbracket_\varrho^{\mathfrak{A}} \quad \text{implies} \quad \llbracket u \rrbracket_\sigma^{\mathfrak{B}} = \llbracket v \rrbracket_\sigma^{\mathfrak{B}}.$$ [solution]

[2] In the special case of zero-ary constants c, we always have $(c^{\mathfrak{A}}, c^{\mathfrak{B}}) \in R$.

feature	formulas preserved
relational homomorphism	positive, quantifier-free
faithfulness	negation "$\neg$"
totality	existential quantification "$\exists$"
surjectivity	universal quantification "$\forall$"
injectivity	equality "="

Figure 2.1: Relational homomorphisms and formulas

Problem 2.11.3 (Fundamental property)**.** Let R be a relational homomorphism between $\mathfrak{A}$ and $\mathfrak{B}$, and consider formulas without equality. Show that

1. All positive quantifier-free formulas are preserved.
2. If R is (left) total, then it preserves all positive existential formulas.
3. If R is total and faithful, then it preserves all existential formulas.
4. If R is surjective (right total), then it preserves all positive universal formulas.
5. If R is surjective and faithful, then it preserves all universal formulas.
6. If R is total and surjective, then it preserves all positive formulas.
7. If R is total, surjective, and faithful, then it preserves all formulas.
8. If R is injective, then it preserves formulas with equality. [solution]

The relationship between relational homomorphisms and the features they preserve is summarised in Figure 2.1

Problem 2.11.4 (Preservation for $\exists^*\forall^*$-sentences)**.** Show that for every $\exists^n\forall^*$-sentence of first-order logic φ over a signature without function symbols, if $\mathfrak{A} \models \varphi$, then there exists a *core* $C \subseteq A$ of at most n elements s.t. every induced substructure $\mathfrak{B}$ of $\mathfrak{A}$ containing $C \subseteq B$ is also a model $\mathfrak{B} \models \varphi$. [solution]

2.11.2 Isomorphisms

Definition 2.11.5. Consider two structures $\mathfrak{A} = (A, \Sigma)$ and $\mathfrak{B} = (B, \Sigma)$ over the same signature Σ. An *isomorphism* between $\mathfrak{A}$ and $\mathfrak{B}$ is a bijection $h : A \to B$ s.t. for every functional symbol $f_i \in \Sigma$ and $a_1, \ldots, a_{l_i} \in A$,

$$h(f^{\mathfrak{A}}(a_1, \ldots, a_{l_i})) = f^{\mathfrak{B}}(h(a_1), \ldots, h(a_{l_i})),$$

and for every relational symbol $R_j \in \Sigma$ and $a_1, \ldots, a_{k_j} \in A$,

$$(a_1, \ldots, a_{k_j}) \in R_j^{\mathfrak{A}} \quad \text{if, and only if,} \quad (h(a_1), \ldots, h(a_{k_j})) \in R_j^{\mathfrak{B}}.$$

When the above holds, we write $\mathfrak{A} \cong_h \mathfrak{B}$. An *automorphism* is an isomorphism on the same structure $\mathfrak{A} \cong_h \mathfrak{A}$. When there exists an isomorphism between $\mathfrak{A}$ and $\mathfrak{B}$, we say that the two structures are *isomorphic*, written $\mathfrak{A} \cong \mathfrak{B}$.

The following problem shows that first-order logic formulas are invariant under isomorphism.

Problem 2.11.6 (Isomorphism theorem)**.** Show that $\mathfrak{A} \cong_h \mathfrak{B}$ implies that, for every formula φ and for every valuation ϱ of $\mathfrak{A}$,

$$\mathfrak{A}, \varrho \models \varphi \quad \text{if, and only if} \quad \mathfrak{B}, \varrho \circ h^{-1} \models \varphi.$$ [solution]

The isomorphism theorem implies that properties which are not invariant under automorphisms cannot be defined with a first-order logic formula or even axiomatised with a set of first-order logic formulas.

Problem 2.11.7. Are $(\mathbb{R}, +)$ and $(\mathbb{R}_+, *)$ isomorphic? [solution]

Problem 2.11.8. Consider the coloured graph $\mathfrak{A} = (\mathbb{Z} \times \mathbb{Z}, E, U)$, where the edge relation E is defined as

$$(x, y, x', y') \in E \text{ iff } (x = x' \text{ and } |y - y'| = 1) \text{ or } (|x - x'| = 1 \text{ and } y = y'),$$

and $U \subseteq \mathbb{Z} \times \mathbb{Z}$ is a unary relation. Is it possible to define in first-order logic that U is a union of complete columns? [solution]

Problem 2.11.9. Construct a set Δ of first-order sentences s.t. every two *countable* models thereof are isomorphic (i.e., Δ is $\aleph_0$-categorical), but there exist two uncountable nonisomorphic models of Δ of the same cardinality (i.e., Δ is not κ-categorical for some $\kappa > \aleph_0$). [solution]

2.11.3 Elementary equivalence

Definition 2.11.10. Fix a signature Σ and consider two structures $\mathfrak{A}, \mathfrak{B}$ over Σ. For $m \in \mathbb{N}$, we write $\mathfrak{A} \equiv_m \mathfrak{B}$ if $\mathfrak{A}$ and $\mathfrak{B}$ satisfy the same first-order sentences of rank $\leq m$. If this holds for every m, then we say that $\mathfrak{A}$ and $\mathfrak{B}$ are *elementarily equivalent*, written $\mathfrak{A} \equiv \mathfrak{B}$.

Problem 2.11.11. Show that isomorphic structures are elementarily equivalent: $\mathfrak{A} \cong \mathfrak{B}$ implies $\mathfrak{A} \equiv \mathfrak{B}$. [solution]

Problem 2.11.12. Is it the case that $(\mathbb{R}, +, *) \equiv (\mathbb{Q}, +, *)$? [solution]

2.12 Ehrenfeucht-Fraïssé games

Definition 2.12.1. Let $k \in \mathbb{N}$ be a parameter and consider two structures $\mathfrak{A}$ and $\mathfrak{B}$ over the same signature Σ. The *Ehrenfeucht-Fraïssé game* $G_k(\mathfrak{A}, \mathfrak{B})$ of length k is defined as follows. At every round $1 \leq i \leq k$, either

(1) Player I selects $a_i \in \mathfrak{A}$, (2) Player II selects $b_i \in \mathfrak{B}$,	or	(1) Player I selects $b_i \in \mathfrak{B}$, (2) Player II selects $a_i \in \mathfrak{A}$.

At the end of the game, the two players have produced two sets $X = \{a_1, \ldots, a_k\}$ and $Y = \{b_1, \ldots, b_k\}$, and Player II wins if $\mathfrak{A}|_X \cong_h \mathfrak{B}|_Y$ for the partial isomorphism $h(a_1) = b_1, \ldots, h(a_k) = b_k$.

Theorem 2.12.2 (Finite EF-games)**.** *Fix a signature Σ and two structures $\mathfrak{A}$ and $\mathfrak{B}$ over Σ. For every $k \in \mathbb{N}$,*

$$\text{Player II wins } G_k(\mathfrak{A}, \mathfrak{B}) \quad \text{if, and only if,} \quad \mathfrak{A} \equiv_k \mathfrak{B}.$$

2.12.1 Equivalent structures

Problem 2.12.3. Is it the case that

$$(\mathbb{Q}, <) \equiv (\mathbb{R}, <)?$$

Are the two structures above isomorphic? [solution]

Problem 2.12.4. Prove that the structures $(\mathbb{Q} \times \mathbb{Z}, \leq)$ and $(\mathbb{R} \times \mathbb{Z}, \leq)$, ordered lexicographically using the natural orders on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, are elementarily equivalent. [solution]

Problem 2.12.5. Consider a finite directed cycle $\mathfrak{A}_n$ of size 2^n (number of vertices) and a path infinite in both directions $\mathfrak{B}$. From a trivial counting argument, $\mathfrak{A}_n$ and $\mathfrak{B}$ can be distinguished by a sentence of rank $2^n + 1$ using only the equality symbol (c.f. Problem 2.1.6 "Cardinality constraints I"). However, if we additionally allow the edge relation "E" sentences of smaller rank suffice. What is the smallest k s.t. Player I wins $G_k(\mathfrak{A}_n, \mathfrak{B})$? [solution]

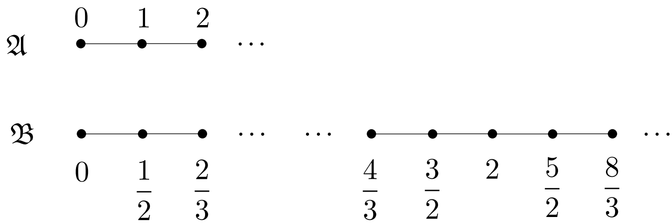


Figure for Problem 2.12.6.

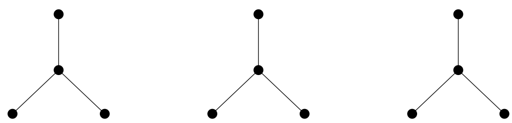


Figure for Problem 2.12.7.

Problem 2.12.6. Show that the following two structures cannot be distinguished by any sentence of first-order logic (c.f. problem figure):

$$\mathfrak{A} = (\mathbb{N}, \leq), \text{ and}$$
$$\mathfrak{B} = (\{1 - \tfrac{1}{n} \mid n > 0\} \cup \{1 + \tfrac{1}{n} \mid n > 0\} \cup \{3 - \tfrac{1}{n} \mid n > 0\}, \leq).$$ [solution]

Problem 2.12.7. Assume that Player II has a winning strategy in $G_4(\mathfrak{A}, \mathfrak{B})$, where $\mathfrak{A}$ is shown in the problem figure and $\mathfrak{B}$ is an unspecified undirected graph with n vertices. How many edges can $\mathfrak{B}$ have? [solution]

Problem 2.12.8. Consider the graph $\mathfrak{G}$ in the problem figure. Prove that

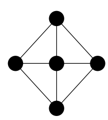


Figure for Problem 2.12.8.

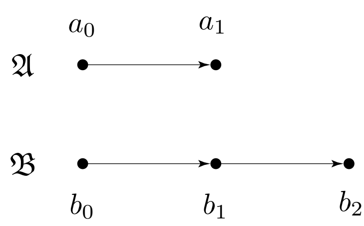


Figure for Problem 2.12.10 "Distinguishing chains".

any graph $\mathfrak{H}$ s.t. $\mathfrak{H} \equiv_3 \mathfrak{G}$ has an odd number of ≥ 3 vertices. [solution]

Problem 2.12.9. For a partial order $\mathfrak{A} = (A, \leq)$, let $\widetilde{\mathfrak{A}} = (\widetilde{A}, \widetilde{\leq})$ be obtained from $\mathfrak{A}$ by adding a new largest and smallest element $\widetilde{A} = A \cup \{\bot, \top\}$.

1. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two partial orders. Prove that

$$\mathfrak{A} \equiv_n \mathfrak{B} \quad \text{implies} \quad \widetilde{\mathfrak{A}} \equiv_n \widetilde{\mathfrak{B}}.$$

2. What about the converse implication? [solution]

2.12.2 Distinguishing sentences

Problem 2.12.10 (Distinguishing chains)**.** Let the signature consist of a single binary relation $\Sigma = \{E\}$, and let $\mathfrak{A}$ and $\mathfrak{B}$ be two directed paths of length 1, resp., 2 (c.f. problem figure). Show that Player I wins $G_k(\mathfrak{A}_1, \mathfrak{B}_1)$ with $k = 2$ and construct the distinguishing formula corresponding to her winning strategy. [solution]

Problem 2.12.11 (The hypercube)**.** Let $\mathfrak{H}_n = (\{0,1\}^n, E)$ be the hypercube graph, i.e., $E(x, y)$ holds iff $x, y \in \{0,1\}^n$ differ on exactly one position. Find two sentences of smallest quantifier rank distinguishing:

- $\mathfrak{H}_4$ and $\mathfrak{H}_3$;
- $\mathfrak{H}_3$ and $\mathfrak{H}_3^-$, where the latter graph is obtained by removing one edge from $\mathfrak{H}_3$. [solution]

2.12.3 Infinite EF-games

Let the infinite EF-game $G_\infty(\mathfrak{A}, \mathfrak{B})$ be played for a countable number of rounds. The following problem shows that countable EF-games capture isomorphism of countable structures.

Problem 2.12.12 (Countable EF-games)**.** Fix a signature Σ and two *countable* structures $\mathfrak{A}$ and $\mathfrak{B}$ over Σ.

$$\text{Player II wins } G_\infty(\mathfrak{A}, \mathfrak{B}) \quad \text{if, and only if,} \quad \mathfrak{A} \cong \mathfrak{B}.$$ [solution]

Problem 2.12.13. Construct two structures $\mathfrak{A}$ and $\mathfrak{B}$ s.t. Player II wins $G_m(\mathfrak{A}, \mathfrak{B})$ for every finite number of rounds $m \in \mathbb{N}$ but loses the infinite game $G_\infty(\mathfrak{A}, \mathfrak{B})$. [solution]

2.12.4 No equality

We are interested in constructing distinguishing formulas not using equality, as motivated by the following simple problem.

Problem 2.12.14. Find two structures $\mathfrak{A}, \mathfrak{B}$ which can be distinguished by a sentence using equality, but cannot be distinguished by any sentence not using equality. [solution]

Definition 2.12.15. Let $\mathfrak{A}, \mathfrak{B}$ be two relational structures over the common signature Σ. An $\mathfrak{A}, \mathfrak{B}$*-invariant* is a relation $\sim \subseteq A \times \mathcal{B}$ s.t. for every k-ary relation $R \in \Sigma$ and elements $a_1 \sim b_1, \dots, a_k \sim b_k$,

$$(a_1, \dots, a_k) \in R^{\mathfrak{A}} \quad \text{if, and only if,} \quad (b_1, \dots, b_k) \in R^{\mathfrak{B}}.$$

Definition 2.12.16. Consider the following modified Ehrenfeucht-Fraïssé game $H_k(\mathfrak{A}, \mathfrak{B})$: Assume that at the end of the play the two players have constructed two sequences $a_1, \dots, a_k \in A$ and $b_1, \dots, b_k \in B$ (possibly containing duplicate elements). Then Player II wins if $\sim = \{(a_1, b_1), \dots, (a_k, b_k)\}$ is a $\mathfrak{A}, \mathfrak{B}$-invariant.

Theorem 2.12.17. *Player I wins $H_k(\mathfrak{A}, \mathfrak{B})$ if, and only if, there exists a sentence of rank k not using equality distinguishing $\mathfrak{A}$ from $\mathfrak{B}$.*

The following exercise has been proposed by Szymon Toruńczyk.

Problem 2.12.18. Let $\mathfrak{A}, \mathfrak{B}$ be two relational structures over a common signature Σ. Propose a modification $\mathfrak{A}'$ of $\mathfrak{A}$ and $\mathfrak{B}'$ of $\mathfrak{B}$ s.t. Player I wins $H_k(\mathfrak{A}, \mathfrak{B})$ if, and only if, she wins $G_k(\mathfrak{A}', \mathfrak{B}')$. [solution]

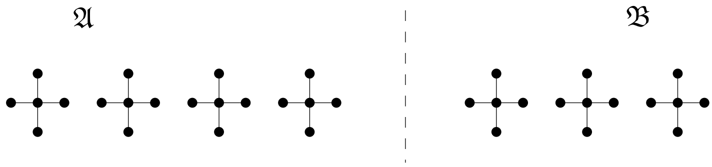


Figure for Problem 2.12.20.

2.12.5 One-sided EF-games

Definition 2.12.19. In the *one-sided Ehrenfeucht-Fraïssé game* of k rounds $G_k^{\mathsf{one}}(\mathfrak{A}_0, \mathfrak{A}_1)$, Player I, after selecting in the first round an element from $\mathfrak{A}_i$ with $i \in \{0, 1\}$, must select elements of the same $\mathfrak{A}_i$ in all the subsequent rounds.

Problem 2.12.20. Show that Player I wins the standard game $G_4(\mathfrak{A}, \mathfrak{B})$, with $\mathfrak{A}, \mathfrak{B}$ as in the problem figure. Is there a winning strategy for Player I in the one-sided variant $G_4^{\mathsf{one}}(\mathfrak{A}, \mathfrak{B})$? [solution]

Problem 2.12.21. Give an example of two structures $\mathfrak{A}_0, \mathfrak{A}_1$ s.t. Player II wins $G_k^{\mathsf{one}}(\mathfrak{A}_0, \mathfrak{A}_1)$ for every $k \in \mathbb{N}$, even though she loses the standard game $G_m(\mathfrak{A}_0, \mathfrak{A}_1)$ for some m. What is the smallest such m? [solution]

2.12.6 Inexpressibility: Non-definability and non-axiomatisability

Compactness is a standard tool to show non-axiomatisability of classes of arbitrary structures, as we have seen in Section 2.9.1. However, compactness fails over *finite* structures (c.f. Problem 2.9.3 "Compactness in finite structures?"). While *any* class of finite structures is axiomatisable (c.f. Problem 2.7.2 "Classes of finite structures are axiomatisable"), they need not be expressible by a single sentence of first-order logic. The following problem shows that EF-games can be used to show inexpressibility results over classes of finite (and infinite) structures.

Problem 2.12.22 (Non-definability via EF-games)**.** Show that, in order to prove that a class of structures $\mathcal{A}$ cannot be defined by a single sentence, it suffices to construct two sequences of structures $\mathfrak{A}_1, \mathfrak{A}_2, \dots \in \mathcal{A}$ and

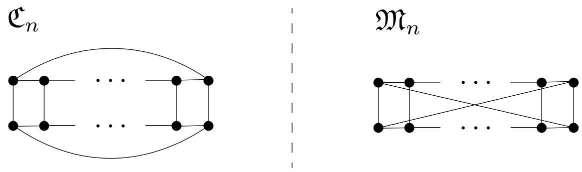


Figure for Problem 2.12.24 "Hanf".

$\mathfrak{B}_1, \mathfrak{B}_2, \cdots \notin \mathcal{A}$ s.t., for every $m \in \mathbb{N}$, $\mathfrak{A}_m \equiv_m \mathfrak{B}_m$. [solution]

Problem 2.12.23 (Eulerian cycles are not definable)**.** An *Eulerian cycle* in a simple graph is a cycle visiting every edge exactly once. Prove that the existence of an Eulerian cycle in *finite* simple graphs is not definable by a sentence of first-order logic. *Hint: Use Problem 2.12.22 "Non-definability via EF-games".* [solution]

Problem 2.12.24 (Hanf)**.** Consider the cylinder $\mathfrak{C}_n$ and the Möbius $\mathfrak{M}_n$ graph shown in the problem figure, both with $2 \cdot n$ vertices. Is there a single first-order sentence φ distinguishing $\mathfrak{C}_n$ from $\mathfrak{M}_n$ for every $n \in \mathbb{N}$? [solution]

Problem 2.12.25 (Non-axiomatisability via EF-games)**.** Show that, in order to prove non-axiomatisability by a set of sentences, it suffices to construct a sequence of structures $\mathfrak{A}_1, \mathfrak{A}_2, \cdots \in \mathcal{A}$ and a single structure $\mathfrak{B} \notin \mathcal{A}$ s.t., for every $m \in \mathbb{N}$, $\mathfrak{A}_m \equiv_m \mathfrak{B}$. [solution]

Problem 2.12.26 (Planarity is not axiomatisable)**.** A simple graph is *planar* if it can be drawn on the plane without crossing edges. Prove that the class of graphs in which each finite subgraph is planar is not axiomatisable. *Hint: Use Problem 2.12.25 "Non-axiomatisability via EF-games".* [solution]

Problem 2.12.27 (The Church-Rosser property is not axiomatisable (via EF-games))**.** We showed in Problem 2.9.14 "The Church-Rosser property is not axiomatisable (via compactness)" using compactness that the Church-Rosser property CR is not axiomatisable. Prove the same using EF games.

expressing $\mathcal{A}$		expressing $\mathcal{A}^c$
not one sentence	$\mathfrak{A}_m \equiv_m \mathfrak{B}_m$	not one sentence
not one sentence	$\mathfrak{A} \equiv_m \mathfrak{B}_m$	not a set of sentences
not a set of sentences	$\mathfrak{A}_m \equiv_m \mathfrak{B}$	not one sentence
not a set of sentences	$\mathfrak{A} \equiv_m \mathfrak{B}$	not a set of sentences

Figure 2.2: Summary of non-definability and non-axiomatisability via EF games.

[solution]

2.12.7 Complexity

Problem 2.12.28 (Solving EF-games in PSPACE)**.** Show that the following problem can be solved in PSPACE.

THE EF-GAME PROBLEM.
Input: Two structures $\mathfrak{A}$ and $\mathfrak{B}$ over a common vocabulary Σ and $k \in \mathbb{N}$.
Output: YES iff Player II wins $G_k(\mathfrak{A}, \mathfrak{B})$. [solution]

The complexity upper bound provided by the previous exercise is in fact optimal since solving EF-games is PSPACE-hard [25].

Problem 2.12.29 (Fixed-length EF-games)**.** Fix a number of rounds $k \in \mathbb{N}$. Show that the following problem can be solved in LOGSPACE:

FIXED-LENGTH EF-GAME.
Input: Two structures $\mathfrak{A}$ and $\mathfrak{B}$ over a common vocabulary Σ.
Output: YES iff Player II wins $G_k(\mathfrak{A}, \mathfrak{B})$. [solution]

2.12.8 Complete theories

Definition 2.12.30. A *theory* over signature Σ is any set of sentences Γ which is closed under logical entailment, in the sense that $\Gamma \models \varphi$ implies $\varphi \in \Gamma$. A set of sentences Γ is *complete* if, for every first-order formula φ over Σ, either $\Gamma \models \varphi$ or $\Gamma \models \neg\varphi$; if Γ is a theory, the latter condition is equivalent to: $\varphi \in \Gamma$ or $\neg\varphi \in \Gamma$. Given a set of formulas Γ over a given signature Σ, the set of *logical consequences* of Γ is the theory

$$\mathsf{Th}(\Gamma) = \{\varphi \mid \Gamma \vDash \varphi\}$$

The set of all valid first-order formulas of a given signature $\mathsf{Th}(\Sigma)$ is a complete theory (i.e., when $\Gamma = \varnothing$). The *theory of a structure* $\mathfrak{A}$ is the set of sentences that it satisfies, denoted by $\mathsf{Th}(\mathfrak{A}) = \{\varphi \mid \mathfrak{A} \vDash \varphi\}$, and it is thus a complete theory.

By Theorem 2.10.1 “Upward Skolem-Löwenheim theorem”, there is no hope for models of a theory Γ to be isomorphic to each other (by a trivial cardinality argument). The situation changes when we look at models of fixed cardinality.

Definition 2.12.31. A theory Γ is *κ-categorical* if any two models of cardinality κ thereof are isomorphic.

Problem 2.12.32 (Łoś-Vaught test)**.** Let κ be an infinite cardinality. Show that every set of sentences Γ over a signature Σ of cardinality $|\Sigma| \leq \kappa$, which has no finite models and is κ-categorical, must be complete. [solution]

Problem 2.12.33 (Theory completeness and decidability)**.** A theory Γ is *recursive* if it is decidable whether $\varphi \in \Gamma$ (membership), and *decidable* if it is decidable whether $\Gamma \vDash \varphi$ (logical consequence). Show that a complete recursive theory over a finite signature Σ is decidable. [solution]

Problem 2.12.34. How many complete theories over a finite signature can exist? Find a finite signature Σ s.t. there are continuum-many complete theories over Σ. [solution]

2.13 Interpolation

Definition 2.13.1. An *preinterpolant* of two first-order formulas φ, ψ satisfying $\vDash \varphi \to \psi$ is a formula ξ s.t. $\vDash \varphi \to \xi$ and $\vDash \xi \to \psi$, $\mathsf{fv}(\xi) = \mathsf{fv}(\varphi) \cap \mathsf{fv}(\psi)$, and ξ contains only relation symbols occurring in both φ and ψ, and an *interpolant* satisfies the further property that it contains only function symbols occurring in both φ and ψ.

The purpose of this section is to show the existence of interpolants for first-order logic.

2.13.1 No equality

In this section we show how to construct interpolants for formulas not using the equality symbol "=".

Problem 2.13.2 (Interpolation for quantifier-free ground formulas)**.** Assume that $\vDash \varphi \to \psi$, where φ, ψ are quantifier-free, ground, and do not contain the equality symbol "=". Construct a quantifier-free ground formula ξ interpolating φ, ψ. [solution]

Problem 2.13.3 (Preinterpolation for $\forall/\exists$ sentences)**.** Assume

$$\vDash (\forall \bar{x} \,.\, \varphi) \to \exists \bar{y} \,.\, \psi,$$

with φ, ψ quantifier-free, not containing the equality symbol "=". Show how to construct a quantifier-free ground preinterpolant ξ for the two sentences above. *Hint: Use Problem 2.5.4 and Problem 2.13.2 "Interpolation for quantifier-free ground formulas".* [solution]

Problem 2.13.4 (Interpolation for $\forall/\exists$ sentences)**.** Show how to transform a quantifier-free ground preinterpolant ξ,

$$\vDash \forall \bar{x} \,.\, \varphi \to \xi \quad \text{and} \quad \vDash \xi \to \exists \bar{y} \,.\, \psi,$$

into a ground interpolant (i.e., a sentence). [solution]

Problem 2.13.5 (Interpolation for sentences)**.** Let $\vDash \varphi \to \psi$, where φ, ψ are two sentences not containing the equality symbol. Show that there exists a sentence ξ interpolating φ, ψ. *Hint: Use Problem 2.4.3 "Herbrandisation" and Problem 2.13.4 "Interpolation for $\forall/\exists$ sentences".* [solution]

Problem 2.13.6 (Interpolation for formulas without equality)**.** Let $\vDash \varphi \to \psi$, where φ, ψ are two formulas (possibly containing free variables) not containing the equality symbol. Show that there exists a formula interpolating φ, ψ. *Hint: Use Problem 2.13.5 "Interpolation for sentences".* [solution]

2.13.2 Extensions

Problem 2.13.7 (Interpolation with equality)**.** Let $\vDash \varphi \to \psi$, where φ, ψ are two formulas possibly containing the equality relation. Show that there exists an interpolant thereof. *Hint: Use Problem 2.13.6 "Interpolation for formulas without equality".* [solution]

Problem 2.13.8. Let Γ be a set of formulas and ψ a formula of first-order logic and s.t. $\Gamma \vDash \psi$. Show that there exists a formula ξ over the common signature and common free variables of $\Gamma \cup \{\psi\}$ s.t. $\Gamma \vDash \xi$ and $\xi \vDash \psi$. *Hint: Apply Problem 2.9.1 "Compactess theorem" and Problem 2.13.7 "Interpolation with equality".* [solution]

Problem 2.13.9 (No interpolation for finite structures)**.** Prove that the interpolation theorem fails for first-order logic over finite structures: Construct two sentences φ, ψ s.t.

- $\varphi \to \psi$ holds in all finite structures, and
- there is no ξ containing only relation and/or function symbols occurring in both φ and ψ s.t. $\varphi \to \xi$ and $\xi \to \psi$ holds in all finite structures.

Hint: Use Problem 2.8.18 "Spectra with only unary relations". [solution]

2.13.3 Applications of interpolation

Problem 2.13.10 (Separability of universal formulas)**.** If two universal formulas φ, ψ over a relational signature without equality are jointly unsatisfiable $\vDash \varphi \wedge \psi \to \bot$, then they can be separated by a quantifier-free formula ξ: $\vDash \varphi \to \xi$ and $\vDash \xi \wedge \psi \to \bot$. [solution]

Theorem 2.13.11 (Lyndon's interpolation theorem)**.** *If $\vDash \varphi \to \psi$, then there exists an interpolant ξ of φ, ψ s.t. every relation used in ξ positively is also used positively in φ, ψ, and similarly for negative uses.*

A *homomorphism* is a total functional logical relation.

Problem 2.13.12 (Lyndon's theorem)**.** Show that a formula of first-order logic is preserved under surjective homomorphisms if, and only if, it is equivalent to a positive formula. *Hint: Express preservation under surjective homomorphisms as a first-order formula and apply Theorem 2.13.11 "Lyndon's interpolation theorem".* [solution]

Problem 2.13.13 (Łoś-Tarski's theorem)**.** Show that a sentence is preserved under induced substructures if, and only if, it is equivalent to a universal sentence.[3] [solution]

Problem 2.13.14 (Robinson's joint consistency theorem)**.** Show that, if Γ, Δ are satisfiable sets of sentences but $\Gamma \cup \Delta$ is not satisfiable, then there exists a sentence ξ over the shared variables and vocabulary s.t. $\Gamma \vDash \xi$ and $\Delta \vDash \neg\xi$. *Hint: Apply Problem 2.9.1 "Compactess theorem" and Problem 2.13.7 "Interpolation with equality".* [solution]

[3]Preservation under induced substructures on all finite models has been conjectured in 1958 by Scott and Suppes [27]. Tait showed that Łoś-Tarski's theorem does not hold on finite structures [31].

2.14 Relational algebra

In this section we investigate the connection between first-order logic and relational algebra, which is a formalism without variables. Let $\Sigma = \{R_1, R_2, \dots\}$ be a relational signature, where R_i has arity k_i. Let $A = \{a_1, a_2, \dots\}$ be the domain. Expressions of *relational algebra* are generated by the following abstract syntax:

$$E, F ::= (a_1, \dots, a_k) \mid R_i \mid E + F \mid E - F \mid E \times F \mid \sigma_{i=j}(E) \mid \pi_{i_1,\dots,i_k}(E)$$

The *dimension* of an expression of relational algebra E is defined inductively as follows:

- $(a_1, \dots, a_k)$ has dimension k;
- R_i has dimension k_i;
- if E, F have the same dimension k, then also $E + F$, $E - F$, and $\sigma_{i=j}(E)$ (when $i, j \in \{1, \dots, k\}$) have dimension k.
- if E has dimension k and F has dimension l, then $E \times F$ has dimension $k + l$;
- if E has dimension k then $\pi_{i_1,\dots,i_l}(E)$ has dimension l whenever $1 \le i_j \le k$ for every $1 \le j \le l$.

An expression is *well-formed* if it has a dimension (which is unique in this case). In the following, we assume that expressions are well-formed. The semantics $[\![E]\!]_{\mathfrak{A}}$ of relational algebra expression E in a relational structure $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, R_2^{\mathfrak{A}}, \dots)$ is:

$$\begin{aligned}
[\![(a_1, \dots, a_k)]\!]_{\mathfrak{A}} &= \{(a_1, \dots, a_k)\}, \\
[\![R_i]\!]_{\mathfrak{A}} &= R_i^{\mathfrak{A}} \\
[\![E + F]\!]_{\mathfrak{A}} &= [\![E]\!]_{\mathfrak{A}} \cup [\![F]\!]_{\mathfrak{A}}, \\
[\![E - F]\!]_{\mathfrak{A}} &= [\![E]\!]_{\mathfrak{A}} \setminus [\![F]\!]_{\mathfrak{A}}, \\
[\![E \times F]\!]_{\mathfrak{A}} &= [\![E]\!]_{\mathfrak{A}} \times [\![F]\!]_{\mathfrak{A}}, \\
[\![\sigma_{i=j}(E)]\!]_{\mathfrak{A}} &= \{(a_1, \dots, a_k) \in [\![E]\!]_{\mathfrak{A}} \mid a_i = a_j\}, \\
[\![\pi_{i_1,\dots,i_k}(E)]\!]_{\mathfrak{A}} &= \{(a_{i_1}, \dots, a_{i_k}) \mid (a_1, \dots, a_k) \in [\![E]\!]_{\mathfrak{A}}\}.
\end{aligned}$$

Problem 2.14.1. Show how to express intersection $E \& F$ in terms of the primitives above. [solution]

Since the semantics of relational algebra is given in a first-order language, it is not surprising that one can transform an expression into an equivalent first-order logic formula.

Problem 2.14.2. Show that given any relational algebra expression E of dimension k one can write an equivalent formula of first-order logic $\varphi_E(x_1, \dots, x_k)$ with k free variables. *Hint: Proceed by structural induction on expressions.* [solution]

What is perhaps more surprising is that in fact *every* formula of first-order logic on a relational signature arise in this way (up to logical equivalence).

Problem 2.14.3. Show that given a formula of first-order logic with equality $\varphi(x_1, \dots, x_k)$ with k free variables and any dimension $n \geq k$, one can write an equivalent expression of relational algebra $E_{\varphi,n}$ of dimension n. *Hint: Proceed by structural induction preserving the invariant*

$$[\![E_{\varphi,n}]\!] = \{\bar{a} \in A^n \mid \mathfrak{A}, \bar{x} : \bar{a} \vDash \varphi\}.$$ [solution]

Note. The two translations in Problems 2.14.2 and 2.14.3 prove the equivalence of first-order logic with equality on relational structures and relational algebra, which is a seminal result due to Codd [7].

2.15 Hilbert's proof system

Fix a signature Σ. We consider a Hilbert-style deduction system for the minimal and functionally complete set of connectives $\{\forall, \to, \bot\}$. This is an extension of Hilbert's proof system for propositional logic (A1)–(A3) (which we repeat below) in order to model the universal quantifier "$\forall$" and the interpretation of equality.

$$\varphi \to \psi \to \varphi, \tag{A1}$$
$$(\varphi \to \psi \to \theta) \to (\varphi \to \psi) \to \varphi \to \theta, \tag{A2}$$
$$\neg\neg\varphi \to \varphi, \tag{A3}$$

$$(\forall x \,.\, \varphi \to \psi) \to (\forall x \,.\, \varphi) \to \forall x \,.\, \psi, \tag{A4}$$
$$\varphi \to \forall x \,.\, \varphi, \qquad (\text{if } x \notin \mathsf{fv}(\varphi)) \tag{A5}$$
$$(\forall x \,.\, \varphi) \to \varphi[x \mapsto t], \qquad (\text{if } (*)) \tag{A6}$$

$$x = x, \tag{A7}$$
$$x_1 = y_1 \to \cdots \to x_n = y_n \to f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n), \tag{A8}$$
$$x_1 = y_1 \to \cdots \to x_n = y_n \to R(x_1, \ldots, x_n) \to R(y_1, \ldots, y_n), \tag{A9}$$

$$\frac{\varphi \to \psi \quad \varphi}{\psi}. \tag{MP}$$

The additional condition (*) in (A6) requires that the term t is *admissible* for x in φ in the sense that no free variable of t becomes bound after the substitution. In axiom (A8), f ranges over all n-ary function symbols in Σ, and similarly in (A9), R ranges over all n-ary relations symbols in Σ. (Thus, we obtain a different system of axioms for every Σ.) The notion of provability $\Delta \vdash \varphi$ is defined in the same way as in the case of propositional logic; c.f. Section 1.8. We say that a set of formulas Δ is *consistent* if it is not possible to derive a contradiction: $\Delta \nvdash \bot$. (Compare this proof-theoretic notion with the model-theoretic notion of *satisfiability* $\Delta \not\models \bot$, i.e., Δ has a model.)

Problem 2.15.1. As an example, we can prove the following familiar properties of equality.

$$\vdash x = y \to y = x, \tag{2.7}$$
$$\vdash x = y \wedge y = z \to x = z. \tag{2.8}$$

[solution]

The next problem demonstrates that provability preserves logical consequence.

Problem 2.15.2 (Soundness)**.** Let $\Delta \cup \{\varphi\}$ be a set of first-order formulas. Then,

$$\Delta \vdash \varphi \quad \text{implies} \quad \Delta \vDash \varphi.$$

Hint: Proceed by complete induction on the length of proofs. [solution]

Problem 2.15.3 (Deduction theorem)**.** Show that for Hilbert's proof system for first-order logic,

$$\Delta \vdash \varphi \to \psi \quad \text{if, and only if,} \quad \Delta \cup \{\varphi\} \vdash \psi.$$ [solution]

In the same way as Problem 2.15.3 "Deduction theorem" simplifies the use of "$\to$" and (MP) in formal proofs, the following problem provides a tool to simplify the use of "$\forall$".

Problem 2.15.4 (Generalisation theorem)**.** Let $x \notin \mathsf{fv}(\Delta)$ be a variable not occurring free in any formula of Δ. Then,

$$\Delta \vdash \forall x \,.\, \varphi \quad \text{if, and only if,} \quad \Delta \vdash \varphi.$$ [solution]

Hint: Use (A4)*,* (A5)*,* (A6)*, and* (MP)*.*

Problem 2.15.5 (Renaming)**.** Consider a formula φ and two variables x, y s.t. $y \notin \mathsf{fv}(\Delta \cup \{\varphi\})$ and y is free for x in φ. Then,

$$\Delta \vdash \forall x \,.\, \varphi \quad \text{implies} \quad \Delta \vdash \forall y \,.\, \varphi[x \mapsto y].$$ [solution]

Hint: Use (A4)*,* (A5)*,* (A6)*, and* (MP)*.*

2.15.1 Completeness

Problem 2.15.6. Show that the two formulations of completeness below are equivalent.

1. For every set of formulas $\Delta \cup \{\varphi\}$, $\Delta \vDash \varphi$ implies $\Delta \vdash \varphi$.
2. For every set of formulas Γ, if Γ is consistent, then it is satisfiable (i.e., it has a model). [solution]

Thanks to Problem 2.15.6, in order to prove completeness it suffices to build a model for a consistent set of sentences Γ.

In general, a structure $\mathfrak{A}$ has the following two essential semantical properties:

1. Has witnesses: The structure $\mathfrak{A}$ has sufficiently many witnesses in the sense that whenever $\mathfrak{A} \nvDash \forall x\,.\,\varphi$ for a formula φ with a single free variable x (which is the same as saying $\mathfrak{A} \vDash \exists x\,.\,\neg\varphi$), then there exists an element $a \in A$ in the domain s.t. $\mathfrak{A}, x : a \vDash \neg\varphi$.
2. Dichotomy: For every sentence φ, either $\mathfrak{A} \vDash \varphi$ or $\mathfrak{A} \vDash \neg\varphi$.

We would like to replicate the properties above in terms of Γ and provability "$\vdash$".

We first address the issue with witnesses. Fix a signature Σ. We say that a consistent set of formulas $\Gamma \subseteq \mathsf{Th}(\Sigma)$ with signature Σ is *saturated* if, for every formula $\varphi \in \mathsf{Th}(\Sigma)$ of one free variable x ($\mathsf{fv}(\varphi) = \{x\}$) over the same signature,

$$\Gamma \nvdash \forall x\,.\,\varphi \quad \text{implies} \quad \Gamma \vdash \neg\varphi[x \mapsto c] \text{ for some constant } c \in \Sigma.$$

Intuitively, this means that if Γ cannot prove an universal sentence, then it can refute it and there is a concrete witness c in the signature achieving this.

Problem 2.15.7 (Saturation)**.** Any consistent set of sentences Δ extends to a consistent and saturated set of sentences $\Gamma \supseteq \Delta$ (over a larger signature). [solution]

Let Γ be a saturated set of sentences over signature Σ. We define the following relation on the constant symbols in Σ:

$$c \sim_\Gamma d \quad \text{if, and only if,} \quad \Gamma \vdash c = d.$$

Intuitively, $c \sim_\Gamma d$ means that they are provably equal from the axioms in Γ.

Problem 2.15.8 (Congruence)**.** Prove the following two crucial properties of $\sim_\Gamma$.

1. The relation $\sim_\Gamma$ is an equivalence: For every constants $c, d, e \in \Sigma$,

$$\begin{array}{lll} c \sim_\Gamma c, & & \\ c \sim_\Gamma d & \text{implies} & d \sim_\Gamma c, \\ c \sim_\Gamma d \text{ and } d \sim_\Gamma e & \text{implies} & c \sim_\Gamma e. \end{array}$$

2. The relation $\sim_\Gamma$ is a congruence w.r.t. the function symbols in Σ: For every n-ary function symbol $f : n \in \Sigma$ and constants $c_1, d_1, \ldots, c_n, d_n \in \Sigma$,

$$c_1 \sim_\Gamma d_1, \cdots, c_n \sim_\Gamma d_n \text{ implies } f(c_1, \ldots, c_n) \sim_\Gamma f(d_1, \ldots, d_n).$$

[solution]

We are now ready to build a syntactic model. Let $\Sigma_0 \subseteq \Sigma$ be the set of constant symbols in Σ. Consider the structure $\mathfrak{A}_\Gamma = (A, \Sigma)$ over signature Σ, where the domain is the set of equivalence classes $A = \Sigma_0 / \sim_\Gamma$ of constants w.r.t. the congruence $\sim_\Gamma$, each constant $c \in \Sigma_0$ is interpreted as its equivalence class

$$c^{\mathfrak{A}_\Gamma} = [c]_{\sim_\Gamma},$$

each n-ary functional symbol $f \in \Sigma$ is interpreted as the relation $\subseteq A^n \times A$ defined as:

$$f^{\mathfrak{A}_\Gamma}([c_1]_{\sim_\Gamma}, \ldots, [c_n]_{\sim_\Gamma}) = [d]_{\sim_\Gamma} \quad \text{if, and only if,} \quad f(c_1, \ldots, c_n) \sim_\Gamma d,$$

and every n-ary relational symbol $R \in \Sigma$ is interpreted as the n-ary relation $\subseteq A^n$ defined as

$$([c_1]_{\sim_\Gamma}, \ldots, [c_n]_{\sim_\Gamma}) \in R^{\mathfrak{A}_\Gamma} \quad \text{if, and only if,} \quad \Gamma \vdash R(c_1, \ldots, c_n).$$

Thanks to the fact that $\sim_\Gamma$ is a congruence, the definition of $f^{\mathfrak{A}_\Gamma}$ does not depend on the choice of representatives and denotes indeed a partial function $A^n \to A$.

Problem 2.15.9 (Functionality)**.** Show that the interpretation of $f^{\mathfrak{A}_\Gamma}$ above does indeed define a total function $A^n \to A$: For every $c_1, \ldots, c_n$, there is d s.t. $f(c_1, \ldots, c_n) \sim_\Gamma d$. *Hint: Use the fact that Γ is saturated.* [solution]

Problem 2.15.10 (Terms)**.** Show that for every term t over Σ with free variables $\mathsf{fv}(t) = \{x_1, \ldots, x_n\}$, valuation $\varrho : X \to A$ with $\varrho(x_1) = [c_1]_{\sim_\Gamma}, \ldots, \varrho(x_n) = [c_n]_{\sim_\Gamma}$, and constant d,

$$[\![t]\!]_\varrho = [d]_{\sim_\Gamma} \quad \text{if, and only if,} \quad t[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] \sim_\Gamma d.$$

Hint: Use structural induction on terms. [solution]

Problem 2.15.11 (Relations)**.** Show that the interpretation of $R^{\mathfrak{A}_\Gamma}$ is well-defined, in the sense that does not depend on the chosen representatives. *Hint: Use* (A9)*.* [solution]

Problem 2.15.12 (Implication)**.** Let $\psi^* \equiv \psi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$ and $\xi^* \equiv \xi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$. Show that

$$\Gamma \vdash \psi^* \to \xi^* \quad \text{if, and only if,} \quad \Gamma \vdash \psi^* \text{ implies } \Gamma \vdash \xi^*$$

Hint: [solution]

Problem 2.15.13 (Universal quantification)**.** Let $\psi^* \equiv \psi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$ Show that

$$\Gamma \vdash \forall x_0 \,.\, \psi^* \quad \text{if, and only if,} \quad \text{for all } [c_0]_{\sim_\Gamma} \in A, \Gamma \vdash \psi^*[x_0 \mapsto c_0].$$

Hint: Use the fact that Γ is saturated and (A6)*.* [solution]

Problem 2.15.14 (Formulas)**.** Show that for every first-order formula φ over Σ with free variables $\mathsf{fv}(\varphi) = \{x_1, \ldots, x_n\}$, and valuation $\varrho : X \to A$ with $\varrho(x_1) = [c_1]_{\sim_\Gamma}, \ldots, \varrho(x_n) = [c_n]_{\sim_\Gamma}$,

$$\mathfrak{A}_\Gamma, \varrho \vDash \varphi \quad \text{if, and only if,} \quad \Gamma \vdash \varphi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n].$$

Hint: Use structural induction on formulas. [solution]

Problem 2.15.15 (Sentences)**.** Show that for every first-order sentence φ over Σ

$$\mathfrak{A}_\Gamma \vDash \varphi \quad \text{if, and only if,} \quad \Gamma \vdash \varphi.$$

In particular, $\mathfrak{A}_\Gamma \vDash \Gamma$. *Hint: Use Problem 2.15.14 "Formulas".* [solution]

Problem 2.15.16 (Strong completeness theorem)**.** Let φ be a formula and let Δ be a set of formulas (possibly infinite). Then,

$$\Delta \vDash \varphi \quad \text{implies} \quad \Delta \vdash \varphi.$$

[solution]

Chapter 3

Second-order predicate logic

Second-order logic is an extension of first-order logic with variables R denoting relations which can be quantified over:

$$\varphi, \psi \ ::\equiv \ \top \mid R(t_1, \ldots, t_{k_j}) \mid t_1 = t_2 \mid \varphi \wedge \psi \mid \neg\varphi \mid \exists x \,.\, \varphi \mid \exists R \,.\, \varphi.$$

A formula of second-order logic is *existential* if it is of the form $\exists R_1, \ldots, R_n \,.\, \varphi$, with φ first-order, and similarly for *universal* formulas, and it is *monadic* if all second-order quantifiers range over unary (monadic) predicates.

3.1 Expressiveness

Problem 3.1.1 (Finiteness)**.** Write a sentence of universal second-order logic which is satisfied precisely in finite models. Can this be done in $\forall\mathsf{MSO}$? [solution]

Problem 3.1.2 (Countability)**.** Write a sentence of second-order logic which is satisfied precisely in countable models.

[solution]

Problem 3.1.3 (Spectrum)**.** Show that spectra of second-order logic are closed under complement. (The analogous statement for first-order spectra is a long-standing open problem.) [solution]

Problem 3.1.4. Construct a sentence of MSO whose spectrum is the set of prime numbers. [solution]

3.1.1 Directed graphs

Problem 3.1.5 (Reachability for directed graphs)**.** Consider a directed graph (V, E) with edge relation $E \subseteq V \times V$. Write a universal formula of second-order logic expressing the reflexive-transitive closure E^* of E. Is it possible to express it with a monadic formula? And with an existential one (possibly non-monadic)? [solution]

Problem 3.1.6 (Connectivity for directed graphs)**.** A finite directed graph (V, E) is *strongly connected* if every two vertices are connected by a directed path. Show how to express strong connectivity in $\forall\mathsf{MSO}$ and $\exists\mathsf{SO}$.

[solution]

The situation on whether reachability and connectivity are expressible in SO and its variants on directed graphs is summarised in Figure 3.1.

Problem 3.1.7 (Eulerian cycles in $\exists\mathsf{SO}$)**.** Express the existence of a Eulerian cycle (c.f. Problem 2.12.23 "Eulerian cycles are not definable") in $\exists\mathsf{SO}$. Is it possible to write a universal sentence as well? [solution]

Problem 3.1.8 (Hamiltonian cycles in $\exists\mathsf{SO}$)**.** A *Hamiltonian cycle* in a finite directed graph is a path that visits each node exactly once.

directed graphs	reachability	connectivity
∀MSO	✓ (3.1.5)	✓ (3.1.6)
∃SO	✓ (3.1.5)	✓ (3.1.6)
∃MSO	no	no [14]

Figure 3.1: Expressing reachability/connectivity in directed graphs.

1. Show that the existence of a Hamiltonian cycle in finite directed graphs can be expressed in ∃SO.
2. Show that the existence of an analogous formula in ∀SO would imply NPTIME = coNPTIME. [solution]

Problem 3.1.9. Show that ∃MSO can already define some NPTIME-complete problem. *Hint: Express* 3*-colourability in* ∃*MSO.* [solution]

Problem 3.1.10 (The Church-Rosser property is MSO definable)**.** We have seen in Problem 2.9.14 "The Church-Rosser property is not axiomatisable (via compactness)" that the Church-Rosser property is not axiomatisable in first-order logic. Show that it can be defined in ∀MSO. [solution]

Problem 3.1.11 (Strong normalisation is MSO definable)**.** We have seen in Problem 2.9.15 "Strong normalisation is not axiomatisable (via compactness)" that strong normalisation of a binary relation $E \subseteq A \times A$ (i.e., well-foundedness of $(E^*)^{-1}$) is not axiomatisable in first-order logic. Show that it is definable in ∀MSO. [solution]

3.1.2 Simple graphs

(*) Problem 3.1.12 (Reachability for simple graphs)**.** Consider simple (i.e., undirected, without self-loops) finite graphs (V, E). Find an ∃MSO formula expressing the transitive closure E^*. Is this possible for directed graphs? [solution]

Problem 3.1.13 (Connectivity for simple graphs)**.** Write a sentence φ_{conn} of MSO expressing that a simple graph is connected. Is it possible to express it in ∃MSO? [solution]

simple graphs	reachability	connectivity
∀MSO	✓	✓
∃SO	✓	✓ (3.1.13)
∃MSO	✓ (!, 3.1.12)	no (3.1.13)

Figure 3.2: Expressing reachability/connectivity in simple graphs.

The situation on whether reachability and connectivity are expressible in SO and its variants on simple graphs is summarised in Figure 3.2.

Problem 3.1.14 (Graph minors in MSO)**.** A graph G is a *minor* of a graph H if it can be obtained from the latter by contracting edges and removing edges and nodes. Let G be a fixed finite simple graph. Write a closed MSO formula φ_G s.t., for every simple graph H, $H \vDash \varphi_G$ holds if, and only if, H contains G as a minor. [solution]

Problem 3.1.15 (Planarity of finite simple graphs in MSO)**.** Express planarity of finite simple graphs (c.f. Problem 2.12.26 "Planarity is not axiomatisable") in MSO. [solution]

3.1.3 MSO on trees

Problem 3.1.16. Consider the tree structure $\mathfrak{T} = (T, L, R, U)$, where the domain is the set of nodes $T = \{0,1\}^*$, L, R are binary relations encoding the left, resp., right child ($L(w, w0)$ and $R(w, w1)$ hold for every $w \in T$), and $U \subseteq T$ is an unspecified set of nodes. Express in MSO the existence of a path in T containing infinitely many elements of U. [solution]

3.1.4 MSO on free monoids

Problem 3.1.17. Consider the free monoid of words over $\{a, b\}$

$$\mathfrak{A} = (\{a, b\}^*, \cdot, a, b, \varepsilon)$$

with additional constants a, b for one-letter words.

1. Prove that for every regular language $L \subseteq \{a, b\}^*$ there is a MSO formula $\varphi(x)$ with one free first-order variable *defining* L in the sense

that

$$L = \{w \in \{a,b\}^* \mid \mathfrak{A}, x : w \models \varphi\}.$$

2. Find a formula of first-order logic with one free variable defining a non-regular language over $\Sigma = \{a, b\}$. [solution]

Problem 3.1.18. Show that every context-free language is MSO definable over the free monoid (in the sense of Problem 3.1.17). [solution]

3.2 Failures

The theme of this section is that many properties of first-order logic fail for second-order logic, and this happens already for its universal fragment. On the other hand, the existential fragment behaves much like first-order logic.

Problem 3.2.1 (Compactness fails for $\forall\mathsf{SO}$)**.** Show that the compactness theorem fails for the universal fragment of second-order logic. What about its existential fragment? [solution]

Problem 3.2.2 (Skolem-Löwenheim and SO)**.** Consider the following problems relating the Skolem-Löwenheim theorem and second-order logic.

1. Prove that the Skolem-Löwenheim theorem does not hold for second-order logic.

2. Show that the Skolem-Löwenheim theorem does not hold for existential second-order logic.

3. Show that the Skolem-Löwenheim theorem does hold for universal second-order logic over the empty signature.

4. What happens in the case of universal second-order logic when the signature is not empty? *Hint: A non-empty signature provides additional prenex existential second-order quantifiers.* [solution]

3.3 Word models

Let $\Sigma = \{a_1, \dots, a_n\}$ be a finite alphabet.

Definition 3.3.1. Every finite nonempty word $w = w_0 \cdots w_{k-1} \in \Sigma^+$ induces a relational structure $\mathfrak{A}_w$, called (finite) *word model*,

$$\mathfrak{A}_w = (\{0, \dots, k-1\}, \leq, P_{a_1}, \dots, P_{a_n}),$$

where the domain is the set of the natural numbers indexing the positions in w, the total order on positions $\leq$ is as on $\mathbb{N}$, and we have n unary predicates $P_{a_1}, \dots, P_{a_n}$ s.t. $P_{a_i}(x)$ holds iff $w_x = a_i$. We can associate to an MSO sentence φ over the signature $\{\leq, P_{a_1}, \dots, P_{a_n}\}$ the set of finite word models it satisfies $[\![\varphi]\!] = \{w \in \Sigma^+ \mid \mathfrak{A}_w \models \varphi\}$. A language of finite nonempty words $L \subseteq \Sigma^+$ is *MSO-definable* if there exists an MSO formula φ s.t. $L = [\![\varphi]\!]$.

Another way to describe languages, perhaps more familiar, is provided by automata.

Definition 3.3.2. A *finite nondeterministic automaton* (NFA) over Σ is a tuple $A = (Q, I, F, \{\xrightarrow{a} \subseteq Q \times Q \mid a \in \Sigma\})$ where Q is a finite set of *states*, $I, F \subseteq Q$ are those states which are *initial*, resp., *final*, and $\rightarrow$ is a labelled transition relation on states. We extend $\rightarrow$ on finite words Σ^* inductively, by writing $q \xrightarrow{\varepsilon} q$ for every $q \in Q$, and $q \xrightarrow{w \cdot a} q'$ whenever there exists $q'' \in Q$ s.t. $q \xrightarrow{w} q'' \xrightarrow{a} q'$. The language *recognised* by a state $q \in Q$ is $[\![q]\!] = \{w \in \Sigma^* \mid \exists q' \in F \,.\, q \xrightarrow{w} q'\}$, and $[\![Q]\!] = \bigcup_{q \in I} [\![q]\!]$. A language is *finite-state* if it can be recognised by a finite NFA.

We will prove the following celebrated result connecting automata theory with logic (c.f. Problems 3.3.3 and 3.3.8)

Theorem (Büchi [5], Elgot [11], and Trakhtenbrot [32])**.** *MSO-definable and finite-state languages coincide.*

We begin with the easier direction of the theorem.

Problem 3.3.3. Show that, for every NFA A one can effectively find an MSO sentence φ s.t. $L(A) = [\![\varphi]\!]$. [solution]

Problem 3.3.4. Show that one can improve Problem 3.3.3 and produce an $\exists$MSO sentence with a *single* second-order quantifier. [solution]

Problem 3.3.5 (Star-free regular languages in first-order logic)**.** Let Σ be a finite alphabet. A *star-free regular expression* over Σ is generated by the following grammar:

$$e, f ::= a \mid \Sigma^* \mid e \cup f \mid e \cdot f \mid \Sigma \setminus e,$$

where $a \in \Sigma$ and $\Sigma \setminus (\_)$ denotes the complementation operation. Show that star-free regular languages are definable in first-order logic over word models. *Hint: Construct the formula inductively over the structure of the expression. For this to go through, use formulas $\varphi_e(x, y)$ of two free variables x, y defining the language of words:*

$$[\![\varphi(x,y)]\!] = \{a_i \cdots a_{j-1} \in \Sigma^* \mid \mathcal{A}_{a_1 \ldots a_n}, x : i, y : j \models \varphi(x,y)\}.$$ [solution]

Problem 3.3.6. Show how to simulate first-order variables with MSO variables over word-models modulo the introduction of few new atomic formulas. *Hint: Interpret a first-order variable x as a second-order one representing the singleton $\{x\}$.* [solution]

In order to prove the more challenging direction of the theorem, we need to define the semantics in terms of word-models not just for MSO sentences, but for MSO formulas (i.e., potentially with free variables). Since first-order variables can be simulated by second-order ones, we only consider second-order variables.

Definition 3.3.7. Let $\varphi(X_1, \ldots, X_k)$ be an MSO formula with k free variables $X_1, \ldots, X_k$. We extend the alphabet to $\Sigma_k = \Sigma \times \{0,1\}^k$ in such a way that a letter $(a, b_1, \ldots, b_k) \in \Sigma_k$ in the new alphabet encodes an additional bit-vector $b_1 \cdots b_k$ s.t. $b_i = 1$ at position x iff $X_i(x)$ holds.

Problem 3.3.8. Show that every MSO formula $\varphi(X_1, \ldots, X_k)$ with k free MSO variables $X_1, \ldots, X_k$ can be converted to an NFA A over Σ_k s.t. $[\![\varphi(X_1, \ldots, X_k)]\!] = [\![A]\!]$. *Hint: Proceed by structural induction on φ.* [solution]

From Problem 3.3.3 we can see that one can convert an NFA into an equivalent MSO formula of size linear in the size of the automaton. The next problem can be used to estimate the complexity of the converse translation provided by Problem 3.3.8.

Problem 3.3.9 (c.f. [22, 29]). Fix an alphabet Σ. Construct an infinite sequence of satisfiable MSO formulas $\varphi_1, \varphi_2, \ldots$ s.t., for every n, φ_n has size linear in n and the smallest word-model of φ_n has size

$$\geq 2^{\left.2^{2^{\cdot^{\cdot^{2^n}}}}\right\}n}.$$
[solution]

Problem 3.3.10. Is the language of palindromes over $\Sigma = \{0, 1\}$ definable in MSO over word-models in the signature $\{\leq, P_0, P_1\}$, where P_0, P_1 are unary predicates encoding the labelling? [solution]

Problem 3.3.11. Consider the alphabet $\Sigma = \{a, b\}$. Is the language defined by the following SO sentence definable in MSO?

$$\begin{aligned}\varphi \;\equiv\; \exists R \,.\, \forall x, y \,.\, (R(x, y) \rightarrow (R(y, x) \wedge (P_a(x) \leftrightarrow P_b(y)))) \wedge \\ \forall x \,.\, \exists! y \,.\, R(x, y)\end{aligned}$$
[solution]

Problem 3.3.12. Let $\Sigma = \{a, b\}$ be a binary alphabet. Prove that there is no MSO formula $\varphi(x, y, z)$ s.t. for every finite word $w \in \Sigma^*$ and positions $a, b, c \in \{0, \ldots, |w| - 1\}$,

$$\mathfrak{A}_w, x : a, y : b, z : c \models \varphi \quad \text{if, and only if,} \quad a + b \equiv c \pmod{|w|}.$$

Hint: Show how to use φ to construct a nonregular language. [solution]

3.4 Miscellaneous problems

Problem 3.4.1 (Elementary separability of projective classes)**.** A set of models is an *elementary class* if it is the set of models of a sentence of first-order logic, and it is a *projective class* if it is the set of models of an existential sentence of second-order logic. Show that any two disjoint projective classes can be separated by an elementary class. *Hint: Use interpolation.* [solution]

Problem 3.4.2. Consider the standard field of real numbers $(\mathbb{R}, +, \cdot, 0, 1)$. Write an MSO formula $\varphi(x)$ which holds precisely when x is a rational number: For every $a \in \mathbb{R}$,

$$\mathbb{R}, x : a \vDash \varphi \quad \text{if, and only if,} \quad a \in \mathbb{Q}.$$

Can the sentence be written in the universal fragment of SO? [solution]

Chapter 4

The decision problem

Preliminaries

Any given theory Γ (which could be an axiomatic theory generated by a set of axioms $\mathsf{Th}(\Delta)$, or the theory of a given structure $\mathsf{Th}(\mathbb{N}, +)$) gives rise to a decision problem.

Decision problem of theory Γ.
Input: A sentence φ in the language of Γ.
Output: YES iff $\varphi \in \Gamma$.

In this section we explore several examples of theories with a decidable/undecidable decision problem and useful techniques to establish these facts.

4.1 Finite model property

Definition 4.1.1. Let $\vDash_{\text{fin}} \varphi$ hold whenever $\mathfrak{A} \vDash \varphi$ holds for every finite model $\mathfrak{A}$. A sentence φ has the *finite model property* if, and only if,

$$\vDash \varphi \quad \text{if, and only if,} \quad \vDash_{\text{fin}} \varphi,$$

and a set of sentences Γ has the finite model property if every sentence $\varphi \in \Gamma$ has it. In other words, validity of sentences in Γ reduces to validity on finite models.

Problem 4.1.2 (Finite model property)**.** Assume that Γ is a complete theory with the finite model property. Is it decidable whether $\varphi \in \Gamma$? [solution]

Problem 4.1.3 (Small model property for the $\exists^*\forall^*$-fragment)**.** Consider sentences of the form

$$\varphi \;\equiv\; \exists x_1, \ldots, x_m \,.\, \forall y_1, \ldots, y_n \,.\, \psi,$$

where ψ is quantifier-free possibly using equality, without function symbols. Can we bound the size of models of φ? What happens if ψ contains (at least) a single functional symbol? [solution]

Problem 4.1.4 (Small model property for monadic logic)**.** Consider a signature consisting only of unary relation symbols without equality $\Sigma = \{P_1, \ldots, P_k\}$ (i.e., monadic predicates) and no constants or function symbols. If a sentence φ over Σ is satisfiable, can we find a bound on the size of a finite model thereof? What happens if we allow equality? [solution]

4.2 Quantifier elimination

Definition 4.2.1. A theory Γ over a signature Σ admits *elimination of quantifiers* if for every formula $\varphi \in \mathsf{Th}(\Sigma)$ over the same signature there exists a quantifier-free formula ψ s.t. 1) $\mathsf{fv}(\psi) \subseteq \mathsf{fv}(\varphi)$ and 2) φ and ψ are Γ-equivalent in the sense that $\Gamma \models \varphi \leftrightarrow \psi$. If there exists a computable procedure which constructs ψ from φ, we then say that the theory admits *effective* elimination of quantifiers.

Problem 4.2.2. Show that a quantifier-elimination procedure needs only eliminate a single existential quantifier in formulas of the form

$$\exists x \,.\, \varphi_1 \wedge \cdots \wedge \varphi_n,$$

where $\varphi_1, \ldots, \varphi_n$ are atomic formulas containing x. (In the context of database theory, such formulas are known as *conjunctive queries.*) [solution]

Problem 4.2.3 (Quantifier elimination and completeness)**.** Let Σ be a vocabulary without constant symbols. Show that if a theory Γ over Σ admits elimination of quantifiers, then Γ is complete. [solution]

4.2.1 Equality

Problem 4.2.4 (Löwenheim (1915))**.** Consider the signature consisting of equality only $\Sigma = \{=\}$. Show that the theory of equality $\mathsf{Th}(A, =)$ admits effective elimination of quantifiers. *Hint: Consider separately the cases of A "big enough" vs. "small".* [solution]

Problem 4.2.5. Consider the empty signature and sentences using only equality. Let Γ be the set of sentences

$$\{\forall x_1, \ldots, x_n \,.\, \exists x_{n+1} \,.\, \bigwedge_{i=1}^{n} \neg x_{n+1} = x_i \mid n \in \mathbb{N}\}.$$

and consider the first-order theory of its logical consequences $\mathsf{Th}(\Gamma) = \{\varphi \mid \Gamma \models \varphi\}$.

1. Prove that $\mathsf{Th}(\Gamma)$ is decidable.
2. Prove that $\mathsf{Th}(\Gamma)$ is in PSPACE. [solution]

4.2.2 One unary function

In this section, consider the signature $\Sigma = \{f, =\}$ consisting of a unary function f and equality. Typical axiomatisable properties of f are

$$\begin{aligned}
\varphi_{\text{inj}} &\equiv \forall x, y \,.\, f(x) = f(y) \to x = y, && \text{(injectivity)}\\
\varphi_{\text{surj}} &\equiv \forall x \exists y \,.\, f(y) = x, && \text{(surjectivity)}\\
\varphi_{\text{bij}} &\equiv \varphi_{\text{inj}} \wedge \varphi_{\text{surj}}. && \text{(bijectivity)}
\end{aligned}$$

Problem 4.2.6 (2-cycles)**.** Fix a signature $\Sigma = \{f : 1, = : 2\}$ containing the equality relation and a single unary function. Consider the following sentence:

$$\varphi \equiv \forall x \,.\, f(f(x)) = x \wedge f(x) \neq x.$$

Let $\Gamma = \{\varphi, \varphi_{\geq 1}, \varphi_{\geq 2}, \dots\}$ be the set of axioms including φ and infinitely many axioms ensuring that Γ has only infinite models (c.f. Problem 2.1.6 "Cardinality constraints I"). Is the theory $\mathsf{Th}(\Gamma)$ of the logical consequences of Γ (over the signature Σ) decidable? Is it complete? *Hint: Show that* $\mathsf{Th}(\Gamma)$ *admits effective elimination of quantifiers.* [solution]

4.2.3 Dense total order

Problem 4.2.7 (Langford (1926) [20])**.** Show that the axiomatic theory of dense total orders without endpoints $\mathsf{Th}(\Delta_{\text{dlo}})$ admits effective elimination of quantifiers, where

$$\begin{aligned}
\Delta_{\text{dlo}} = \Delta_{\text{lin}} \cup \{&\forall x \forall y \,.\, x < y \to \exists z \,.\, x < z \wedge z < y, && \text{(density)}\\
&\forall x \exists y \,.\, y < x, && \text{(no minimal element)}\\
&\forall x \exists y \,.\, x < y\}. && \text{(no maximal element)}
\end{aligned}$$

[solution]

4.2.4 Discrete total order

Problem 4.2.8. Consider the theory of the integer numbers with order $\mathsf{Th}(\mathbb{Z}, \leq)$.

1. Does it admit elimination of quantifiers?

2. Consider the extended vocabulary $\mathfrak{A} = (\mathbb{Z}, s, \leq)$, where s is the successor function $s(z) = z+1$. Does $\mathsf{Th}(\mathfrak{A})$ admit elimination of quantifiers?

3. Is $\mathsf{Th}(\mathfrak{A})$ complete? [solution]

Problem 4.2.9. Consider the theory of natural numbers with order and successor $\mathsf{Th}(\mathbb{N}, s, \leq)$. Does it admit elimination of quantifiers? If not, how can one extend the vocabulary in order to ensure that in the extended vocabulary elimination of quantifiers holds? [solution]

4.2.5 Rational linear arithmetic

Problem 4.2.10 (Fourier-Motzkin elimination)**.** *Rational arithmetic* is the structure $(\mathbb{Q}, \leq, +, (c\,\cdot)_{c\in\mathbb{Q}}, 1)$. Show that the theory of rational arithmetic admits effective elimination of quantifiers, where "+" is the binary sum operator and there is a unary function $\lambda x \,.\, c \cdot x$ for every rational number $c \in \mathbb{Q}$. Is the introduction of all the functions "$(c\,\cdot)$" necessary? [solution]

4.2.6 Integral linear arithmetic

Problem 4.2.11 (Presburger's logic)**.** Consider the theory of natural numbers with addition $\mathsf{Th}(\mathbb{N}, +, =)$. Show that it is decidable via effective elimination of quantifiers. *Hint: Extend the signature with suitable constants and relations.* [solution]

4.3 Interpretations

4.3.1 Real numbers

Problem 4.3.1. Consider the language of $(\mathbb{R}, +, \cdot, 0, 1, \leq)$, and let

$$p(x) = a + b \cdot x + c \cdot x^2$$

be a second-degree polynomial, where x, a, b, c are its free variables. Find quantifier-free equivalents for the following formulas

$$\begin{aligned}
\varphi_1 &\equiv \exists x \,.\, p(x) = 0, \\
\varphi_2 &\equiv \forall x \,.\, p(x) = 0, \\
\varphi_3 &\equiv \exists x_1, x_2 \,.\, x_1 \neq x_2 \wedge p(x_1) = 0 \wedge p(x_2) = 0, \\
\varphi_4 &\equiv \forall (x \leq y \leq z) \,.\, p(y) > 0.
\end{aligned}$$

[solution]

The previous problem is greatly generalised by the following theorem.

Theorem 4.3.2 (Tarski–Seidenberg)**.** *The theory of real numbers* $\mathsf{Th}(\mathbb{R}, +, \cdot, 0, 1, \leq)$ *admits effective elimination of quantifiers.*

In the following problems we explore some applications of Theorem 4.3.2 "Tarski–Seidenberg".

Problem 4.3.3 (First-order theory of the complex numbers)**.** Is the first-order theory of the complex numbers $\mathsf{Th}(\mathbb{C}, +, \cdot, 0, 1)$ decidable? *Hint: Interpret the complex numbers in the real numbers.* [solution]

Problem 4.3.4 (First-order theory of planar Euclidean geometry)**.** Consider planar Euclidean geometry (P, B, C) where P is the set of points of the plane, the *betweenness* relation $B \subseteq P^3$ contains triples of points (a, b, c) on the same line s.t. b is between a and c, and the *congruence* relation $C \subseteq P^4$ contains four-tuples of points (a, b, c, d) s.t. the line segment ab has the same length as cd. Show that (P, B, C) is complete and decidable. *Hint: Interpret euclidean geometry in the real numbers.* [solution]

4.4 Model-checking on finite structures

In this section we investigate the complexity of the model-checking problem over finite structures.

Problem 4.4.1 (First-order logic model-checking)**.** Consider the following decision problem.

FIRST-ORDER LOGIC MODEL-CHECKING PROBLEM.
Input: A first-order logic sentence φ and a finite structure $\mathfrak{A}$.
Output: YES if, and only if, $\mathfrak{A} \models \varphi$.

What is its computational complexity? What happens if we bound the width of the input formulas (maximal number of free variables in every subformula)? [solution]

Problem 4.4.2 (SO model-checking)**.** What is the computational complexity of the following decision problem?

SO MODEL-CHECKING PROBLEM.
Input: A SO sentence φ and a finite structure $\mathfrak{A}$.
Output: YES if, and only if, $\mathfrak{A} \models \varphi$. [solution]

Chapter 5

Arithmetic

In this chapter we study the theory of natural numbers with addition and multiplication $\mathsf{Th}(\mathbb{N}, +, \cdot)$, commonly called *arithmetic*.

5.1 Numbers

(*) Problem 5.1.1 (Gödel's β function)**.** Show that there exists a predicate $\beta \subseteq \mathbb{N}^4$ definable in arithmetic s.t. for every sequence of natural numbers $a_1, \ldots, a_k \in \mathbb{N}$ there are numbers $a, b \in \mathbb{N}$ s.t. for every index $1 \le i \le k$ and any $x \in \mathbb{N}$,

$$\beta(a,b,i,x) \qquad \text{if, and only if,} \qquad a_i = x. \tag{β}$$

[solution]

The encoding power of β paves the way to show that arithmetic has very high expressive power, ranging from elementary arithmetic operations to undecidable sets of numbers. In the following exercise we combine the first two argument of β for readability in the rest of the section.

Problem 5.1.2 (Simplified function χ)**.** From the definition of β it is clear that a sequence of natural numbers is encoded as a *pair* of numbers $a, b \in \mathbb{N}$. Is it possible to encode it as a *single* natural number $p \in \mathbb{N}$? [solution]

Problem 5.1.3. Express the following functions and predicates in arithmetic:

1. The divisibility predicate $m \mid n$.
2. The predicate $\mathrm{prime}(n)$ which is true iff n is a prime number.
3. The binary predicate saying that m, n are relatively prime.
4. The least common multiplier function $\mathrm{lcm}(m, n)$.
5. The binary predicate saying that m is the largest power of a prime that divides n. [solution]

Problem 5.1.4. Express the following functions and predicates in arithmetic:

1. The exponential function 2^n.
2. The factorial function $n!$.
3. The Fibonacci function:

$$f(0) = 0, \quad f(1) = 1, \quad f(n+2) = f(n+1) + f(n), n \ge 0.$$

4. The inverse of the exponential function $\lfloor \log n \rfloor$.

5. The unary predicate saying that n is a *perfect number*, i.e., it is the sum of its divisors, except itself. [solution]

Problem 5.1.5 (Collatz problem)**.** Write a sentence φ_{Collatz} expressing that the following sequence always reaches value 1, for every starting value a_0:

$$a_{n+1} = \begin{cases} \frac{a_n}{2} & \text{if } n \text{ is even,} \\ 3 \cdot n + 1 & \text{otherwise.} \end{cases}$$

Whether φ_{Collatz} is true in arithmetic is a long-standing open problem in number theory. [solution]

Problem 5.1.6. Consider arithmetic $\mathfrak{A} = (\mathbb{N}, +, \cdot, f)$ extended with an uninterpreted function symbol f. Write a sentence φ expressing the fact that f is a univariate polynomial with coefficients from $\mathbb{N}$. [solution]

Problem 5.1.7 (Counting solutions)**.** For a given formula $\varphi(x)$ in the language of first-order arithmetic of one free variable x construct a formula $\#\varphi(y)$ s.t., for every $n \in \mathbb{N}$,

$$\mathbb{N}, y : n \models \#\varphi(y) \quad \text{if, and only if,} \quad |\{m \in \mathbb{N} \mid \mathbb{N}, x : m \models \varphi(x)\}| = n.$$

[solution]

5.2 Automata and formal languages

In this section, we consider the finite alphabet $\Sigma = \{0,1\}$. A string $w = a_0 \cdots a_n \in \Sigma^*$ encodes a natural number $[w]_2 \in \mathbb{N}$ under the least significant digit (LSD) encoding:

$$[w]_2 = a_0 \cdot 2^0 + \cdots + a_n \cdot 2^n.$$

Under this encoding, we say that an arithmetic formula $\varphi(x)$ with a single free variable x *recognises* a language $L \subseteq \Sigma^*$ if

$$L = \{w \in \Sigma^* \mid \mathbb{N}, x : [w]_2 \models \varphi\}.$$

Problem 5.2.1. Show that every regular language $L \subseteq \Sigma^*$ can be recognised by a formula of arithmetic φ_L. [solution]

Problem 5.2.2. Show that a context-free language $L \subseteq \Sigma^*$ can be recognised by a formula of arithmetic φ_L [solution]

Problem 5.2.3. Show that for any recursively-enumerable language $L \subseteq \Sigma^*$ there is a formula of arithmetic φ_L recognising it. [solution]

Problem 5.2.4. Prove that the decision problem for arithmetic is undecidable. [solution]

Problem 5.2.5 (Modular arithmetic)**.** Let $\Sigma = \{R, =\}$ be a signature containing a binary relation R and equality. Provide an axiomatisation of addition and multiplication over the signature Σ admitting finite models. [solution]

Problem 5.2.6 (Trakhtrenbrot's theorem)**.** Show that the finite validity problem of first-order logic over a signature containing at least one non-unary relation (i.e., not monadic) is undecidable. What about the finite satisfiability problem? [solution]

Problem 5.2.7. Is the first-order theory of the structure $\mathsf{Th}(\mathbb{Z}, +, \cdot)$ decidable? *Hint: Show that $\leq$ is definable by appealing to Lagrange's four square theorem.* [solution]

5.3 Miscellanea

Problem 5.3.1. Recall the definition of finitely generated monoids $\mathfrak{M} = (M, \circ, e)$ from Problem 2.9.11 "Finitely generated monoids are not axiomatisable". We can encode a monoid $\mathfrak{M}$ by arithmetic formulas $\mu(x), \nu(x, y, z), \epsilon(x)$ whenever

$$\begin{aligned} M &= \{a \in \mathbb{N} \mid \mathbb{N}, x : a \vDash \mu\}, \\ \circ &= \{(a, b, c) \in \mathbb{N}^3 \mid \mathbb{N}, x : a, y : b, z : c \vDash \nu\}, \text{and} \\ \{e\} &= \{a \in \mathbb{N} \mid \mathbb{N}, x : a \vDash \epsilon\}. \end{aligned}$$

Write an arithmetic sentence $\gamma_{\mathfrak{M}}$ which may use μ, ν, ϵ encoding that $\mathfrak{M}$ is finitely generated. [solution]

Problem 5.3.2 (Second-order quantifier elimination)**.** Weak monadic second-order logic (WMSO) has the same syntax as MSO. Semantically, the second-order quantifier $\exists X$ means that *there exists a finite subset of the universe* X, and dually for $\forall X$. Prove that for any WMSO formula φ over the signature of arithmetic without free variables of second-order there is a equivalent formula ψ of first-order logic. [solution]

Part II

Solutions

Chapter 1

Propositional logic

1.1 Logical consequence

Statement of Problem 1.1.1. Consider the following statements about formulas of classical propositional logic. For each of them, establish whether it holds or not, giving a proof in the positive cases and a counterexample in the negative ones.

1. If φ and $\varphi \leftrightarrow \psi$ are tautologies, then so is ψ.
2. If φ and $\varphi \leftrightarrow \psi$ are satisfiable, then so is ψ.
3. If φ is satisfiable and $\varphi \leftrightarrow \psi$ is a tautology, then ψ is satisfiable.
4. If φ is a tautology and $\varphi \leftrightarrow \psi$ is satisfiable, then ψ is a tautology.
5. If φ is a tautology and $\varphi \leftrightarrow \psi$ is satisfiable, then ψ is satisfiable. □

Solution of Problem 1.1.1. 1. Yes, this statement holds. Indeed, suppose by way of contradiction that there is a valuation ϱ such that $[\![\psi]\!]_\varrho = 0$. φ is a tautology, hence $[\![\varphi]\!]_\varrho = 1$. We get

$$\begin{aligned}
[\![\varphi \leftrightarrow \psi]\!]_\varrho &= F_\leftrightarrow([\![\varphi]\!]_\varrho, [\![\psi]\!]_\varrho) && \text{by definition}\\
&= F_\leftrightarrow(1,0) && \text{by assumptions}\\
&= 0 && \text{by definition of } F_\leftrightarrow
\end{aligned}$$

We have got that $\varphi \leftrightarrow \psi$ is not a tautology, a contradiction.

2. No, this statement does not hold. Take $\varphi \equiv p$, which is satisfied by any valuation ϱ such that $\varrho(p) = 1$, and let ψ be $\bot$, which is not satisfiable. Then $\varphi \leftrightarrow \psi$ is $p \leftrightarrow \bot$, which is satisfied by any valuation ϱ such that $\varrho(p) = 0$.

3. Yes, this statement holds. Indeed, suppose that a valuation ϱ is such that $[\![\varphi]\!]_\varrho = 1$. We want to prove that $[\![\psi]\!]_\varrho = 1$. Suppose by way of contradiction that $[\![\psi]\!]_\varrho = 0$. We get

$$\begin{aligned} 1 &= [\![\varphi \leftrightarrow \psi]\!]_\varrho && \varphi \leftrightarrow \psi \text{ is a tautology} \\ &= F_\leftrightarrow([\![\varphi]\!]_\varrho, [\![\psi]\!]_\varrho) && \text{by definition of semantics} \\ &= F_\leftrightarrow(1, 0) && \text{by assumptions} \\ &= 0 && \text{by definition of } F_\leftrightarrow\text{, a contradiction} \end{aligned}$$

4. No, this statement does not hold. Take $\varphi \equiv \top$, which is a tautology, and let $\psi \equiv p$, which is not a tautology. Nevertheless $\top \leftrightarrow p$ is satisfied by any valuation ϱ such that $\varrho(p) = 1$, so it is satisfiable.

5. Yes, this statement holds. By assumption, there is a valuation ϱ s.t. $[\![\varphi \leftrightarrow \psi]\!]_\varrho = 1$. Since φ is a tautology, $[\![\varphi]\!]_\varrho = 1$, and, by the definition of $F_\leftrightarrow$, $[\![\psi]\!]_\varrho = 1$ as well. □

Statement of Problem 1.1.2 "Transitivity of "$\models$"". Show that the logical consequence relation is *transitive*, in the sense that:

$$\Gamma \models \Delta \quad \text{and} \quad \Delta \models \Xi \qquad \text{implies} \qquad \Gamma \models \Xi. \qquad \square$$

Solution of Problem 1.1.2 "Transitivity of "$\models$"". Assume ϱ is a valuation satisfying all formulas in Γ. From the first assumption it satisfies all formulas in Δ, and from the second assumption all formulas in Ξ, as required. □

Statement of Problem 1.1.3 "Semantic deduction theorem". Prove that for classical propositional logic,

$$\Gamma \cup \{\varphi\} \models \psi \quad \text{if, and only if,} \quad \Gamma \models \varphi \to \psi. \qquad \square$$

Solution of Problem 1.1.3 "Semantic deduction theorem". Assume $\Gamma \cup \{\varphi\} \vDash \psi$ and take any valuation ϱ satisfying all formulas in Γ. To show $[\![\varphi \to \psi]\!]_\varrho = 1$, by the definition of classical semantics, we must show that $[\![\varphi]\!]_\varrho = 1$ implies $[\![\psi]\!]_\varrho = 1$. This follows from the assumption $\Gamma \cup \{\varphi\} \vDash \psi$. The other direction is similar. □

Statement of Problem 1.1.4 "Weak soundness of modus ponens". Prove that $\vDash \varphi$ and $\vDash \varphi \to \psi$ imply $\vDash \psi$. □

Solution of Problem 1.1.4 "Weak soundness of modus ponens". From Problem 1.1.3 "Semantic deduction theorem", if $\vDash \varphi \to \psi$, then $\varphi \vDash \psi$. We conclude by the transitivity of "$\vDash$" established in Problem 1.1.2 "Transitivity of "$\vDash$"". □

Statement of Problem 1.1.5 "Strong soundness of modus ponens". Show that modus ponens is *strongly sound*, in the sense that

$$\varphi, \varphi \to \psi \vDash \psi. \qquad \square$$

Solution of Problem 1.1.5 "Strong soundness of modus ponens". Let ϱ be a truth valuation satisfying φ and $\varphi \to \psi$. By the truth table of $\to$ we derive that ϱ also satisfies ψ, as required. □

Statement of Problem 1.1.6. Let S be a function mapping propositional variables to propositional formulas. Show that if $\Gamma \vDash \varphi$ holds, then $S(\Gamma) \vDash S(\varphi)$ holds, too. In particular, if φ is a tautology, then so is $S(\varphi)$. □

Solution of Problem 1.1.6. A variable valuation ϱ extends uniquely to a valuation of formulas $[\![-]\!]_\varrho$. The composite function $\sigma = [\![-]\!]_\varrho \circ S$ is a new valuation of variables. We claim the following commutativity property:

$$[\![\varphi]\!]_\sigma = [\![S(\varphi)]\!]_\varrho.$$

The proof is by a standard structural induction on φ, where the only interesting case is the one for variables:

$$[\![p]\!]_\sigma = \sigma(p) = [\![S(p)]\!]_\varrho.$$

Consequently, if ϱ satisfies all formulas in $S(\Gamma)$, then σ satisfies Γ. It follows that σ satisfies φ, so ϱ satisfies $S(\varphi)$. □

Statement of Problem 1.1.7. A logic is called *monotone*, if $\Delta \vDash \varphi$ and $\Gamma \supseteq \Delta$ imply $\Gamma \vDash \varphi$. Prove that classical propositional logic is monotone. □

Solution of Problem 1.1.7. By definition, $\Delta \vDash \varphi$ if, for every valuation ϱ s.t. $[\![\psi]\!]_\varrho = 1$ for every $\psi \in \Delta$, we have $[\![\varphi]\!]_\varrho = 1$ as well. Replacing Δ with a larger set of formulas Γ results in a smaller set of such valuations ϱ's, and thus $\Gamma \vDash \varphi$ follows.

L: the completeness theorem is a big hammer (not even in the book now); this is a purely semantical property

An alternative proof is obtained by the Completeness Theorem. Assuming $\Delta \vDash \varphi$, we get that there is a proof of φ from Δ. Because $\Gamma \supseteq \Delta$, the very same proof demonstrates that $\Gamma \vdash \varphi$ and hence $\Gamma \vDash \varphi$. □

Statement of Problem 1.1.8. Consider formulas built only from conjunction $\wedge$ and disjunction $\vee$. For such a formula φ, its *dualisation* $\hat{\varphi}$ is the formula obtained by replacing every occurrence of $\vee$ by $\wedge$, and vice-versa.

1. Prove that φ is a classical tautology if, and only if, $\neg\hat{\varphi}$ is a classical tautology.
2. Prove that $\varphi \leftrightarrow \psi$ is a tautology if, and only if, $\hat{\varphi} \leftrightarrow \hat{\psi}$ is a tautology.
3. Propose a method to dualise formulas additionally containing the logical constants $\bot$ and $\top$, such that the above equivalences remain valid. □

Solution of Problem 1.1.8. By pushing the negation inside, $\neg\hat{\varphi}$ is the same as φ, except that a variable p is replaced by $\neg p$. For every truth assignment ϱ, $\varrho(\varphi) = \hat{\varrho}(\neg\hat{\varphi})$, where $\hat{\varrho}(p) = 1 - \varrho(p)$ is the truth assignment that flips the truth value of ϱ at every propositional variable. If $\varrho(\varphi) = 1$ for every $\varrho(\varphi)$, then the same holds true for $\neg\hat{\varphi}$, and vice-versa, thus proving the first point. For the second point, if $\varrho(\varphi) = \varrho(\psi)$ for every ϱ, then the same holds true for $\neg\hat{\varphi}, \neg\hat{\psi}$, and thus for $\hat{\varphi}, \hat{\psi}$. For the third point it suffices to swap $\bot$ with $\top$. □

Statement of Problem 1.1.9. Let φ, ψ be two formulas without common propositional variables. Assume that $\nvDash \neg\varphi$ and $\nvDash \psi$. Is it possible that $\vDash \varphi \to \psi$? □

Solution of Problem 1.1.9. No. By assumption there are two partial valuations ϱ_1, ϱ_2 s.t. $\varrho_1 \models \varphi$ and $\varrho_2 \models \neg\psi$. Since there are no common variables, $\varrho = \varrho_1 \cup \varrho_2$ is well-defined and $\varrho \models \varphi \wedge \neg\psi$, thus showing $\not\models \varphi \to \psi$. □

Statement of Problem 1.1.10. Let $G = (V, E)$ be a finite directed graph with vertices $V = \{v_1, \ldots, v_n\}$ and consider the set of propositional formulas over variables $\{p_1, \ldots, p_n\}$

$$\Delta = \{p_i \to p_j \mid (v_i, v_j) \in E\}.$$

1. Let $\Gamma_{ij} = \Delta \cup \{\neg(p_i \to p_j)\}$. Which property of G does satisfiability of Γ_{ij} expresses?

2. Provide a propositional formula φ_n, depending only on n, s.t. $\Delta \models \varphi_n$ if, and only if, G is strongly connected. □

Solution of Problem 1.1.10. The set of formulas Γ_{ij} is satisfiable if, and only if, there is no path from p_i to p_j. A graph is strongly connected if there is a path between any two distinct vertices thereof. Take $\varphi_n \equiv \bigwedge_{i \neq j}(p_i \to p_j)$. □

1.2 Normal forms

Statement of Problem 1.2.2 "Normal forms". Prove that for each propositional formula φ, there exists a propositional formula ψ in each of the following normal forms, s.t. ψ is logically equivalent to φ, i.e., $\varphi \leftrightarrow \psi$ is a tautology:

1. Negation normal form (NNF).

2. Disjunctive normal form (DNF).

3. Conjunctive normal form (CNF). *Hint: Apply point 2.*

In each case, how large is ψ in terms of the size of φ? □

Solution of Problem 1.2.2 "Normal forms". The translation into NNF is obtained by repeatedly pushing negations inside the formula according to *De Morgan's laws* (to be used as left-to-right rewrite rules):

$$\neg(\varphi_1 \wedge \varphi_2) \leftrightarrow \neg\varphi_1 \vee \neg\varphi_2 \quad \text{and} \quad \neg(\varphi_1 \vee \varphi_2) \leftrightarrow \neg\varphi_1 \vee \neg\varphi_2.$$

If at any point a negation is in front of another negation, we eliminate them thanks to the *double negation law*

$$\neg\neg\varphi_1 \leftrightarrow \varphi_1. \tag{1.1}$$

This process is repeated until negation appears only in literals. The complexity of this translation is polynomial in the worst case (and sometimes may even make the formula *smaller*).

We give two solutions for the DNF translation. Assume that the propositional variables of φ are precisely those in $P = \{p_1, \ldots, p_n\}$. The first solution is to enumerate all the 2^n truth assignments $\varrho : P \to \{0, 1\}$, and, whenever $\varrho \vDash \varphi$, then the *characteristic formula* φ_ϱ is a disjunct of ψ. The latter formula is of the form

$$\varphi_\varrho \equiv \ell_1 \wedge \cdots \wedge \ell_n$$

where $\ell_i \equiv p_i$ if $\varrho(p_i) = 1$, and $\ell_i \equiv \neg p_i$ otherwise. This translation is (always) exponential in the number of variables.

The second solution consists in first applying the NNF translation above, and then repeatedly applying the left and right distributivity law of disjunction over conjunction:

$$\begin{aligned}(\varphi \vee \psi) \wedge \xi &\leftrightarrow (\varphi \wedge \xi) \vee (\psi \wedge \xi) \quad \text{and} \\ \xi \wedge (\varphi \vee \psi) &\leftrightarrow (\xi \wedge \varphi) \vee (\xi \wedge \psi).\end{aligned}$$

In the worst case, this solution is exponential in the size of the input formula, but for some formulas (such as those already in DNF) it is not.

The translation to CNF can be obtained by using the double negation law (1.1): First translate $\neg\varphi$ into a ψ in DNF, and then return as the result the NNF of $\neg\psi$. □

Statement of Problem 1.2.3. A formula φ using propositional variables from the set $\{p_1, \ldots, p_k\}$ *defines* the function $f : \{0,1\}^k \to \{0,1\}$ if, for any valuation ϱ,

$$[\![\varphi]\!]_\varrho = f(\varrho(p_1), \ldots, \varrho(p_k)).$$

We say that a set of logical connectives is *functionally complete* if *any* function $f : \{0,1\}^k \to \{0,1\}$ can be defined by a formula using only the connectives from the set. Show that:

1. $\{\wedge, \vee, \neg\}$ is functionally complete;
2. $\{\wedge, \neg\}$ and $\{\vee, \neg\}$ are functionally complete;
3. $\{\to, \bot\}$ is functionally complete;
4. $\{\wedge, \vee\}$ is functionally complete for all monotonic functions (w.r.t. the natural order $0 \leq 1$);
5. $\{\wedge, \vee, \to, \top\}$ is not functionally complete;
6. $\{\uparrow\}$ is functionally complete, where "$\uparrow$" is the so-called *Sheffer stroke* (a.k.a. *nand* function), which is defined as

$$\varphi \uparrow \psi \;\equiv\; \neg(\varphi \wedge \psi). \qquad \square$$

Solution of Problem 1.2.3. The first point is proved by the first method of obtaining the DNF Problem 1.2.2 "Normal forms". The second point follows from the first point and De Morgan's law $\varphi \vee \psi \;\equiv\; \neg(\neg\varphi \wedge \neg\psi)$. For the third point, notice that we can define negation as $\neg\varphi \;\equiv\; \varphi \to \bot$, and thus we obtain disjunction $\varphi \vee \psi \;\equiv\; \neg\varphi \to \psi$, and we are back in the previous point.

For the fourth point, let $f : \{0,1\}^k \to \{0,1\}$ be a monotonic Boolean function. We can produce as before an equivalent DNF formula φ. Let ψ be obtained from φ by replacing all negative literals $\neg p_i$ in φ with $\top$; thus ψ uses only connectives $\{\wedge, \vee\}$. (At this point, ψ may be further simplified by removing redundant clauses, but this is not important for this exercise.) Since $[\![\varphi]\!]$ is monotonic and the formula is in DNF, $[\![\psi]\!] = [\![\varphi]\!]$, as required.

For the fifth point, it suffices to notice that any formula build solely from $\wedge, \vee, \to, \top$ and propositional variables necessarily outputs 1 when all inputs are 1's. In particular, $\neg$ cannot be represented.

The last point follows from the second one, since $\neg\varphi \equiv \varphi \uparrow \varphi$, and $\varphi \wedge \psi \equiv \neg(\varphi \uparrow \psi)$. □

Statement of Problem 1.2.4 "Equisatisfiable 3CNF". Show that for each propositional formula φ there exists a propositional formula ψ in 3CNF such that 1) ψ is satisfiable if, and only if, φ is satisfiable, and 2) ψ has size linear in the size of φ. *Hint: Introduce new propositional variables.* □

Solution of Problem 1.2.4 "Equisatisfiable 3CNF". For each subformula ψ of φ add one propositional variable $[\psi]$ and consider the equivalences:

$$\begin{aligned} [\neg\sigma] &\leftrightarrow \neg[\sigma], \\ [\sigma \wedge \theta] &\leftrightarrow [\sigma] \wedge [\theta], \\ [\sigma \vee \theta] &\leftrightarrow [\sigma] \vee [\theta], \\ [\sigma \to \theta] &\leftrightarrow [\sigma] \to [\theta], \\ [\sigma \leftrightarrow \theta] &\leftrightarrow [\sigma] \leftrightarrow [\theta]. \end{aligned}$$

Each of the formulas above can be put into an *equivalent* 3CNF of constant size by Problem 1.2.2 "Normal forms". The formula $[\varphi] \wedge \xi$, where ξ is the conjunction of all formulas $[\psi] \leftrightarrow \psi$ above with ψ ranging over all subformulas of φ, is equisatisfiable with φ, has linear size, and it is in 3CNF. □

Statement of Problem 1.2.5. Fix a $k \in \mathbb{N}$. Does there exist an infinite sequence of formulas $\varphi_0, \varphi_1, \ldots$ in k-CNF giving rise to an infinite strictly increasing chain of valuations

$$[\![\varphi_0]\!] \subsetneq [\![\varphi_1]\!] \subsetneq \cdots ?$$

What about k-DNF formulas? And CNF formulas? □

Solution of Problem 1.2.5. First note that for 1-DNF and CNF formulas one can indeed find such a sequence, for instance

$$p_0, p_0 \vee p_1, p_0 \vee p_1 \vee p_2, \ldots.$$

The formulas above are not in k-CNF form for any fixed k, and in fact for fixed k we show that there is no such sequence. Towards reaching a contradiction, assume that k is the least natural number s.t. there is an infinite sequence of k-CNF formulas $\varphi_0, \varphi_1, \dots$ s.t.

$$\vDash \{\varphi_0 \to \varphi_1, \varphi_1 \to \varphi_2, \dots\}.$$

Let φ_i be of the form $\varphi_{i,1} \wedge \cdots \wedge \varphi_{i,n_i}$, where each conjunct $\varphi_{i,j}$ has at most k disjuncts. Each conjunct $\varphi_{i,j}$ contains at least one variable from the first formula φ_0: Since $\vDash \varphi_0 \to \varphi_{i,j}$ holds, by the interpolation theorem (c.f. Problem 1.7.2 "Propositional interpolation") $\varphi_{i,j}$ is $\top$ and could be removed ($\bot$ is excluded since we work with satisfiable formulas). For every propositional variable p, the strict implication $\vDash \varphi_i \to \varphi_{i+1}$ entails

$$\vDash \varphi_i[p \mapsto \bot] \to \varphi_{i+1}[p \mapsto \bot] \quad \text{and} \quad \vDash \varphi_i[p \mapsto \top] \to \varphi_{i+1}[p \mapsto \top],$$

and moreover at least one of the two implications above is strict. By the infinite pigeon-hole principle, we can replace p everywhere with (say) $\bot$ and still get infinitely many strict implications

$$\vDash \{\varphi_0[p \mapsto \bot] \to \varphi_1[p \mapsto \bot], \varphi_1[p \mapsto \bot] \to \varphi_2[p \mapsto \bot], \dots\}.$$

By repeatedly applying this substitution for every propositional variable of the first formula φ_0, we obtain a new chain containing infinitely many strict implications

$$\vDash \{\psi_0 \to \psi_1, \psi_1 \to \psi_2, \dots\},$$

where each ψ_i is in $(k-1)$-CNF. This contradicts the minimality of k. $\square$

1.3 Satisfiability

Statement of Problem 1.3.1. Show that the satisfiability problem for DNF formulas is in $\mathsf{NLOGSPACE}$. $\square$

Solution of Problem 1.3.1. A DNF formula is satisfiable if, and only if, it contains a non-contradictory clause, i.e., one where no variable occurs together with its negation. The latter condition can be checked in

NLOGSPACE, since checking that a clause *is* contradictory can be done in NLOGSPACE by guessing an occurrence of a variable and one of its negation, and coNLOGSPACE = NLOGSPACE by the Immerman-Szelepcsényi's theorem [16, 30]. □

Statement of Problem 1.3.2. Show that the satisfiability problem for 2-CNF formulas is in NLOGSPACE. □

Solution of Problem 1.3.2. We construct the so called *implication graph* $G = (V, E)$: Each literal $\ell \in V$ is a node and for every clause $\ell_1 \vee \ell_2$ there are two edges $(\neg\ell_1, \ell_2), (\neg\ell_2, \ell_1) \in E$ (where we identify $\neg\neg\ell$ with ℓ). Intuitively, an edge $(\ell_1, \ell_2) \in E$ represents the constraint that, if ℓ_1 is true, then ℓ_2 must also be true. Then φ is *not satisfiable* if, and only if, there is a vertex ℓ and two paths, one from ℓ to its negation $\neg\ell$, and the other from $\neg\ell$ back to ℓ (i.e., ℓ and $\neg\ell$ are in the same strongly connected component). Since graph reachability is in NLOGSPACE, and the latter class is closed under complement (by the Immerman-Szelepcsényi theorem [16, 30]), we can check satisfiability in NLOGSPACE. □

Statement of Problem 1.3.3. A formula is in XOR-CNF if it is a conjunction of *xor clauses* of the form

$$\ell_1 \oplus \cdots \oplus \ell_n,$$

where $p \oplus q$ is defined as $p \wedge \neg q \vee \neg p \wedge q$. Show that the satisfiability problem xor-formulas in CNF is in PTIME. □

Solution of Problem 1.3.3. By interpreting "$\oplus$" as addition "+" and complement "$\neg p$" as $1 - p$, formulas in XOR-CNF can be seen as systems of linear equations modulo 2. The latter can be solved in cubic time with Gaussian elimination, or even in deterministic space complexity $O(\log^2 n)$ [8]. □

Statement of Problem 1.3.4. A *Horn clause* is an implication of the form either

$$p_1 \wedge \cdots \wedge p_n \rightarrow q, \quad (n \geq 0)$$

or

$$p_1 \wedge \cdots \wedge p_n \to \bot, \quad (n \geq 0)$$

and a *Horn formula* is a conjunction of Horn clauses. Show that the satisfiability problem for Horn formulas is in PTIME. □

Solution of Problem 1.3.4. We present a dynamic programming algorithm solving the satisfiability problem for Horn formulas φ. We maintain a set P of propositional variables which must be true under any satisfying assignment for φ. Initially, we set $P := \varnothing$. We have only one update rule for P: For every Horn clause $p_1 \wedge \cdots \wedge p_n \to q$ of φ, whenever $\{p_1, \ldots, p_n\} \subseteq P$, then let $P := P \cup \{q\}$. The algorithm terminates when there is a clause $p_1 \wedge \cdots \wedge p_n \to \bot$ such that $\{p_1, \ldots, p_n\} \subseteq P$, or, after examining each clause, no new variables can be added to P.

In the former case the set is unsatisfiable, in the latter case it is satifiable by a valuation which assigns 1 to all variables in P and 0 to all remaining variables. Since at each iteration at least one propositional variable is added to P, and each step has polynomial complexity, the algorithm works in PTIME. □

Statement of Problem 1.3.5 "Self-reducibility of SAT". Assume an oracle that solves the SAT problem and let φ be a satisfiable formula. Show how to construct a satisfying assignment for φ using polynomially many invocations of the oracle. □

Solution of Problem 1.3.5 "Self-reducibility of SAT". We do binary search on the set of all assignments by fixing a total order $p_1, \ldots, p_n$ on the propositional variables of φ. At stage i, we construct a partial assignment $\varrho_i : \{p_1, \ldots, p_i\} \to \{0, 1\}$ which can be extended to a satisfying assignment of the entire φ, and a satisfiable formula φ_i obtained by replacing propositional variables $p_1, \ldots, p_i$ according to ϱ_i. Initially, we start with the everywhere undefined assignment $\varrho_0 = \varnothing$ and the original formula $\varphi_0 \equiv \varphi$. At stage $i+1$, we use the oracle to determine which one of the following two sentences is satisfiable:

$$\varphi_i[p_{i+1} \mapsto 0] \qquad \text{or} \qquad \varphi_i[p_{i+1} \mapsto 1].$$

At least one of the two formulas above is satisfiable, since by inductive hypothesis φ_i is a satisfiable sentence. If the first sentence is satisfiable, then we let $\varrho_{i+1} = \varrho_i[p_{i+1} \mapsto 0]$ and $\varphi_{i+1} \equiv \varphi_i[p_{i+1} \mapsto 0]$; similarly if the second sentence is satisfiable. At the end of the process, $\varphi_n \equiv \top$ and ϱ_n is a satisfying assignment for φ. The number of calls to the oracle is at most $2 \cdot n$. □

1.4 Complexity

Statement of Problem 1.4.1. Construct a sequence of formulas $(\varphi_n)_{n\in\mathbb{N}}$ s.t. φ is of size $O(n)$ and admits n^2 different satisfying valuations. □

Solution of Problem 1.4.1. Consider the following formula:

$$\begin{aligned}\varphi_n \equiv\ & (p_1 \to p_2) \wedge (p_2 \to p_3) \wedge \ldots \wedge (p_{n-2} \to p_{n-1}) \wedge \\ & (q_1 \to q_2) \wedge (q_2 \to q_3) \wedge \ldots \wedge (q_{n-1} \to q_{n-1}).\end{aligned}$$

Valuations satisfying this formula are those for which the sequence of values assigned to the p_i's is nondecreasing, of which there are n of them; similarly for the q_i's. There are precisely n^2 such valuations. □

Statement of Problem 1.4.2. Prove that there are Boolean functions of n variables $p_1, \ldots, p_n$ s.t. any propositional formula defining them has size $\Omega(2^n/\log n)$. □

Solution of Problem 1.4.2. We first estimate the number of propositional formulas over $p_1, \ldots, p_n$ of length m, where p_i is written down using $\log i$ binary digits $\{0, 1\}$. We call this the *binary length*. Each letter in a formula is one of the symbols

$$0, 1, \top, \bot, \wedge, \vee, \to, \leftrightarrow, \neg, (,).$$

Thus there are at most $11^m \leq 2^{4m}$ formulas of binary length m. On the other hand, there are 2^{2^n} Boolean functions of n variables. Therefore for $4m < 2^n$ the number of formulas is lower than the number of functions, and consequently there exist Boolean functions which require a formula of binary length at least $2^n/4$ to be expressed.

Now we want to come back to the standard measure of size of formulas, where each variables has size 1. Because we are using variables $p_1, \ldots, p_n$, their binary length is never greater than $\log n$. If we take the function which needs a formula of binary length at least $2^n/4$, its standard length can not be lower than $2^n/4 \log n$, even if it consists entirely of variables, which is of order $\Omega(2^n/\log n)$. □

Statement of Problem 1.4.3. In this problem we show an exponential blowup when converting a formula to an equivalent one in CNF. We proceed in two steps.

1. Prove that there is no $k \in \mathbb{N}$ s.t. every formula of classical propositional logic is equivalent to a k-CNF formula.

2. Prove that there is no polynomial $p(n)$ s.t. every formula of classical propositional logic with n variables is equivalent to a CNF formula with $O(p(n))$ clauses. □

Solution of Problem 1.4.3. We present two solutions for this exercise.

First solution. Consider the following sequence of formulas φ_n:

$$\varphi_1 \equiv p_1 \quad \text{and} \quad \varphi_n \equiv \neg(\varphi_{n-1} \leftrightarrow p_n) \text{ for every } n \geq 2.$$

One can prove by induction on n that φ_n is the xor of $p_1, \ldots, p_n$, i.e., $\varrho \vDash \varphi_n$ if $\varrho(p_i) = 1$ for an odd number of p_i's. By way of contradiction to item 1, suppose that φ_n is defined by a k-CNF formula φ. There exists a non-trivial clause ψ of φ not containing some variable p_i. Consider a valuation ϱ s.t. $[\![\psi]\!]_\varrho = 0$, and let $\varrho' = \varrho[p_i \mapsto 1 - \varrho(p_i)]$ be obtained from ϱ by flipping the value of p_i. We still have $[\![\psi]\!]_{\varrho'} = 0$, since p_i does not appear in ψ, and thus $[\![\varphi]\!]_{\varrho'} = 0$. This contradicts the assumption that φ is logically equivalent to φ_n, because the value of φ_n under ϱ and ϱ' must be different.

By the argument above, every clause of every CNF formula equivalent to φ_n must contain all variables. Each such clause is false for precisely one valuation. Since φ_n is false under 2^{n-1} valuations, it must contain 2^{n-1} clauses, and therefore be of exponential length, proving item 2.

Second solution. A k-CNF formula over $p_1, \ldots, p_n$ has at most $\binom{2n}{k}$ distinct clauses, since each clause is a subset of $\{p_1, \ldots, p_n\} \cup \{\neg p_1, \ldots, \neg p_n\}$. Therefore any k-CNF formula is equivalent to a (k-CNF) formula of length $O\left(k \cdot \binom{2n}{k}\right)$. For fixed k, the latter quantity is a polynomial $O(n^k)$. By Problem 1.4.2, there are Boolean functions expressible only by propositional formulas of the asymptotically larger length $\Omega\left(2^n / \log n\right)$, proving item 1.

Concerning item 2, if there are at most $p(n)$ non-trivial clauses and no repeating literal, then the length of the whole formula is $O(n \cdot p(n))$, and we reach a contradiction as in the previous paragraph. □

Statement of Problem 1.4.4. Consider formulas of n variables, where we allow all possible $(n-1)$-ary Boolean functions $\{0,1\}^{n-1} \to \{0,1\}$ as connectives.

1. Prove that there is a formula which is not logically equivalent to one in which every propositional variable is used only once.

2. Assume now that we allow only all possible unary $\{0,1\} \to \{0,1\}$ and binary $\{0,1\}^2 \to \{0,1\}$ Boolean functions as connectives. Prove that there is no polynomial $p(n)$ s.t. every classical propositional formula of n variables is equivalent to one in which every variable is used at most $p(n)$ times. □

Solution of Problem 1.4.4. Concerning the first point, for $n = 1$ the claim trivially holds since 0-ary functions do not have any arguments and thus no propositional variable can be used at all. Let $n \geq 2$. Consider the Boolean function $EQ(p_1, \ldots, p_n)$ which is 1 iff all its arguments are equal. This function can be expressed by the formula

$$\bigwedge_{i=1}^{n-1} (p_i \leftrightarrow p_{i+1}),$$

which uses only binary connectives and every variable at most twice. We claim that $EQ(p_1, \ldots, p_n)$ cannot be represented by a formula which uses each variable only once, even if all Boolean functions of at most $n-1$ variables are permitted as connectives. Assume, to the contrary, that such a formula φ exists. W.l.o.g. φ is of the form

$$\varphi \equiv G(F(p_1, \ldots, p_k), p_{k+1}, \ldots, p_n),$$

where F and G are some Boolean connectives.In order to keep the presentation light, we identify F and G with their respective Boolean functions. Let us consider $F(0,\dots,0), F(1,\dots,1)$, and $F(1,0,\dots,0)$. They belong to a two-element set $\{0,1\}$, hence at least two of them must be equal. If $F(0,\dots,0) = F(1,\dots,1)$, then

$$1 = EQ(0,\dots,0) = G(F(0,\dots,0),0,\dots,0) = \\ = G(F(1,\dots,1),0,\dots,0) = EQ(1,\dots,1,0,\dots,0) = 0,$$

which is a contradiction. The other cases are analogous.

Regarding the second point, a formula over n variables using each variable at most $p(n)$ times is of length $O(n \cdot p(n))$. It follows from Problem 1.4.2 that such formulas are too short to express all Boolean functions of n variables. □

Statement of Problem 1.4.5. Consider a *simple graph* $G = (V,E)$ with vertices in $V = \{v_1,\dots,v_n\}$, i.e., an undirected graph without loops $(v,v) \in E$. Let us introduce a propositional variable p_i for every vertex v_i. Given two propositional formulas $\varphi(x,y)$ and $\psi(x,y)$ over two variables x,y, consider the set of formulas

$$\Delta_{\varphi,\psi}(G) = \{\varphi(p_i,p_j) \mid (v_i,v_j) \in E\} \cup \{\psi(p_i,p_j) \mid (v_i,v_j) \notin E\}. \tag{1.2}$$

For which values of $k \in \mathbb{N}$ there are formulas φ,ψ such that for every simple graph G, the set $\Delta_{\varphi,\psi}(G)$ is satisfiable if, and only if, G is k-colourable? □

Solution of Problem 1.4.5. By a trivial counting argument there are finitely many k's for which we can express k-colourability with formulas φ,ψ. More precisely, there are only $2^{2^2} \cdot 2^{2^2} = 256$ possible choices of φ,ψ up to logical equivalence, and thus at most 256 values of k for which the answer might be positive.

For $k \in \{1,2\}$, we can write the required formulas. For $k = 1$, the graph is k-colourable if, and only if, there are no edges, and thus we can take $\varphi \equiv \bot$ and $\psi \equiv \top$. For $k = 2$, it suffices to notice that the truth value of p_i can be interpreted as the colour of the corresponding vertex v_i, and thus the required formulas are

$$\varphi(p_i,p_j) \equiv p_i \wedge \neg p_j \vee \neg p_i \wedge p_j \quad \text{and} \quad \psi(p_i,p_j) \equiv \top.$$

For $k > 2$ this is impossible. We present two solutions of this fact.

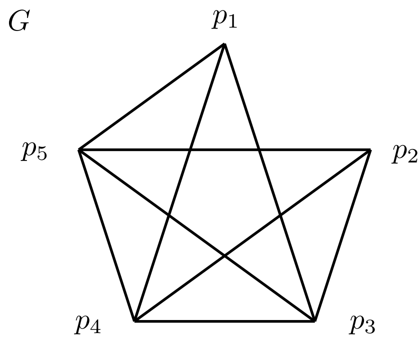


Figure for Problem 1.4.5.

First solution. The first solution holds under the assumption $\mathsf{NLOGSPACE} \neq \mathsf{NPTIME}$. We can assume w.l.o.g. that φ, ψ are in 2-CNF, and thus $\Delta_{\varphi,\psi}(G)$ is equivalent to a 2-CNF formula whose size is polynomial in the size of the graph. Satisfiability of 2-CNF formulas is in $\mathsf{NLOGSPACE}$ (c.f. Problem 1.3.2), and consequently so it is satisfiability of $\Delta_{\varphi,\psi}(G)$. Since k-colourability is NPTIME-complete for every $k > 2$, there are no such φ, ψ unless $\mathsf{NLOGSPACE} = \mathsf{NPTIME}$.

Second solution. The second solution has been proposed by Tadeusz Dudkiewicz and does not require any complexity-theoretic assumption. Suppose, by way of contradiction, that the required formulas φ, ψ exist. Consider the graph G over vertices $\{v_1, \ldots, v_n\}$ obtained from the complete graph K_n by removing edge (v_1, v_2) (c.f. figure). The graph G is n-colourable, and thus $\Delta_{\varphi,\psi}(G)$ is satisfiable, say by valuation ϱ. By definition of $\Delta_{\varphi,\psi}(G)$, $\varrho \vDash \varphi(p_1, p_3), \varphi(p_1, p_4)$. On the other hand, $\varrho \nvDash \varphi(p_1, p_2)$, because, otherwise, we would have $\varrho \vDash \Delta_{\varphi,\psi}(K_n)$, even though K_n is not n-colourable. Thus, $\varrho(p_2) \neq \varrho(p_3), \varrho(p_2) \neq \varrho(p_4)$, implying $\varrho(p_3) = \varrho(p_4)$. Since $\varrho \vDash \varphi(p_3, p_4)$ by definition of $\Delta_{\varphi,\psi}(G)$, φ is satisfied when both its arguments are set to $1 - \varrho(p_2)$. Consequently, $\Delta_{\varphi,\psi}(K_n) = \{\varphi(p_i, p_j) \mid 0 \leq i, j \leq n\}$ is satisfied by the valuation assigning $1 - \varrho(p_2)$ to every variable. This is a contradiction, because K_n is not n-colourable. $\square$

1.5 Compactness

Statement of Problem 1.5.1 "Compactness theorem for propositional logic". Let Γ be an infinite set of formulas of propositional logic. Show that if every finite subset of Γ is satisfiable, then Γ is satisfiable. *Hint: Use König's lemma.* □

Solution of Problem 1.5.1 "Compactness theorem for propositional logic". Let $\Gamma = \{\varphi_1, \varphi_2, \dots\}$ be an infinite set of sentences of propositional logic s.t. every finite subset thereof is satisfiable. Consider now the set of sentences

$$\Delta = \{\top, \varphi_1, \varphi_1 \wedge \varphi_2, \dots\}.$$

Clearly, also every finite subset of Δ is satisfiable, and if Δ is satisfiable, then so is Γ. Let $\psi_i \equiv \varphi_1 \wedge \dots \wedge \varphi_i$. Consider the tree where vertices of height i are the partial valuations $\varrho : \{p \text{ in } \psi_i\} \to \{0,1\}$ satisfying ψ_i, and there is an edge from ϱ at height i to ϱ' at height $i+1$ whenever ϱ and ϱ' agree on the variables of ψ_i. Each level of the tree is finite since ψ_i has finitely many variables, and thus the tree is finitely branching. Since the tree is infinite, by König's lemma there is an infinite branch $\varrho_0, \varrho_1, \dots$, where each subsequent valuation extends the previous one. Thus, $\varrho_\omega = \varrho_0 \cup \varrho_1 \cup \cdots$ is a total valuation satisfying every ψ_i's. Consequently, Δ is satisfiable, as required. □

Statement of Problem 1.5.2. Prove that Problem 1.5.1 "Compactness theorem for propositional logic" implies the following alternative reformulation: If $\Gamma \vDash \varphi$, then there exists a finite subset $\Delta \subseteq_{\text{fin}} \Gamma$ s.t. $\Delta \vDash \varphi$. □

Proof. Assume $\Gamma \vDash \varphi$. By way of contradiction, assume $\Delta \nvDash \varphi$, for every $\Delta \subseteq_{\text{fin}} \Gamma$. Consequently, $\Gamma \cup \{\neg\varphi\}$ is finitely satisfiable, and thus by Problem 1.5.1 "Compactness theorem for propositional logic" $\Gamma \cup \{\neg\varphi\}$ is satisfiable, which is a contradiction. □

Statement of Problem 1.5.3 "Compactness implies König's lemma". Use the compactness theorem for propositional logic to prove König's lemma.

□

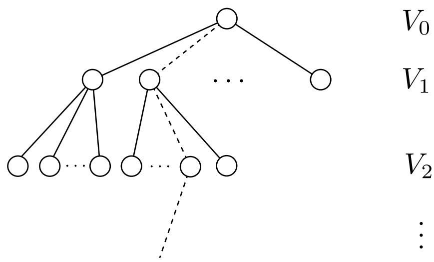


Figure for Problem 1.5.3 "Compactness implies König's lemma".

Solution of Problem 1.5.3 "Compactness implies König's lemma". Let $G = (V, E)$ be an infinite, finitely branching tree, and we need to show that it has an infinite branch. We first observe that the assumptions on G imply that we can find arbitrarily long branches starting from the root. We layer the vertices in the tree according to their height, i.e., their distance from the root: $V = V_0 \cup V_1 \cup \cdots$, where

$$V_i = \{v \in V \mid v \text{ is at height } i\} = \{v_{i,1}, \ldots, v_{i,n_i}\}.$$

For each vertex $v_{i,j} \in V_i$ we have a propositional variable $p_{i,j}$ indicating that $v_{i,j}$ belongs to an infinite branch. The local requirements are the following:

1. For every height i, exactly one $v_{i,j}$ is selected:

$$\varphi_i \equiv \bigvee_{1 \le j \le n_i} p_{i,j} \wedge \bigwedge_{1 \le j < k \le n_i} \neg p_{i,j} \vee \neg p_{i,k}.$$

2. For every height i, $v_{i,j}$ and $v_{i+1,k}$ can be selected only if there is an edge between them in the tree:

$$\psi_i \equiv \bigvee_{(v_{i,j}, v_{i+1,k}) \in E} p_{i,j} \wedge p_{i+1,k}.$$

Consider the infinite set of sentences

$$\Gamma = \Gamma_0 \cup \Gamma_1 \cup \cdots, \qquad \text{where } \Gamma_i = \{\varphi_0, \ldots, \varphi_i, \psi_0, \ldots, \psi_i\}.$$

By construction, Γ_i is satisfiable if, and only if, G contains a branch of length i, and Γ is satisfiable if, and only if, G contains an infinite branch.

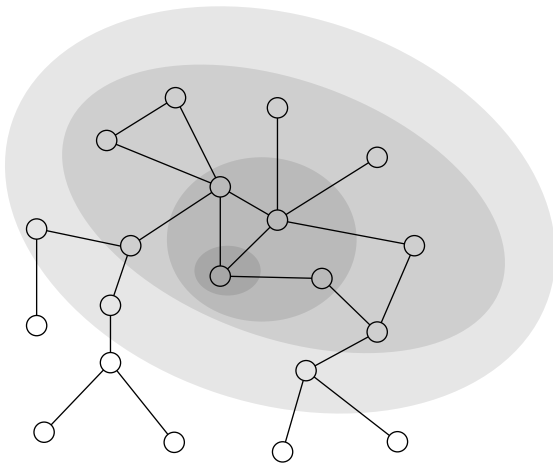


Figure for Problem 1.5.4 "De Bruijn–Erdős theorem".

Towards reaching a contradiction, assume that Γ is not satisfiable, and thus, by the compactness theorem there is an unsatisfiable finite subset thereof $\Delta \subseteq_{\text{fin}} \Gamma$. Since Δ is finite, there is a level i s.t. $\Delta \subseteq \Gamma_i$, and since Δ is unsatisfiable, then also the larger Γ_i is unsatisfiable. However, this contradicts the fact that G contains arbitrarily long branches. □

Statement of Problem 1.5.4 "De Bruijn–Erdős theorem". Let k be a fixed natural number. Prove, using the compactness theorem, that if every finite subgraph of an infinite graph $G = (V, E)$ is k-colourable, then G is k-colourable as well. □

Solution of Problem 1.5.4 "De Bruijn–Erdős theorem". We encode colourability as an infinite set of sentences. For each country $i \in V$ and colour $1 \leq j \leq k$, let p_{ij} be a propositional variable indicating that the i-th country has colour j. Then, k-colourability of G can be described by an infinite set of sentences Γ: For each country i, we have a sentence to make sure i is uniquely coloured, and for each pair of neighbouring countries $(i, j) \in E$ we have a sentence ensuring that their colours differ. If Γ is unsatisfiable, then by compactness it has a finite unsatisfiable subset $\Delta \subseteq_{\text{fin}} \Gamma$. Since Δ is finite, it can only refer to a finite subgraph G' of G, expressing a necessary (but not sufficient in general) condition to k-colourability of G'. Since Δ' is unsatisfiable, G' is not k-colourable, and thus G has a finite subgraph which is not k-colourable. □

Statement of Problem 1.5.5. Consider an infinite set of people with the property that 1) each man has a *finite* number of girlfriends, and 2) any $k \in \mathbb{N}$ men collectively have at least k girlfriends. Demonstrate that each man can marry one of his girlfriends without committing polygamy, i.e., no man marries two or more women (polygyny) and no woman marries two or more men (polyandry). Are the two assumptions necessary? □

Solution of Problem 1.5.5. For $i, j \in \mathbb{N}$, let p_{ij} be a propositional variable indicating that the i-th man and the j-th woman are married. For each man i, let $J_i \subseteq_{\text{fin}} \mathbb{N}$ be the finite set of his girlfriends. The constraints of the problem are expressed by the following infinite set Γ of formulas (to be interpreted conjunctively):

$$\{\bigvee_{j \in J_i} p_{ij} \mid i \in \mathbb{N}\} \cup \{\neg(p_{ij_1} \wedge p_{ij_2}) \mid i, j_1, j_2 \in \mathbb{N}, j_1 \neq j_2\} \cup$$
$$\cup \{\neg(p_{i_1 j} \wedge p_{i_2 j}) \mid i_1, i_2, j \in \mathbb{N}, i_1 \neq i_2\}.$$

The first group expresses the fact that every man marries some of his girlfriends, the second one forbids polygyny, and the third one polyandry. Let $\Delta_k \subseteq \Gamma$ be the (infinite) subset of Γ referring to men $\{0, \dots, k-1\}$. Since by assumption any k man jointly have at least k girlfriends, Δ_k is satisfiable. Any finite subset of formulas $\Delta \subseteq_{\text{fin}} \Gamma$ refers to finitely many men, which implies $\Delta \subseteq \Delta_k$ for some finite k (the maximum index of a man referred to by Δ), and thus also Δ is satisfiable. By the compactness theorem, Γ is satisfiable. □

Statement of Problem 1.5.6. The following equivalence holds, for any truth assignment ϱ:

$$\varrho \models r \leftrightarrow (p_0 \vee p_1) \quad \text{if, and only if,} \quad \varrho(r) = \max(\varrho(p_0), \varrho(p_1)).$$

Does there exist a (possibly infinite) set of formulas Γ over propositional variables $\{r, p_0, p_1, \dots\}$ s.t., for every ϱ,

$$\varrho \models \Gamma \quad \text{if, and only if,} \quad \varrho(r) = \max_{n \in \mathbb{N}}(\varrho(p_n))? \qquad \square$$

Solution of Problem 1.5.6. There is no such set. By way of contradiction, let us suppose that such a set Γ exists. Consider

$$\Delta = \Gamma \cup \{r, \neg p_0, \neg p_1, \dots\}.$$

Every finite subset $\Delta_0 \subseteq_{\text{fin}} \Delta$ is satisfiable: it contains only finitely many negated variables; take a valuation ϱ which makes r and one of the not mentioned variables true. By assumption $\varrho \models \Gamma$, hence $\varrho \models \Delta_0$. By the compactness theorem, Δ is satisfiable. This is a contradiction, because the only valuation ϱ which may satisfy it assigns 0 to all the p_i's (by the added negations) and 1 to r, and thus by assumption it cannot satisfy Γ. $\square$

Statement of Problem 1.5.7. Does there exist a set Γ of sentences over propositional variables $\{p_0, p_1, \dots\}$ s.t. the valuations ϱ satisfying Γ are exactly those s.t. $\{i \in \mathbb{N} \mid \varrho(p_i) = 1\}$ is finite? $\square$

Solution of Problem 1.5.7. No. By way of contradiction, suppose that such a set Γ exists and consider the set

$$\Delta = \Gamma \cup \{p_0, p_1, \dots\}.$$

Take any finite subset $\Delta_0 \subseteq_{\text{fin}} \Delta$. It contains only finitely many sentences of the form p_i. The valuation ϱ assigning 1 to those p_i's and 0 to the remaining ones assigns 1 to finitely many variables, hence $\Gamma \models \varrho$ by assumption, and thus $\Delta_0 \models \varrho$. By the compactness theorem, Δ is satisfiable. However, the only valuation that may satisfy it assigns 1 to all variables, and hence does not satisfy Γ, contradicting the assumption. $\square$

Statement of Problem 1.5.9 "The name of the game". Let Z be a countable set of propositional variables and for a set of sentences Γ let

$$[\![\Gamma]\!] = \{\varrho : Z \to \{0,1\} \mid \varrho \models \Gamma\}.$$

Consider the topological space (X, τ), where X is the set of all valuations $[\![\top]\!]$ and τ is the topology generated by basic open sets of the form $[\![\varphi]\!]$. Show, using the compactness theorem for propositional logic, that (X, τ) is a countably compact topological space. $\square$

Solution of Problem 1.5.9 "The name of the game". Closed sets are precisely those of the form $[\![\Gamma]\!]$. Let $\mathcal{C} = \{[\![\Gamma_0]\!], [\![\Gamma_1]\!], \dots\}$ be a countable family of closed sets with the property that every finite subfamily thereof has nonempty intersection. W.l.o.g. we can assume that each Γ_i is finite and that they form a nondecreasing chain under set inclusion:

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots.$$

By assumption, $[\![\Gamma_i]\!] \neq \varnothing$, i.e., Γ_i is satisfiable. By compactness of propositional logic, $\Gamma_\omega = \Gamma_0 \cup \Gamma_1 \cup \cdots$ is also satisfiable, and thus $[\![\Gamma_\omega]\!] = [\![\Gamma_0]\!] \cap [\![\Gamma_1]\!] \cap \cdots = \bigcap \mathcal{C} \neq \varnothing$, as required. $\square$

Statement of Problem 1.5.10 "Compactness with infinitary conjunction". Show that the compactness theorem still holds for infinite CNF formulas with infinitary conjunction

$$\bigwedge_{i=1}^{\infty} \bigvee_{j=1}^{n_i} l_{ij},$$

where l_{ij} is a literal (a propositional variable or a negation thereof). $\square$

Solution of Problem 1.5.10 "Compactness with infinitary conjunction". This is immediate, since a set of formulas $\Gamma = \{\varphi_1, \varphi_2, \dots\}$ in the form above is equivalent to set of formulas $\Delta = \bigcup_i \Gamma_i$, where $\Gamma_i = \{\psi_1, \psi_2, \dots\}$, whenever $\varphi_i = \psi_1 \wedge \psi_2 \wedge \cdots$. If Γ is finitely satisfiable, then Δ is also finitely satisfiable. One can then apply Problem 1.5.1 "Compactness theorem for propositional logic" to Δ to obtain that Δ is satisfiable, and thus Γ is satisfiable. $\square$

Statement of Problem 1.5.11 "No compactness with infinitary disjunction". Show that the compactness fails infinite DNF formulas with infinitary disjunction

$$\bigvee_{i=1}^{\infty} \bigwedge_{j=1}^{n_i} l_{ij}. \qquad \square$$

Solution of Problem 1.5.11 "No compactness with infinitary disjunction". Consider $\Delta = \{p_0 \vee p_1 \vee \cdots, \neg p_0, \neg p_1, \dots\}$. Then Δ is an unsatisfiable set s.t. every finite subset thereof is satisfiable. □

1.6 Resolution

Statement of Problem 1.6.1 "Resolution is sound". Show that the resolution rule (1.3) is sound. *Hint: Proceed by induction on the length of derivations.* □

Solution of Problem 1.6.1 "Resolution is sound". We show by rule induction that resolution (1.3) preserves validity: Assume $\Gamma \vDash p \vee \varphi$ and $\Gamma \vDash \neg p \vee \psi$, and let ϱ be any valuation satisfying all formulas in Γ. If $\varrho(p) = 0$, then $\varrho \vDash \varphi$; if $\varrho(p) = 1$, then $\varrho \vDash \psi$. We obtain $\varrho \vDash \varphi \vee \psi$, as required. □

A set of inference rules is *complete* if it can prove all logical entailments,

$$\Gamma \vDash \varphi \quad \text{implies} \quad \Gamma \vdash \varphi,$$

and *refutation complete* if it can derive a contradiction from any unsatisfiable set of formulas:

$$\Gamma \vDash \bot \quad \text{implies} \quad \Gamma \vdash \bot.$$

Statement of Problem 1.6.2 "Resolution is refutation complete". Show that resolution (1.3) is refutation complete when Γ is a set of clauses. Is it complete? *Hint: Proceed by induction on the number of propositional variables.* □

Solution of Problem 1.6.2 "Resolution is refutation complete". Assume Γ is an unsatisfiable finite set of clauses not containing any tautology. Call such a set *stable*. We build a sequence of stable sets related by provability

$$\Gamma = \Gamma_0 \vdash \Gamma_1 \vdash \cdots \vdash \Gamma_n = \bot,$$

starting at Γ and ending in the empty set of clauses Γ_n. Assume Γ_i has already been built. Since Γ_i is unsatisfiable, there exists a propositional variable p appearing positively and negatively. Consider the following decomposition

$$\Gamma_i = \Gamma_i^p \cup \Gamma_i^{\neg p} \cup \Delta,$$

where Γ_i^p is the set of clauses containing p, $\Gamma_i^{\neg p}$ is the set of clauses containing $\neg p$, and Δ is the remaining set of clauses. Since Γ_i does not contain any tautology, $\Gamma_i^p, \Gamma_i^{\neg p}$ are disjoint. We build the next set as

$$\Gamma_{i+1} = \{\varphi \vee \psi \mid (p \vee \varphi) \in \Gamma_i^p, (\neg p \vee \psi) \in \Gamma_i^{\neg p}\} \cup \Delta.$$

Since Γ_{i+1} is obtained from Γ_i by repeated applications of resolution, $\Gamma_i \vdash \Gamma_{i+1}$. By soundness of resolution (c.f. Problem 1.6.1 "Resolution is sound"), also Γ_{i+1} is unsatisfiable. Since no tautologies are introduced, Γ_{i+1} is a stable set of clauses containing one less propositional variable than Γ_i. The procedure eventually terminates with an empty Γ_n. By transitivity, we get $\Gamma \vdash \bot$, as required.

The case when Γ is infinite is handled with an application of compactness (c.f. Problem 1.5.1 "Compactness theorem for propositional logic"), by finding a finite unsatisfiable set of formulas $\Delta \subseteq_{\text{fin}} \Gamma$ and applying the reasoning above to Δ.

Finally, resolution is incomplete, as witnessed by $\vDash a \to (a \vee b)$: there is no way to apply resolution (1.3) to derive $a \vdash a \vee b$. □

Statement of Problem 1.6.3. Let there be m pigeons and n holes, and for every $1 \leq i \leq m$ and $1 \leq j \leq n$, let $p_{i,j}$ be a propositional variable encoding that pigeon i is in hole j. Consider the following CNF family of *pigeonhole formulas*

$$\varphi_{m,n} \equiv \bigwedge_{i=1}^{m} \bigvee_{j=1}^{n} p_{ij} \wedge \bigwedge_{j=1}^{n} \bigwedge_{i=1}^{m} \bigwedge_{k=i+1}^{m} \neg p_{ij} \vee \neg p_{kj},$$

stating that 1) each pigeon is inside some hole, and 2) no hole contains two pigeons. Show that $\varphi_{n+1,n}$ has only resolution refutation trees of size exponential in n. □

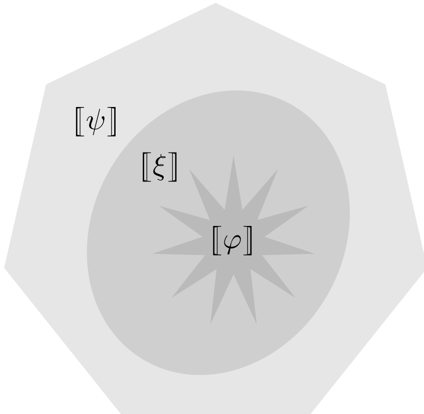


Figure for Problem 1.7.2 "Propositional interpolation".

1.7 Interpolation

Statement of Problem 1.7.2 "Propositional interpolation". Let φ and ψ be two formulas of classical propositional logic s.t. $\vDash \varphi \to \psi$. Show that there exists a formula ξ interpolating φ, ψ. □

Solution of Problem 1.7.2 "Propositional interpolation". We remove a single propositional variable p occurring in φ but not in ψ by virtue of the tautology

$$\vDash \varphi \to \xi, \qquad \text{where } \xi \ \equiv \ \varphi[p \mapsto \top] \vee \varphi[p \mapsto \bot].$$

In order to also have $\vDash \xi \to \psi$, we rely on the following tautology:

$$\vDash \varphi \to \psi \ \text{ implies } \ \vDash \varphi[p \mapsto \top] \vee \varphi[p \mapsto \bot] \to \psi \qquad (p \text{ not in } \psi).$$

The latter tautology follows from the fact that every valuation ϱ satisfying ξ extends to a valuation ϱ' satisfying φ for some choice of $\varrho'(p)$; by the assumption ϱ' satisfies ψ, and since p does not occur in ψ, the same holds for the original ϱ. The interpolation theorem follows by removing all such p's one after the other. □

Statement of Problem 1.7.3 "Beth's definability theorem". Let φ be a formula of propositional logic and let p, q be two propositional variables s.t. p occurs in φ, q does not occur in φ, and

$$\varphi, \varphi[p \mapsto q] \vDash p \leftrightarrow q. \qquad \text{(implicit definability of } p\text{)}$$

Prove that there exists a formula ψ not containing p, q s.t.

$$\varphi \vDash p \leftrightarrow \psi. \qquad \text{(explicit definability } p\text{)}$$

Hint: Use interpolation. □

First solution of Problem 1.7.3 "Beth's definability theorem". By Problem 1.1.3 "Semantic deduction theorem", we can rewrite the assumption on the implicit definability of p as

$$\vDash \varphi \to \varphi[p \mapsto q] \to p \to q.$$

We group first the formulas containing p and later those containing q:

$$\vDash \varphi \land p \to \varphi[p \mapsto q] \to q.$$

From the interpolation theorem for propositional logic (c.f. Problem 1.7.2 "Propositional interpolation") there exists an interpolant ψ not containing neither p nor q s.t.

$$\vDash \varphi \land p \to \psi \qquad \text{and} \qquad \vDash \psi \to \varphi[p \mapsto q] \to q.$$

By another application of Problem 1.1.3 "Semantic deduction theorem", we obtain the required explicit definability of p. □

Second solution of Problem 1.7.3 "Beth's definability theorem". This solution uses a brute force approach.

Assume that the variables of φ are $p, r_1, \ldots r_k$. First observe that for any valuation $\varrho : \{r_1, \ldots r_k\} \to \{0, 1\}$ there is at most one $a \in \{0, 1\}$ such that $\varrho[p \mapsto a] \vDash \varphi$. Indeed, suppose to the contrary that for some ϱ both its extensions satisfy φ. Then $\varrho[q \mapsto 0][p \mapsto 1] \vDash \varphi, \varphi[p \mapsto q], \neg(p \leftrightarrow r)$, which contradicts the assumptions.

Let this a be denoted $p(\varrho)$. We extend it to a total function $p : \{0, 1\}^k \to \{0, 1\}$ in an arbitrary way. We know that any such function can be defined by a propositional formula ψ involving only variables $r_1, \ldots, r_k$ (c.f. Problem 1.2.3). Now ψ is the desired explicit definition of p. □

Statement of Problem 1.7.4. Prove the following infinite extension of the interpolation theorem for propositional logic: If Δ, Γ are two sets of formulas satisfying $\Gamma \vDash \Delta$, then there is a set of formulas Θ containing only propositional variables occurring both in (some formula of) Γ and in (some formula of) Δ s.t. $\Gamma \vDash \Theta$ and $\Theta \vDash \Delta$. □

First solution of Problem 1.7.4. We propose two solutions to this problem. Let $\Delta = \{\varphi_1, \varphi_2, \ldots\}$. For each i we have $\Gamma \vDash \varphi_i$. From the compactness theorem there is a finite subset $\Gamma_i \subseteq_{\text{fin}} \Gamma$ such that $\Gamma_i \vDash \varphi_i$. Thus, $\bigwedge \Gamma_i$ is a sentence s.t. $\vDash \bigwedge \Gamma_i \to \varphi_i$. It follows from the standard interpolation theorem that there is a sentence ϑ_i containing only the common variables of Γ_i and φ_i s.t. $\vDash \bigwedge \Gamma_i \to \vartheta_i$ and $\vDash \vartheta_i \to \varphi_i$. Take $\Theta = \{\vartheta_1, \vartheta_2, \ldots\}$. □

Second solution of Problem 1.7.4. We simulate the proof of the interpolation theorem for individual formulas; cf. Problem 1.7.2 "Propositional interpolation". The interpolant was constructed by repeatedly replacing φ with

$$\varphi[p \mapsto \top] \vee \varphi[p \mapsto \bot]$$

whenever p did not occur in ψ. We slightly modify this step by postulating that, if p does not appear in φ, then the result is just φ (instead of $\varphi \vee \varphi$). We apply the modified step to all formulas of Γ simultaneously, and we do so for each of the (possibly infinitely many) propositional variables occurring in Δ but not in Γ. Since each of the formulas in Γ contains only finitely many variables, thanks to the modification above it stabilises after finitely many steps. Let the stable variant of $\gamma \in \Gamma$ be $\hat{\gamma}$. In this way, the result of applying infinitely many steps to Γ is well-defined as $\{\hat{\gamma} \mid \gamma \in \Gamma\}$ and is the desired Θ. □

Statement of Problem 1.7.5. Show that if one could bound the circuit size of an interpolant by a polynomial in the size of the input formulas, then any disjoint pair of NPTIME languages would be separable by a circuit of polynomial size. Deduce that $\mathsf{NPTIME} \cap \mathsf{coNPTIME}$ would have polynomial size circuits in this case. □

Solution of Problem 1.7.5. As in Cook's theorem showing that SAT is NPTIME-complete, for every language $L \in \mathsf{NPTIME}$ there exists a polynomial p and a family of propositional formulas $\varphi_n^L(\bar{p}, \bar{q})$, each with n input variables $\bar{p} = (p_1, \ldots, p_n)$ and polynomially many $p(n)$ advice variables $\bar{q} = (q_1, \ldots, q_{p(n)})$, s.t. for every input $\bar{p}$ of length n,

$$\bar{p} \in L \quad \text{if, and only if,} \quad \text{there is } \bar{q} \text{ s.t.} \vDash \varphi_n^L(\bar{p}, \bar{q}).$$

If $L, M \in \mathsf{NPTIME}$ are disjoint, then for every input length n, input variables $\bar{p}$, polynomial advice $\bar{q}$ for L, and polynomial advice $\bar{r}$ for M,

$$\vDash \varphi_n^L(\bar{p}, \bar{q}) \to \neg\varphi_n^M(\bar{p}, \bar{r}).$$

By assumption, there exists an interpolant $\psi(\bar{p})$ of polynomial circuit size using only the common variables $\bar{p}$, and thus L, M can be separated by a circuit of polynomial size, as required.

If $L \in \mathsf{NPTIME} \cap \mathsf{coNPTIME}$, then it suffices to apply the result with M equal to the complement of L. □

Statement of Problem 1.7.6. A proof system has the *polynomial interpolation property* if, whenever $\neg(\varphi \to \psi)$ has a proof of size n, there exists an interpolant ξ of size polynomial in n. Show that resolution has the polynomial interpolation property. □

Solution of Problem 1.7.6. Let φ, ψ be CNF formulas of the form

$$\varphi \equiv \varphi_1 \wedge \ldots \wedge \varphi_m \quad \text{and} \quad \psi \equiv \psi_1 \wedge \ldots \wedge \psi_n,$$

s.t. $\varphi \wedge \psi$ is unsatisfiable. We enrich the resolution rule as follows:

$$\frac{\vdash p \vee \eta \ [\xi] \qquad \vdash \neg p \vee \eta' \ [\xi']}{\vdash \eta \vee \eta' \ [\xi'']}, \text{ where} \tag{1.3}$$

$$\xi'' \equiv \begin{cases} \xi \vee \xi' & \text{if } p \in \mathsf{var}(\varphi) \setminus \mathsf{var}(\psi) \quad \text{(I)}, \\ \xi \wedge \xi' & \text{if } p \in \mathsf{var}(\psi) \setminus \mathsf{var}(\varphi) \quad \text{(II)}, \\ (p \vee \xi) \wedge (\neg p \vee \xi') & \text{if } p \in \mathsf{var}(\psi) \cap \mathsf{var}(\varphi) \quad \text{(III)}. \end{cases}$$

together with two new rules allowing us to get started:

$$\frac{}{\vdash \varphi_i \ [\bot]} \qquad \text{and} \qquad \frac{}{\vdash \psi_j \ [\top]}. \tag{1.4}$$

In $\vdash \eta\ [\xi]$, the formula ξ is called a *partial interpolant*, and we prove that it satisfies the invariant of being an interpolant of $\varphi \wedge \neg\eta$ and $\psi \rightarrow \eta$:

$$\vdash \eta\ [\xi] \qquad \text{implies} \qquad (I_1)\ \varphi \wedge \neg\eta \vDash \xi \quad \text{and} \quad (I_2)\ \xi \vDash \psi \rightarrow \eta.$$

The invariant is clearly satisfied in the base cases (1.4). Regarding the inductive case (1.3), assume

$$\begin{aligned} &(I_{1\mathrm{L}})\ \varphi \wedge \neg(p \vee \eta) \vDash \xi && \text{and} \quad (I_{2\mathrm{L}})\ \xi \vDash \psi \rightarrow (p \vee \eta), \\ &(I_{1\mathrm{R}})\ \varphi \wedge \neg(\neg p \vee \eta') \vDash \xi' && \text{and} \quad (I_{2\mathrm{R}})\ \xi' \vDash \psi \rightarrow (\neg p \vee \eta'). \end{aligned}$$

In case (I), we have to prove

$$(I_1)\ \varphi \wedge \neg(\eta \vee \eta') \vDash \xi \vee \xi' \quad \text{and} \quad (I_2)\ \xi \vee \xi' \vDash \psi \rightarrow (\eta \vee \eta').$$

In order to prove (I_1), let $\varrho \vDash \varphi \wedge \neg(\eta \vee \eta')$. If $\varrho(p) = 1$, then from $(I_{1\mathrm{R}})$ we get $\varrho \vDash \xi'$; the other case is similar. In order to prove (I_2), let $\varrho \vDash (\xi \vee \xi') \wedge \psi$. If $\varrho \vDash \xi$, since p does not appear in ξ, we also have $\varrho[p \mapsto 0] \vDash \xi$, and, by $(I_{2\mathrm{L}})$, $\varrho[p \mapsto 0] \vDash \eta$, and thus $\varrho \vDash \eta$ since p does not occur in η; the other case $\varrho \vDash \xi'$ is similar.

In case (II), we have to prove

$$(I_1)\ \varphi \wedge \neg(\eta \vee \eta') \vDash \xi \wedge \xi' \quad \text{and} \quad (I_2)\ \xi \wedge \xi' \vDash \psi \rightarrow \eta \vee \eta'.$$

In order to prove (I_1), let $\varrho \vDash \varphi \wedge \neg(\eta \vee \eta')$. Since p occurs neither in φ nor in η, the same holds by replacing ϱ with $\varrho[p \mapsto 0]$, resp., $\varrho[p \mapsto 1] \vDash \varphi \wedge \neg\eta$; by $(I_{1\mathrm{L}}), (I_{1\mathrm{R}})$ we obtain $\varrho \vDash \xi \wedge \xi'$. In order to prove (I_2), let $\varrho \vDash \xi \wedge \xi' \wedge \psi$. By $(I_{2\mathrm{L}}), (I_{2\mathrm{R}})$ and a step of resolution we obtain $\varrho \vDash \eta \vee \eta'$, as required.

Finally, in case (III), we have to prove

$$\begin{aligned} &(I_1)\ \varphi \wedge \neg(\eta \vee \eta') \vDash (p \vee \xi) \wedge (\neg p \vee \xi'), \text{ and} \\ &(I_2)\ (p \vee \xi) \wedge (\neg p \vee \xi') \vDash \psi \rightarrow \eta \vee \eta'. \end{aligned}$$

We prove (I_1) first. Let ϱ satisfy $\varrho \vDash \varphi \wedge \neg(\eta \vee \eta')$. In particular, $\varrho \vDash \{\varphi, \neg\eta, \neg\eta'\}$. We do a case analysis on $\varrho(p)$. In the first case, assume $\varrho(p) = 1$. By the inductive hypothesis $(I_{1\mathrm{R}})$, we have $\varrho \vDash \xi'$. Consequently, $\varrho \vDash (p \vee \xi) \wedge (\neg p \vee \xi')$, as required. The second case $\varrho(p) = 0$ follows analogously by using $(I_{1\mathrm{L}})$. We now prove (I_2). Assume $\varrho \vDash \{p \vee \xi, \neg p \vee \xi', \psi\}$. If $\varrho(p) = 1$, then $\varrho \vDash \xi'$, and thus by $(I_{2\mathrm{R}})$ we get $\varrho \vDash \eta'$. If $\varrho(p) = 0$, then $\varrho \vDash \xi$, and thus by $(I_{2\mathrm{L}})$ we get $\varrho \vDash \eta$. Putting together the two cases, we obtain $\varrho \vDash \eta \vee \eta'$, as required. □

1.8 Hilbert's proof system

Statement of Problem 1.8.1. As an example, provide a formal proof in Hilbert's system of the following tautology:

$$\varphi \to \varphi. \tag{B0}$$

□

Solution of Problem 1.8.1. Here is a sequence of theorems proving (B0):

1. $\varphi \to \varphi \to \varphi$, (from (A1))
2. $\varphi \to (\varphi \to \varphi) \to \varphi$, (from (A1))
3. $(\varphi \to (\varphi \to \varphi) \to \varphi) \to (\varphi \to \varphi \to \varphi) \to \varphi \to \varphi$, (from (A2))
4. $(\varphi \to \varphi \to \varphi) \to \varphi \to \varphi$, (from 2, 3 by (MP))
5. $\varphi \to \varphi$. (from 1, 4 by (MP))

□

Statement of Problem 1.8.3 "Soundness". Let φ be a formula. Then,

$$\Delta \vdash \varphi \quad \text{implies} \quad \Delta \vDash \varphi.$$

Hint: Proceed by complete induction on the length of proofs. □

Solution of Problem 1.8.3 "Soundness". Assume φ is obtained from a proof of length n. There are three cases. If it is an axiom, then one can check with the method of truth tables that (A1), (A2), and (A3) are tautologies. If it is a formula $\varphi \in \Delta$, then $\Delta \vDash \varphi$ is immediate. Finally, if φ is obtained by (MP) from formulas $\psi, \psi \to \varphi$, then the latter have having strictly shorter proofs than φ. By inductive assumption, $\Delta \vDash \{\psi, \psi \to \varphi\}$. By Problem 1.1.5 "Strong soundness of modus ponens", $\Delta \vDash \varphi$, as required. □

Statement of Problem 1.8.4 "Deduction theorem". Show that $\Delta \vdash \varphi \to \psi$ if, and only if, $\Delta \cup \{\varphi\} \vdash \psi$. □

Solution of Problem 1.8.4 "Deduction theorem". The "only if" direction is immediate: A proof of $\Delta \vdash \varphi \to \psi$ is also a proof of $\Delta \cup \{\varphi\} \vdash \varphi \to \psi$; by an extra application of (MP) to φ and $\varphi \to \psi$, we obtain $\Delta \cup \{\varphi\} \vdash \psi$, as required.

For the "if" direction, assume $\Delta \cup \{\varphi\} \vdash \psi$ has proof $\psi_1, \dots, \psi_n$ with $\psi_n \equiv \psi$. We prove the stronger claim: For every $1 \le i \le n$,

$$\Delta \vdash \varphi \to \psi_i.$$

(Clearly, when $i = n$ we obtain the "if" direction of the deduction theorem.) We proceed by complete induction on i. Assume the claim holds for every $j < i$ and we prove it for i. The formula ψ_i is either an axiom, a formula in $\Delta \cup \{\varphi\}$, or it is obtained by (MP) from some ψ_j, ψ_k with $j, k < i$. If ψ_i an axiom or in Δ, then we have $\Delta \vdash \varphi \to \psi_i$ by an application of (MP) to ψ_i and the axiom instance $\psi_i \to \varphi \to \psi_i$ of (A1). If $\psi_i \equiv \varphi$, then $\vdash \varphi \to \psi_i$ follows from (B0). Finally, assume ψ_i is obtained by (MP) from some ψ_j, ψ_k with $j, k < i$, where $\psi_k \equiv \psi_j \to \psi_i$. By a double application of the inductive assumption, we have $\Delta \vdash \varphi \to \psi_j$ and $\Delta \vdash \varphi \to \psi_j \to \psi_i$. By instantiating (A1) as $(\varphi \to \psi_j \to \psi_i) \to (\varphi \to \psi_j) \to \varphi \to \psi_i$ and with two applications of (MP), we obtain $\Delta \vdash \varphi \to \psi_i$, as required. □

Statement of Problem 1.8.5 "Derived theorems". Show how to derive the following tautologies in Hilbert's deduction system.

$$\bot \to \varphi, \tag{B1}$$

$$\varphi \to \neg\neg\varphi, \tag{B2}$$

$$\neg\varphi \to \varphi \to \psi, \tag{B3}$$

$$(\varphi \to \psi) \to (\neg\varphi \to \psi) \to \psi. \tag{B4}$$

$$\varphi \to \neg\psi \to \neg(\varphi \to \psi). \tag{B5}$$

Hint: Do use Problem 1.8.4 "Deduction theorem". □

Solution of Problem 1.8.5 "Derived theorems". For (B1), we start from $\bot, \neg\varphi \vdash \bot$, and thus by Problem 1.8.4 "Deduction theorem" we have $\bot \vdash \neg\varphi \to \bot$. By folding the definition of "$\neg$", we equivalently have $\bot \vdash \neg\neg\varphi$. By (A3) and (MP), we have $\bot \vdash \varphi$, and thus by Problem 1.8.4 "Deduction theorem" we have $\vdash \bot \to \varphi$, as required.

For (B2), we can rewrite it as $\varphi \to \neg\varphi \to \bot$. Consider $\Delta = \{\varphi, \neg\varphi\}$. Obviously $\Delta \vdash \varphi$ and $\Delta \vdash \neg\varphi$, and thus by (MP), $\Delta \vdash \bot$. Two applications of Problem 1.8.4 "Deduction theorem" conclude this case.

For (B3), take $\Delta = \{\varphi, \neg\varphi\}$. By Problem 1.8.4 "Deduction theorem" applied (twice) to (B2) we have $\Delta \vdash \bot$, and thus by (B1) and (MP) we have $\Delta \vdash \psi$. By two applications of Problem 1.8.4 "Deduction theorem" we obtain $\vdash \neg\varphi \to \varphi \to \psi$.

For (B4), take $\Delta = \{\varphi \to \psi, \neg\varphi \to \psi\}$. Then, $\Delta \cup \varphi, \neg\psi \vdash \bot$ (two applications of (MP)), and thus by Problem 1.8.4 "Deduction theorem" $\Delta \cup \neg\psi \vdash \neg\varphi$. Another application of (MP) yields $\Delta \cup \neg\psi \vdash \psi$, and yet one more gives $\Delta \cup \neg\psi \vdash \bot$. By Problem 1.8.4 "Deduction theorem", $\Delta \vdash \neg\neg\psi$, and thus by (A3) and (MP) we obtain $\Delta \vdash \psi$. We conclude by a further double application of Problem 1.8.4 "Deduction theorem".

Finally, for (B5), take $\Delta = \{\varphi, \neg\psi, \varphi \to \psi\}$. With a routine application of (MP) and Problem 1.8.4 "Deduction theorem" we obtain $\Delta \vdash \psi$, $\Delta \vdash \bot$, $\{\varphi, \neg\psi\} \vdash \neg(\varphi \to \psi)$, and finally $\vdash \varphi \to \neg\psi \to \neg(\varphi \to \psi)$. □

Statement of Problem 1.8.7 "Core lemma". Let φ be a formula and let $\bar{q} = (q_1, \dots, q_n)$ be its variables. For every truth valuation $\varrho : \bar{q} \to \{\top, \bot\}$,

$$\bar{q}^{\varrho} \vdash \varphi^{\varrho}.$$

Hint: Proceed by structural induction on φ. □

Solution of Problem 1.8.7 "Core lemma". In the base case, we have $\varphi \equiv q_i$. There are two subcases to consider.

1. If $\varrho(q_i) = \top$, then $q_i^{\varrho} \equiv q_i$. By (B0), $\vdash q_i \to q_i$, by Problem 1.8.4 "Deduction theorem" $q_i \vdash q_i$, and thus by Lemma 1.8.2 "Monotonicity" $\bar{q}^{\varrho} \vdash q_i$, as required.

2. If $\varrho(q_i) = \bot$, then $q_i^{\varrho} \equiv \neg q_i$, we can proceed as in the previous case.

In the first inductive case, we have $\varphi \equiv \neg\psi$. There are two subcases to consider.

1. Assume $\varrho(\psi) \equiv \top$. Consequently, $\psi^{\varrho} \equiv \psi$ and $\varphi^{\varrho} \equiv \neg\varphi \equiv \neg\neg\psi$. By (B2), $\vdash \psi \to \neg\neg\psi$. By the inductive assumption, $\bar{q}^{\varrho} \vdash \psi$, and thus by (MP), $\bar{q}^{\varrho} \vdash \neg\neg\psi$, as required.

2. Assume $\varrho(\psi) \equiv \bot$. Consequently, $\psi^{\varrho} \equiv \neg\psi$ and $\varphi^{\varrho} \equiv \varphi \equiv \neg\psi$. By the inductive assumption, $\bar{q}^{\varrho} \vdash \neg\psi$, as required.

In the second inductive case, we have $\varphi \equiv \psi \to \theta$. There are two subcases to consider.

1. Assume $\varrho(\theta) = \top$. Consequently, $\theta^{\varrho} \equiv \theta$ and $\varphi^{\varrho} \equiv \varphi$. By the inductive assumption, $\bar{q}^{\varrho} \vdash \theta$, and thus, by Lemma 1.8.2 "Monotonicity", $\bar{q}^{\varrho}, \psi \vdash \theta$. By Problem 1.8.4 "Deduction theorem", we have $\bar{q}^{\varrho} \vdash \psi \to \theta$, as required.

2. Assume $\varrho(\psi) = \bot$. Consequently, $\psi^{\varrho} \equiv \neg\psi$ and $\varphi^{\varrho} \equiv \varphi$. By the inductive assumption, $\bar{q}^{\varrho} \vdash \neg\psi$. By (B3), we have $\vdash \neg\psi \to \psi \to \varphi$, and thus by (MP) we have $\bar{q}^{\varrho} \vdash \psi \to \varphi$, as required.

3. Finally, assume $\varrho(\psi) = \top$ and $\varrho(\theta) = \bot$. Consequently, $\psi^{\varrho} \equiv \psi$, $\theta^{\varrho} \equiv \neg\theta$, and $\varphi^{\varrho} \equiv \neg\varphi$. By the inductive assumption (applied twice), we have $\bar{q}^{\varrho} \vdash \psi$ and $\bar{q}^{\varrho} \vdash \neg\theta$. By (B5), $\vdash \psi \to \neg\theta \to \neg(\psi \to \theta)$, and thus by (MP) applied twice, $\bar{q}^{\varrho} \vdash \neg(\psi \to \theta)$, as required. □

Statement of Problem 1.8.8 "Weak completeness theorem". Let φ be a formula. Then,

$$\vDash \varphi \quad \text{implies} \quad \vdash \varphi. \qquad \square$$

Solution of Problem 1.8.8 "Weak completeness theorem". Assume $\varrho(\varphi) = \top$ for every truth valuation ϱ. Let $q_1, \ldots, q_n$ be all propositional variables appearing in φ. We show by induction on $0 \le m \le n$ that,

$$q_1^{\varrho}, \ldots, q_{n-(m+1)}^{\varrho}, q_{n-m}^{\varrho} \vdash \varphi, \quad \text{for every } \varrho : \{q_1, \ldots, q_{n-m}\} \to \{\top, \bot\}. \tag{1.5}$$

This suffices since for $m = n$ it yields $\vdash \varphi$. The base case $m = 0$ follows from Problem 1.8.7 "Core lemma" (since $\varphi^{\rho} \equiv \varphi$). For the inductive step, we assume (1.5) and we prove

$$q_1^{\varrho}, \ldots, q_{n-(m+1)}^{\varrho} \vdash \varphi.$$

for an arbitrary truth valuation $\varrho : \{q_1, \ldots, q_{n-(m+1)}\} \to \{\top, \bot\}$. In other words, we show how to eliminate q^{ϱ}_{n-m} from the assumptions. We extend ϱ in two possible ways on q_{n-m} as

$$\varrho_\top = \varrho[q_{n-m} \mapsto \top] \qquad \text{and} \qquad \varrho_\bot = \varrho[q_{n-m} \mapsto \bot].$$

By the inductive assumption (1.5) applied on $\varrho_\top$ and on $\varrho_\bot$, we have $q_1^{\varrho_\top}, \ldots, q_{n-m}^{\varrho_\top} \vdash \varphi$, resp., $q_1^{\varrho_\bot}, \ldots, q_{n-m}^{\varrho_\bot} \vdash \varphi$. By Problem 1.8.4 "Deduction theorem" using the fact that $q_{n-m}^{\varrho_\top} \equiv q_{n-m}$ and $q_{n-m}^{\varrho_\bot} \equiv \neg q_{n-m}$, and that $\varrho_\top, \varrho_\bot$ agree with ϱ on the first $n-(m+1)$ variables, we have

$$q_1^{\varrho}, \ldots, q^{\varrho}_{n-(m+1)} \vdash q_{n-m} \to \varphi \qquad \text{and} \qquad q_1^{\varrho}, \ldots, q^{\varrho}_{n-(m+1)} \vdash \neg q_{n-m} \to \varphi.$$

By (B4), we have $\vdash (q_{n-m} \to \varphi) \to (\neg q_{n-m} \to \varphi) \to \varphi$, and thus, by two applications of (MP), we get $q_1^{\varrho}, \ldots, q^{\varrho}_{n-(m+1)} \vdash \varphi$, as required. □

Statement of Problem 1.8.9 "Strong completeness theorem". Let φ be a formula and let Δ be a set of formulas (possibly infinite). Then,

$$\Delta \vDash \varphi \quad \text{implies} \quad \Delta \vdash \varphi.$$

Hint: Use Problem 1.8.8 "Weak completeness theorem" and Problem 1.5.2. □

Solution of Problem 1.8.9 "Strong completeness theorem". Assume $\Delta \vDash \varphi$. By Problem 1.5.2, there exists a finite subset $\Gamma = \{\varphi_1, \ldots, \varphi_n\} \subseteq_{\text{fin}} \Delta$ s.t. $\Gamma \vDash \varphi$. By n applications of Problem 1.1.3 "Semantic deduction theorem", $\vDash \varphi_1 \to \cdots \to \varphi_n \to \varphi$. By Problem 1.8.8 "Weak completeness theorem", $\vdash \varphi_1 \to \cdots \to \varphi_n \to \varphi$, and thus, by n applications of Problem 1.8.4 "Deduction theorem", $\Gamma \vdash \varphi$. By Lemma 1.8.2 "Monotonicity", we have $\Delta \vdash \varphi$, as required. □

1.9 Intuitionistic propositional logic

1.9.1 Gentzen's natural deduction

Statement of Problem 1.9.1. As a warm-up, prove the following intuitionistic tautologies using natural deduction:

$$
\begin{aligned}
&p \to \neg\neg p,\\
&\neg(p \vee q) \to \neg p \wedge \neg q,\\
&\neg p \wedge \neg q \to \neg(p \vee q),\\
&\neg p \vee \neg q \to \neg(p \wedge q).
\end{aligned}
$$
□

Statement of Problem 1.9.2. Is intuitionistic propositional logic monotonic, in the sense that $\Delta \vdash_{\mathrm{ND}} \varphi$ and $\Gamma \supseteq \Delta$ imply $\Gamma \vdash_{\mathrm{ND}} \varphi$? □

Solution of Problem 1.9.2. Yes, intuitionistic propositional logic is monotonic. This can be proved by structural induction on proof trees. The base case is proved by observing that the axiom rule is monotonic. The inductive case follows directly by the induction hypothesis. □

1.9.2 Kripke models

Statement of Problem 1.9.3. Show that φ is a classical tautology if, and only if, $\mathcal{K} \vDash \varphi$ holds for every Kripke model with just $|W| = 1$ possible world. □

Solution of Problem 1.9.3. For the "if" direction, assume that φ is a classical tautology, and consider an arbitrary one-world Kripke model $\mathcal{K} = (\{w\}, \leq, \vDash)$. For every propositional variable $p \in Z$, either $w \vDash p$ or $w \nvDash p$. Since $\mathcal{K}$ has only one possible world w, in the latter case we even have $w \vDash \neg p$, and thus $\mathcal{K}$ behaves "classically". With this observation we can define the corresponding truth valuation $\varrho_{\mathcal{K}} : Z \to \{0, 1\}$ as follows:

$$\varrho_{\mathcal{K}}(p) = \begin{cases} 1 & \text{if } w \vDash p, \\ 0 & \text{if } w \vDash \neg p. \end{cases}$$

One can show by structural induction on formulas the following correspondence between truth table semantics and Kripke semantics (details omitted):

$$[\![\varphi]\!]_{\varrho\mathcal{K}} = 1 \quad \text{if, and only if,} \quad w \vDash \varphi. \tag{1.6}$$

Since φ is a classical tautology, $[\![\varphi]\!]_{\varrho\mathcal{K}} = 1$, and thus $w \vDash \varphi$, as required.

For the "only if" direction, assume that φ holds in every one-world Kripke model $\mathcal{K}$ as above, and consider an arbitrary truth valuation $\varrho : Z \to \{0,1\}$. We can define a corresponding one-world Kripke model

$$\mathcal{K}_\varrho = (\{w\}, \leq, \vDash),$$

where $\leq$ is the identity relation $\{(w,w)\}$, and $w \vDash p$ if, and only if, $\varrho(p) = 1$. Since there is only one world, $w \vDash \neg p$ if, and only if, $\varrho(p) = 0$ and, inductively (as in (1.6)), $w \vDash \varphi$ if, and only if, $[\![\varphi]\!]_\varrho = 1$. Since $\mathcal{K}_\varrho \vDash \varphi$ by assumption, we conclude $[\![\varphi]\!]_\varrho = 1$, as required. □

Statement of Problem 1.9.4. Show that the satisfiability relation "$\vDash$" is *monotonic* on all propositional formulas:

$$w \vDash \varphi \text{ and } w \leq w' \quad \text{implies} \quad w' \vDash \varphi.$$

Hint: Proceed by structural induction on formulas. □

Solution of Problem 1.9.4. The base case is provided by the definition of $\vDash$. The other cases follow by induction on the structure of formulas. □

Statement of Problem 1.9.5 "Soundness of intuitionistic propositional logic". Show that the rules of natural deduction are *sound* w.r.t. Kripke models, in the sense that, for every set of formulas Γ and formula φ of propositional logic,

$$\Gamma \vdash_{\mathrm{ND}} \varphi \quad \text{implies} \quad \Gamma \vDash \varphi.$$

Hint: Use induction on proof trees. □

Statement of Problem 1.9.6 "Completeness of intuitionistic propositional logic". Show that the rules of natural deduction are *complete* w.r.t. Kripke models, in the sense that, for every set of formulas Γ and formula φ of propositional logic,

$$\Gamma \vDash \varphi \quad \text{implies} \quad \Gamma \vdash_{\mathrm{ND}} \varphi. \qquad \square$$

Statement of Problem 1.9.7. Show that the following formulas are not theorems of intuitionistic propositional logic by providing Kripke models as counterexamples:

1. The law of excluded middle: $\varphi_1 \equiv p \vee \neg p$.
2. *Peirce's formula*: $\varphi_2 \equiv ((p \to q) \to p) \to p$.
3. One of De Morgan's laws: $\varphi_3 \equiv \neg(p \wedge q) \to (\neg p \vee \neg q)$.

Can one find Kripke models *with one state* in which the formulas above are not enforced? $\square$

Solution of Problem 1.9.7. The general approach showing that a formula φ is not provable in natural deduction is to build a Kripke counter-model $\mathcal{K}$ with a possible world w in $\mathcal{K}$ s.t. $w \nvDash \varphi$. If to the contrary $\vdash_{\mathrm{ND}} \varphi$, then by Problem 1.9.5 "Soundness of intuitionistic propositional logic" we would have $w \vDash \varphi$, which is a contradiction. We now proceed to construct counter-models to the formulas $\varphi_1, \varphi_2, \varphi_3$ above.

The law of excluded middle φ_1 is not forced by the model $\mathcal{K}_2$ consisting of two distinct possible worlds $w_0 \leq w_1$ s.t. p does not hold initially $[\![w_0]\!] = \varnothing$ and p holds in one step $[\![w_1]\!] = \{p\}$. We have neither $w_0 \vDash p$ (by construction) nor $w_0 \vDash \neg p$ (which would mean that p can never hold in the future, which is false since $w_1 \vDash p$). Thus, $w_0 \nvDash \varphi_1$.

Pierce's formula φ_2 is not forced by the same model $\mathcal{K}_2$ as above (where q is false in w_0 and w_1), albeit the reasoning is more involved. Assume that φ_2 is forced by $\mathcal{K}_2$, and we derive a contradiction. (Incidentally, this step in the reasoning is intuitionistically valid, because this is *what it means* to prove $\neg\psi \equiv \psi \to \bot$.) In particular, $w_0 \vDash \varphi_2$. Consequently, $w_0 \vDash (p \to q) \to p$ implies $w_0 \vDash p$. Since $w_0 \nvDash p$, we have $w_0 \nvDash (p \to q) \to p$. Since $w_1 \vDash p$, the only possibility is that $w_0 \vDash p \to q$ and $w_0 \nvDash p$. The first condition entails that, if $w_1 \vDash p$, then $w_1 \vDash q$. This is a contradiction since $w_1 \vDash p$ and $w_1 \nvDash q$ by construction.

Regarding φ_3, we consider the three-worlds Kripke model

$$\mathcal{K}_3 = (\{w_0, w_1, w_2\}, \leq, \vDash),$$

where $w_0 \leq w_1, w_2$ and w_1, w_2 are incomparable, initially neither p nor q hold $[\![w_0]\!] = \varnothing$, in the possible-world w_1 only p holds $[\![w_1]\!] = \{p\}$, and in the possible-world w_2 only q holds $[\![w_1]\!] = \{q\}$. We show that $w_0 \nvDash \varphi_3$. To the contrary, assume $w_0 \vDash \varphi_3$. Since $w_0 \vDash \neg(p \wedge q)$ (p and q never hold simultaneously in any possible world), we obtain $w_0 \vDash \neg p \vee \neg q$. However, the latter condition does not hold, since $w_0 \nvDash \neg p$ (as witnessed by w_1 where p holds) and $w_0 \nvDash \neg q$ (as witnessed by w_2 where q holds). This is the sought contradiction, as required.

There are no such counterexamples, since all the φ_i's above are classical tautologies, and by Problem 1.9.3 one-world Kripke models satisfy classical tautologies. □

Statement of Problem 1.9.8. In which class of Kripke models is the following formula φ satisfied?

$$\varphi \equiv (p \to q) \vee (q \to p). \qquad \square$$

Solution of Problem 1.9.8. We observe that, if $\mathcal{K}$ is *linearly ordered* (i.e., $\leq$ is a total order), then either 1) p becomes true before q possibly does, or 2) q becomes true before p possibly does, or 3) p, q are never true. In case 1), $\mathcal{K} \vDash q \to p$, in case 2), $\mathcal{K} \vDash p \to q$, and in case 3) we even have both conditions $\mathcal{K} \vDash p \to q$ and $\mathcal{K} \vDash q \to p$. Thus $\mathcal{K} \vDash \varphi$ holds when $\mathcal{K}$ is linearly ordered.

This is optimal. We construct a non-linearly ordered Kripke model $\mathcal{K} = (\{w_0, w_1, w_2, w_3\}, \leq, \vDash)$ where φ is not satisfied $w_0 \nvDash \varphi$. Let $w_0 \leq w_i \leq w_3$ for $i \in \{1, 2\}$, and let w_1, w_2 be incomparable. Initially neither p nor q holds $[\![w_0]\!] = \varnothing$. In one possible future only p holds $[\![w_1]\!] = \{p\}$, in the other possible future only q holds $[\![w_2]\!] = \{q\}$, and then these two futures join again as to make both p and q hold $[\![w_3]\!] = \{p, q\}$. It can now be checked directly that $w_0 \nvDash \varphi$. □

Statement of Problem 1.9.9 "Disjunction property". Prove that natural deduction has the following *disjunction property*:

$$\vdash_{\mathrm{ND}} \varphi \vee \psi \quad \text{if, and only if,} \quad \vdash_{\mathrm{ND}} \varphi \text{ or } \vdash_{\mathrm{ND}} \psi.$$

Hint: Use Problem 1.9.6 "Completeness of intuitionistic propositional logic". □

Solution of Problem 1.9.9 "Disjunction property". The "if" direction is obvious. For the "only if" direction, assume by way of contradiction that $\vdash_{\mathrm{ND}} \varphi \vee \psi$, $\nvdash_{\mathrm{ND}} \varphi$, and $\nvdash_{\mathrm{ND}} \psi$. By two applications of the contrapositive of Problem 1.9.6 "Completeness of intuitionistic propositional logic" there are two Kripke models $\mathcal{K}_1$ and $\mathcal{K}_2$ with possible worlds w_1, resp., w_2, s.t. $\mathcal{K}_1, w_1 \nvDash \varphi$ and $\mathcal{K}_2, w_2 \nvDash \psi$. We can assume w.l.o.g. that $\mathcal{K}_1$ and $\mathcal{K}_2$ are disjoint (no world in common). Since the relation $w_1 \vDash \_$ depends only on worlds $w' \geq w_1$, we can assume w.l.o.g. that w_1 is the least element of $\mathcal{K}_1$ (i.e., its root); similarly, w_2 is the least element of $\mathcal{K}_2$. Consider now the model $\mathcal{K}$ obtained by taking the disjoint union of $\mathcal{K}_1, \mathcal{K}_2$ and adjoining a fresh least possible world $w \leq w_1, w_2$ satisfying no propositional variable $[\![w]\!] = \varnothing$. Clearly we still have $\mathcal{K}, w_1 \nvDash \varphi$ and $\mathcal{K}, w_2 \nvDash_{\mathcal{K}} \psi$ in $\mathcal{K}$, and thus, by Problem 1.9.4, we have as well $\mathcal{K}, w \nvDash \varphi$ and $\mathcal{K}, w \nvDash \psi$. By the definition of satisfaction "$\vDash$" we conclude $\mathcal{K}, w \nvDash \varphi \vee \psi$, and, by Problem 1.9.5 "Soundness of intuitionistic propositional logic", $\nvdash_{\mathrm{ND}} \varphi \vee \psi$, which is a contradiction. □

Chapter 2

First-order predicate logic

2.1 Definability

2.1.1 Real numbers

Statement of Problem 2.1.2. Show that one can define the natural order "$\leq$" on $\mathbb{R}^2$ as a formula $\varphi(x, y)$ of first-order logic of two free variables x, y. $\square$

Solution of Problem 2.1.2. We use the fact that squaring produces nonnegative reals:

$$\varphi(x, y) \equiv \exists z \,.\, x = y + z * z. \qquad \square$$

Statement of Problem 2.1.3 "Periodicity". Extend the signature of the reals with an arbitrary function of one variable $f : \mathbb{R} \to \mathbb{R}$. Show that one can express as a first-order logic sentence φ that f is a periodic function whose smallest strictly positive period is 1. $\square$

Solution of Problem 2.1.3 "Periodicity". Let $\varphi(x)$ be a first-order formula of one free variable saying that x is a period of f:

$$\varphi(x) \equiv \forall y \,.\, f(y + x) = f(y).$$

The required property is expressed as

$$\varphi(1) \wedge \forall x \,.\, x > 0 \wedge \varphi(x) \to x \geq 1.$$

Strictly speaking, "$x > 0$" and "$x \geq 1$" are not atomic formulas in the signature we are considering. However, they are first-order expressible as we have seen in Problem 2.1.2. □

Statement of Problem 2.1.4 "Continuity and uniform continuity". Express that f is a continuous, resp., uniformly continuous function. □

Solution of Problem 2.1.4 "Continuity and uniform continuity". We express continuity as $\lim_{y \to x} f(y) = f(x)$ for every x:

$$\varphi \ \equiv \ \forall x \,.\, \forall \varepsilon > 0 \,.\, \exists \delta > 0 \,.\, \forall y \,.\, |y - x| \leq \delta \to |f(y) - f(x)| \leq \varepsilon.$$

We have used the following custom notational conventions:

$$\begin{array}{ll} \forall \varepsilon > 0 \,.\, \psi & \text{stands for } \forall \varepsilon \,.\, \varepsilon > 0 \to \psi, \text{ and} \\ \exists \delta > 0 \,.\, \psi & \text{stands for } \exists \delta \,.\, \delta > 0 \wedge \psi. \end{array}$$

Strictly speaking, the subtraction operation "$\_ - \_$" and the absolute value function "$|\_|$" are not in the signature we are considering. However, we can rewrite "$|y - x| \leq \delta$" as

$$(y \geq x \to y \leq \delta + x) \wedge (y < x \to x \leq \delta + y).$$

Uniform continuity is the stronger property obtained by pushing the "$\forall x$" quantifier inside the formula:

$$\psi \ \equiv \ \forall \varepsilon > 0 \,.\, \exists \delta > 0 \,.\, \forall x, y \,.\, |y - x| \leq \delta \to |f(y) - f(x)| \leq \varepsilon. \qquad \square$$

Statement of Problem 2.1.5 "Differentiability". With the same setting as in Problem 2.1.3 "Periodicity", write a formula of first-order logic $\varphi(x)$ with one free variable x expressing that f is differentiable in x. □

Solution of Problem 2.1.5 "Differentiability". Let $g(x, \delta) = \frac{f(x+\delta) - f(x)}{\delta}$. We express that $\lim_{\delta \to 0} g(x, \delta)$ exists:

$$\varphi(x) \ \equiv \ \exists y \,.\, \forall \varepsilon > 0 \,.\, \exists \delta > 0 \,.\, \forall (0 < z < \delta) \,.\, |g(z, \delta) - y| \leq \varepsilon.$$

As in Problem 2.1.4 "Continuity and uniform continuity", we can rewrite "$|g(z, \delta) - y| \leq \varepsilon$" in order to use only symbols from the signature. □

2.1.2 Cardinality constraints

Statement of Problem 2.1.6 "Cardinality constraints I". For every n, construct a sentence $\varphi_{\geq n}$ of first-order logic with equality, s.t. the following holds for every model $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$:

$$\mathfrak{A} \models \varphi_{\geq n} \qquad \text{if, and only if,} \qquad |A| \geq n.$$

Can $\varphi_{\geq n}$ be a universal sentence? □

Solution of Problem 2.1.6 "Cardinality constraints I". Let $\varphi_{\geq n}$ be the existential sentence

$$\varphi_{\geq n} \;\equiv\; \exists x_1 \cdots \exists x_n \,.\, \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j .$$

It is clear that $\varphi_{\geq n}$ satisfies the required property. There is no universal sentence ψ with the same property, since for any universal sentence ψ, $\mathfrak{A} \models \psi$ implies $\mathfrak{B} \models \psi$ for every submodel $\mathfrak{B}$ of $\mathfrak{A}$, which in particular implies that we can take $\mathfrak{B}$ with less than n elements. □

Statement of Problem 2.1.7 "Cardinality constraints II". This exercise is dual to Problem 2.1.6 "Cardinality constraints I". For every n, construct a sentence $\varphi_{\leq n}$ of first-order logic with equality, s.t. the following holds for every model $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$:

$$\mathfrak{A} \models \varphi_{\leq n} \qquad \text{if, and only if,} \qquad |A| \leq n.$$

Can $\varphi_{\leq n}$ be an existential sentence? □

Solution of Problem 2.1.7 "Cardinality constraints II". Let $\varphi_{\geq n}$ any (existential) sentence satisfying the requirements of Problem 2.1.6 "Cardinality constraints I". Then, $\varphi_{\leq n} \;\equiv\; \neg\varphi_{\geq n+1}$ is a universal sentence constraining the cardinality of the model to be $\ngeq n+1$, i.e., $\leq n$ as required. There is no existential such $\varphi_{\leq n}$ because any finite model of an existential sentence can be extended to a model of larger finite cardinality by adding spurious elements. □

2.1.3 Characteristic sentences

Statement of Problem 2.1.8 "Characteristic sentences". Show that for each *finite* structure $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_m^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$ there exists a first-order sentence $\delta_{\mathfrak{A}}$, called the *characteristic sentence* of $\mathfrak{A}$, s.t., for all structures $\mathfrak{B}$,

$$\mathfrak{B} \models \delta_{\mathfrak{A}} \qquad \text{if, and only if,} \qquad \mathfrak{B} \cong \mathfrak{A}.$$

In other words, $\delta_{\mathfrak{A}}$ uniquely determines $\mathfrak{A}$ up to isomorphism. □

Solution of Problem 2.1.8 "Characteristic sentences". W.l.o.g. we prove the claim for a relational structure $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}})$ with domain $A = \{a_1, \ldots, a_m\}$. For every relation $R_i^{\mathfrak{A}} \subseteq A^{n_i}$, let its characteristic sentence be

$$\begin{aligned}\delta_i(x_1, \ldots, x_m) \;\equiv\; & \bigwedge\{R_i(x_{j_1}, \ldots, x_{j_{n_i}}) \mid (a_{j_1}, \ldots, a_{j_{n_i}}) \in R_i^{\mathfrak{A}}\} \wedge \\ & \bigwedge\{\neg R_i(x_{j_1}, \ldots, x_{j_{n_i}}) \mid (a_{j_1}, \ldots, a_{j_{n_i}}) \in A^{n_i} \smallsetminus R_i^{\mathfrak{A}}\}.\end{aligned}$$

The sentence $\delta_{\mathfrak{A}}$ states that there are precisely n pairwise distinct elements in the model $x_1, \ldots, x_n$ satisfying precisely all relations $R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}}$:

$$\delta_{\mathfrak{A}} \;\equiv\; \exists x_1 \cdots \exists x_m \,.\, \bigwedge_{1 \le i < j \le m} x_i \neq x_j \wedge \forall y \,.\, \bigvee_{1 \le i \le m} y = x_i \wedge \bigwedge_{1 \le i \le n} \delta_i(x_1, \ldots, x_m).$$

□

2.1.4 Miscellanea

Statement of Problem 2.1.9 "Binary trees". In this problem we consider finite trees $\mathfrak{T}$ where each vertex can have zero, one, or two children. The signature consists of two binary relational symbols L and R: $L(x, y)$ means that y is the left son of x, and $R(x, y)$ for the right son; there is always at most one left son, and at most one right son. Prove that, for any natural number $n \in \mathbb{N}$, one can express that $\mathfrak{T}$ is the complete binary tree of depth n (i.e., one where all leaves are at depth n and all other nodes have exactly two children) as a first-order logic sentence φ_n of size $O(n)$ using only two variables x and y (which can be re-quantified as often as necessary). □

Solution of Problem 2.1.9 "Binary trees". Let $\psi_n(x)$ express that x is located at depth n from the root, and similarly for $\xi_n(y)$. In the base case, we have

$$\begin{aligned}\psi_0(x) &\equiv \neg\exists y\,.\,L(y,x)\vee R(y,x), \text{ and}\\ \xi_0(y) &\equiv \neg\exists x\,.\,L(x,y)\vee R(x,y),\end{aligned}$$

and in the inductive case,

$$\begin{aligned}\psi_{n+1}(x) &\equiv \exists y\,.\,(L(y,x)\vee R(y,x))\wedge\xi_n(y), \text{ and}\\ \xi_{n+1}(y) &\equiv \exists x\,.\,(L(x,y)\vee R(x,y))\wedge\psi_n(x).\end{aligned}$$

Finally, we define

$$\varphi_n \equiv \forall x\,.\,(\exists y\,.\,L(x,y))\wedge(\exists y\,.\,R(x,y))\vee\psi_n(x). \qquad\square$$

Statement of Problem 2.1.10 "Conway's "Game of Life"". Conway's *game of life* is played on the bidimensional grid

$$\mathfrak{A} = (\mathbb{Z}\times\mathbb{Z}, \le_1, \le_2, U),$$

where $U \subseteq \mathbb{Z}\times\mathbb{Z}$ is a unary relation (on $\mathfrak{A}$) denoting the *alive* cells (cells in $(\mathbb{Z}\times\mathbb{Z})\smallsetminus U$ are *dead*), and $(x_1,x_2)\le_i(y_1,y_2)$ holds iff $x_i\le y_i$, for $i\in\{1,2\}$. The neighbours of a cell (x,y) are the eight cells $(x',y')\ne(x,y)$ satisfying $|x-x'|\le 1$ and $|y-y'|\le 1$. At each discrete time step, the status of all cells in the grid changes simultaneously, according to the following rules:

- a dead cell with exactly three alive neighbours becomes alive;
- an alive cell with two or three living neighbours remains alive;
- all other cells remain or become dead.

Prove that, for any $k\in\mathbb{N}$, there is a formula $\varphi_k(x)$ of one free variable s.t. $\mathfrak{A}, x : a \vDash \varphi$ if cell a is alive after the k-th step of the game of life, starting from the position described by U. $\square$

Solution of Problem 2.1.10 "Conway's "Game of Life"". As a warm-up, we observe that we can express $x =_i y$ as $x \le_i y \wedge y \le_i x$, and $x <_i y$ as $x \le_i y \wedge \neg(x =_i y)$. We can express $x - y \le_i 1$ as

$$x =_i y \;\vee\; y <_i x \wedge \forall (z <_i x)\,.\,z \le_i y,$$

and $|x-y| \leq_i 1$ as

$$y \leq_i x \wedge x - y \leq_i 1 \ \vee \ x \leq_i y \wedge y - x \leq_i 1.$$

We can write a formula of two free variables $\varphi(x,y) \equiv x \neq y \wedge |x-y| \leq_1 1 \wedge |x-y| \leq_2 1$ stating that x and y are neighbours. We can say that x has exactly three alive neighbours at time k as

$$\begin{aligned}\psi_{k,3}(x) \ \equiv\ & \exists y_1, y_2, y_3 \,.\, y_1 \neq y_2 \wedge y_1 \neq y_3 \wedge y_2 \neq y_3 \wedge \\ & \varphi_k(y_1) \wedge \varphi_k(y_2) \wedge \varphi_k(y_3) \wedge \\ & \varphi(x,y_1) \wedge \varphi(x,y_2) \wedge \varphi(x,y_3) \wedge \\ & \forall y \,.\, \varphi_k(y) \wedge \varphi(x,y) \to y = y_1 \vee y = y_2 \vee y = y_3.\end{aligned}$$

A formula $\psi_{k,2,3}(x)$ stating that x has two or three living neighbours can be written in a similar fashion.

We are now ready to define $\varphi_k(x)$. We proceed by induction on k. For the base case $k = 0$ we have directly $\varphi_0(x) \equiv U(x)$. For the inductive case $k > 0$, we have

$$\varphi_k(x) \ \equiv\ \neg\varphi_{k-1}(x) \wedge \psi_{k-1,3}(x) \ \vee\ \varphi_{k-1}(x) \wedge \psi_{k-1,2,3}(x). \qquad \square$$

2.2 Normal forms

Statement of Problem 2.2.1 "Negation normal form". A formula φ is in *negation normal form* (NNF) if negation is only applied to atomic formulas, i.e., for every subformula of the form $\neg\psi$, $\psi \equiv R_j(\cdots)$ is atomic. Show that each first-order logic formula can be transformed into an equivalent one in NNF. $\square$

Solution of Problem 2.2.1 "Negation normal form". We use the following tautologies to transform the given formula into NNF. Each tautology must be read as a left-to-right rewrite rule. First, remove the connectives "$\to$" and "$\leftrightarrow$" by expanding their definition:

$$\begin{aligned}(\varphi \leftrightarrow \psi) \ &\leftrightarrow\ (\varphi \to \psi) \wedge (\psi \to \varphi), \\ (\varphi \to \psi) \ &\leftrightarrow\ \neg\varphi \vee \psi.\end{aligned}$$

Then, push negations inside to the atomic formulas using De Morgan's laws:

$$\begin{aligned} \neg(\varphi \land \psi) &\leftrightarrow \neg\varphi \lor \neg\psi, \\ \neg(\varphi \lor \psi) &\leftrightarrow \neg\varphi \land \neg\psi, \\ \neg\forall x \,.\, \varphi &\leftrightarrow \exists x \,.\, \neg\varphi, \\ \neg\exists x \,.\, \varphi &\leftrightarrow \forall x \,.\, \neg\varphi. \end{aligned}$$ □

Statement of Problem 2.2.2 "Prenex normal form". A formula φ is in *prenex normal form* (PNF) if it is of the form

$$\varphi \equiv Q_1 x_1 \cdots Q_n x_n \,.\, \psi$$

where $Q_i \in \{\forall, \exists\}$ and ψ is quantifier-free. Show that for each first-order logic formula there is an equivalent one in PNF. □

Solution of Problem 2.2.2 "Prenex normal form". By Problem 2.2.1 "Negation normal form", we assume the formula is in NNF. We transform the formula to PNF by pulling out the quantifiers:

$$\begin{aligned} (\forall x \,.\, \varphi) \land \psi &\leftrightarrow \forall x \,.\, \varphi \land \psi, && (\text{if } x \notin \mathsf{fv}(\psi)) \\ (\forall x \,.\, \varphi) \lor \psi &\leftrightarrow \forall x \,.\, \varphi \lor \psi, && (\text{if } x \notin \mathsf{fv}(\psi)) \\ (\exists x \,.\, \varphi) \land \psi &\leftrightarrow \exists x \,.\, \varphi \land \psi, && (\text{if } x \notin \mathsf{fv}(\psi)) \\ (\exists x \,.\, \varphi) \lor \psi &\leftrightarrow \exists x \,.\, \varphi \lor \psi. && (\text{if } x \notin \mathsf{fv}(\psi)) \end{aligned}$$

Sometimes fresh variable rename is necessary in order to allow the quantifiers to be pulled out:

$$\forall x \,.\, \varphi \leftrightarrow \forall y \,.\, \varphi[x \mapsto y]. \qquad (\text{if } y \notin \mathsf{fv}(\varphi)).$$ □

Statement of Problem 2.2.3. Show that there exists a sentence of first-order logic φ s.t. for any logically equivalent sentence ψ in PNF, ψ has greater quantifier rank: $\mathsf{rank}(\psi) > \mathsf{rank}(\varphi)$. □

Solution of Problem 2.2.3. Let U be a unary symbol and consider the following rank 1 sentence:

$$\varphi \equiv (\exists x \,.\, U(x)) \land \exists x \,.\, \neg U(x).$$

By way of contradiction, assume that a logically equivalent formula ψ of $\mathsf{rank}(\psi) = 1$ exists. The formula ψ must be either of the form $\exists x \,.\, \xi(x)$ or $\forall x \,.\, \xi(x)$, with ξ quantifier-free. Observe that φ is true in a model with two elements, and has no one-element model. If $\exists x \,.\, \xi(x)$ is true in a two-element model $\mathfrak{A} = (\{a, b\}, U^{\mathfrak{A}})$ under valuation $x : a$, then it is also true in the one-element submodel $\mathfrak{A}|_{\{a\}}$. Hence this sentence cannot be equivalent to φ. If $\forall x \,.\, \xi(x)$ is true in a two-element model $\mathfrak{A}$ as above, then it is also true in both its single-element submodels $\mathfrak{A}|_{\{a\}}$ and $\mathfrak{A}|_{\{b\}}$, because truth of universal sentences is preserved under submodels. Hence this sentence cannot be equivalent to φ, either. □

Statement of Problem 2.2.4. Fix a finite signature Σ. Is there a $k \in \mathbb{N}$ s.t. every first-order sentence φ over Σ is logically equivalent to a sentence of rank k? □

Solution of Problem 2.2.4. This is not the case. For a given finite signature Σ and fixed number of free variables $k \in \mathbb{N}$, there are only finitely many quantifier-free formulas up to logical equivalence. By Problem 2.2.2 "Prenex normal form", a sentence of size n and rank k can be written in PNF with rank $O(k \cdot n)$, and thus there are also finitely many sentences of rank k up to logical equivalence. It suffices to construct any infinite sequence of pairwise inequivalent sentences $\varphi_1, \varphi_2, \ldots$. For instance, one can take the empty signature $\Sigma = \varnothing$ and the cardinality lower-bound constraints from Problem 2.1.6 "Cardinality constraints I". □

2.3 Satisfaction relation

Statement of Problem 2.3.1. In which structures is the following formula of one free variable $\varphi(x) \equiv \exists y \,.\, y \neq x$ satisfied? And the closed formula $\psi \equiv \exists y \,.\, y \neq y$ obtained by "naive" substitution of y in place of x? □

Solution of Problem 2.3.1. The first formula $\varphi(x)$ is satisfied precisely in those structures containing at least two elements. The second formula ψ is not satisfied in any structure, i.e., it is not satisfiable. This shows that in order to preserve the meaning of a formula substitution must avoid capturing free variables. □

Statement of Problem 2.3.2. Consider the formula

$$\varphi \equiv R(x, f(x)) \to \forall x \exists y \,.\, R(f(y), x).$$

Construct two structures $\mathfrak{A} = (A, f^{\mathfrak{A}}, R^{\mathfrak{A}})$ and $\mathfrak{B} = (B, f^{\mathfrak{B}}, R^{\mathfrak{B}})$ and valuations $\rho^{\mathfrak{A}}, \rho^{\mathfrak{B}}$ s.t. $\mathfrak{A}, \rho^{\mathfrak{A}} \models \varphi$ and $\mathfrak{B}, \rho^{\mathfrak{B}} \not\models \varphi$. □

Solution of Problem 2.3.2. Take $\mathfrak{A} = (\{a\}, \mathsf{id}^{\mathfrak{A}}, \mathsf{id}^{\mathfrak{A}}), \rho^{\mathfrak{A}}(x) = a$ and $\mathfrak{B} = (\mathbb{N}, (+1)^{\mathfrak{B}}, <^{\mathfrak{B}}), \rho^{\mathfrak{B}}(x) = 0$. □

Statement of Problem 2.3.3. For each one of the following formulas, check whether it is 1) a tautology, and 2) satisfiable:

$$\begin{aligned}
\varphi_1 &\equiv (\forall x \,.\, P(x) \vee Q(f(x))) \to \forall x \exists y \,.\, P(x) \vee Q(y),\\
\varphi_2 &\equiv (\forall x \exists y \,.\, P(x) \vee Q(y)) \to \forall x \,.\, P(x) \vee Q(f(x)),\\
\varphi_3 &\equiv (\forall x \,.\, P(x) \vee Q(f(x))) \wedge \exists x \forall y \,.\, \neg P(x) \wedge \neg Q(y),\\
\varphi_4 &\equiv (\exists x \,.\, (\forall y \,.\, Q(y)) \to P(x)) \to \exists x \,.\, Q(x) \to P(x).
\end{aligned}$$
□

Solution of Problem 2.3.3. The formula φ_1 is a tautology, hence satisfiable (the l.h.s. is the skolemisation of the r.h.s.). The formula φ_2 (which is the converse of φ_1) is not a tautology: suppose P is everywhere false; then the l.h.s. says that $Q(y)$ is true for some y, and the r.h.s. says that Q holds on the codomain of f, but there are choices of f s.t. $Q(f(x))$ is false and $f(x) \neq y$. However, φ_2 is satisfiable: It suffices to choose a model where the l.h.s. does not hold, such as Q never holds and P holds somewhere. The formula φ_3 is the complement of φ_1 and thus not satisfiable (and hence not a tautology). The formula φ_4 is a tautology (push all quantifiers inside). □

Statement of Problem 2.3.4. Show that the following formula has only infinite models:

$$\varphi \equiv \forall x \,.\, \exists y \,.\, R(x, y) \wedge \forall x \,.\, \neg R(x, x) \wedge \forall x, y, z \,.\, R(x, y) \wedge R(y, z) \to R(x, z).$$
□

Solution of Problem 2.3.4. Let $\mathfrak{A} = (A, R^{\mathfrak{A}})$ be a model of φ. Then, $R^{\mathfrak{A}} \subseteq A \times A$ is a total, irreflexive, and transitive relation. We show, by induction on n, that A contains an R-chain of $n+1$ pairwise distinct elements, for every $n \in \mathbb{N}$:

$$a_0 \; R \; a_1 \; R \; a_2 \cdots a_{n-1} \; R \; a_n.$$

For $n = 0$, the trivial chain composed just of a_0 exists because models are nonempty. Assume we have a chain of size $n+1$ as above, and we show how to extend it to a chain of size $n+2$. By totality, there exists an element a_{n+1} s.t. $a_n \; R \; a_{n+1}$. Consider any a_i with $0 \leq i \leq n$. By transitivity, $a_i \; R \; a_{n+1}$, and by irreflexivity $a_i \neq a_{n+1}$. Thus, all the elements of the new chain are pairwise distinct. Thus, A contains arbitrarily large chains of pairwise distinct elements, and therefore must be infinite. □

Statement of Problem 2.3.5. For each of the following signatures, write a sentence that has only infinite models:

1. One unary functional symbol and no relational symbols.
2. One binary relation symbol and no function symbols. □

Solution of Problem 2.3.5.

1. We express that f is one-to-one, but not onto: $\forall x, y \, . \, (f(x) = f(y) \to x = y) \wedge \exists x \, . \, \forall y \, . \, x \neq f(y)$.
2. We can express that $R(x, y)$ is functional and fall back in the previous case. Alternatively, we can express that R is a partial order without maximal elements. □

Statement of Problem 2.3.6. Show that the following formula is not a tautology:

$$\varphi \;\equiv\; (\forall x \forall y \, . \, f(x) = f(y) \to x = y) \to \forall x \exists y \, . \, f(y) = x.$$

Does its negation have a finite model? □

Solution of Problem 2.3.6. The premise says that f is injective and the conclusion that f is surjective. In any model $\mathfrak{A} = (A, f^{\mathfrak{A}})$ of $\neg\varphi$ the function $f^{\mathfrak{A}} : A \to A$ is injective but not surjective. Consequently, the codomain of $f^{\mathfrak{A}}$ is a strict subset of A, i.e., $f^{\mathfrak{A}}(A) \subsetneq A$. Only infinite sets A admit an injection to a strict subset thereof. Thus, there are no finite models of $\neg\varphi$. □

Statement of Problem 2.3.7. Show that the following formula is not a tautology:

$$\varphi \ \equiv\ \exists x \exists y \exists u \exists v \,.\, (\neg(x = u) \vee \neg(y = v)) \wedge f(x, y) = f(u, v).$$

1. How many non-isomorphic finite models does $\neg\varphi$ have?

2. Is $\psi \ \equiv\ \varphi \vee \forall x \forall y \,.\, x = y$ a tautology? □

Solution of Problem 2.3.7. Let $\mathfrak{A} = (A, f^{\mathfrak{A}})$ be a structure. Then, $\mathfrak{A} \models \neg\varphi$ holds precisely when $f^{\mathfrak{A}} : A \times A \to A$ is injective. For instance, taking the one-element domain $A = \{a\}$ with $f^{\mathfrak{A}}(a, a) = a$ (uniquely defined by A) makes $f^{\mathfrak{A}}$ injective. More generally, if A is of finite cardinality $|A| = n > 0$, then the existence of an injection from $A \times A$ to A would imply $n^2 \leq n$, and this is possible only if $n = 1$. Thus, there are no other non-isomorphic finite models of $\neg\varphi$.

For the second point, ψ is still not a tautology, and by the discussion above any model of $\neg\psi$ must be infinite. For example, it suffices to consider $\mathfrak{A} = (\mathbb{N}, f^{\mathfrak{A}})$ where $f^{\mathfrak{A}}$ is any injection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$, such as the Cantor's pairing function $f^{\mathfrak{A}}(m, n) = \frac{(m+n)(m+n+1)}{2} + n$. □

Statement of Problem 2.3.8. Consider the set Δ consisting of the sentences

$$\begin{aligned}
&\exists x \exists y \,.\, x \neq y, \\
&\forall x \,.\, \neg E(x, x), \text{ and} \\
&\forall x \forall y \,.\, x \neq y \to \exists z \,.\, E(x, z) \wedge E(y, z).
\end{aligned}$$

What is the smallest possible number of edges in a graph $\mathfrak{A} = (A, E^{\mathfrak{A}})$ which is a model of Δ? □

Solution of Problem 2.3.8. Six. By the first condition there are at least two distinct vertices $a, b \in A$ in the graph. By the second condition the edge relation $E^{\mathfrak{A}}$ is irreflexive, i.e., there are no self-loops. By the third condition, distinct vertices a, b share a common neighbour c, which distinct by the previous condition. Thus A has at least three vertices, and by repeatedly applying the third condition we obtain six edges. □

Statement of Problem 2.3.9. Prove that each satisfiable *existential* sentence has both a finite and an infinite model. □

Solution of Problem 2.3.9. Let $\varphi \equiv \exists x_1 \cdots \exists x_n . \psi$ be an existential formula, with ψ quantifier-free. Consider first the case when the signature of φ consists only of relations $R_1, \ldots, R_m$. Let $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \ldots, R_m^{\mathfrak{A}})$ be a model of φ. There exist $a_1, \ldots, a_n \in A$ s.t.

$$\mathfrak{A}, x_1 : a_1, \ldots, x_n : a_n \vDash \psi.$$

Consequently,

$$\mathfrak{A}|_{\{a_1,\ldots,a_n\}}, x_1 : a_1, \ldots, x_n : a_n \vDash \psi,$$

and thus $\mathfrak{A}|_{\{a_1,\ldots,a_n\}}$ is a finite model of φ. Moreover, if B is any infinite set, then $\mathfrak{B} = (A \cup B, R_1^{\mathfrak{A}}, \ldots, R_m^{\mathfrak{A}})$ is an infinite model of φ.

Now let us consider the case when the signature of φ contains function symbols $f_1, \ldots, f_l$, and let $\mathfrak{A} = (A, f_1^{\mathfrak{A}}, \ldots, f_l^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_m^{\mathfrak{A}})$ be a model of φ, where $f_i^{\mathfrak{A}} : A^{\alpha_i} \to A$ and $R_j^{\mathfrak{A}} \subseteq A^{\beta_j}$. As before, there exist $a_1, \ldots, a_n \in A$ defining a valuation $\rho = (x_1 : a_1, \ldots, x_n : a_n)$ s.t.

$$\mathfrak{A}, \rho \vDash \psi.$$

There are two cases to consider, depending on whether $\mathfrak{A}$ is infinite or finite.

If $\mathfrak{A}$ is infinite, then we only need to create a finite model for φ. Let $t_1, \ldots, t_k$ be all terms appearing in ψ, and let $A' = \{[\![t_1]\!]_\rho^{\mathfrak{A}}, \ldots, [\![t_k]\!]_\rho^{\mathfrak{A}}\} \subseteq A$ be the finite set of all elements of A which are values of terms appearing in ψ under the valuation ρ. We assume w.l.o.g. that every variable x_i appears in ψ, and thus $\{a_1, \ldots, a_n\} \subseteq A'$. Let $\hat{a} \in A \setminus A'$ be some fresh element of A, and consider the new model

$$\mathfrak{B} = (B, f_1^{\mathfrak{B}}, \ldots, f_l^{\mathfrak{B}}, R_1^{\mathfrak{B}}, \ldots, R_m^{\mathfrak{B}}),$$

where $B = A' \cup \{\hat{a}\}$,

- $f_i^{\mathfrak{B}}$ is obtained $f_i^{\mathfrak{A}}$ by assigning it the "default value" $\hat{a}$ whenever $f_i^{\mathfrak{A}}$ is not in B: $f_i^{\mathfrak{B}}(b_1, \ldots, b_{\alpha_i}) = f_i^{\mathfrak{A}}(b_1, \ldots, b_{\alpha_i})$ if the latter value is in B, and $f_i^{\mathfrak{B}}(b_1, \ldots, b_{\alpha_i}) = \hat{a}$ otherwise.

- $R_j^{\mathfrak{B}} = R_j^{\mathfrak{A}}\big|_{B^{\beta_j}}$ is simply obtained by restricting $R_j^{\mathfrak{A}}$ to the new domain B.

It is clear that $\mathfrak{B}, \rho \vDash \psi$, and hence $\mathfrak{B} \vDash \varphi$.

If $\mathfrak{A}$ is finite, then we only need to create an infinite model for φ. This time let the universe of the new model $\mathfrak{B}$ be $A \cup B$, where B is an infinite set, the interpretations of relations remain unaltered, and the interpretations of functions be extended to become total by assigning arbitrary values from $B \setminus A$. It is again clear that $\mathfrak{B}, \rho \vDash \psi$ and thus $\mathfrak{B} \vDash \varphi$. □

Statement of Problem 2.3.10. Find two *universal* sentences φ_1, φ_2 s.t.

1. φ_1 has a finite model, but no infinite one.
2. φ_2 has an infinite model, but no finite one. □

Solution of Problem 2.3.10. For the first point, the required sentence is $\varphi_1 \equiv \forall x \forall y \,.\, x = y$. For the second point, an initial idea may be to axiomatise an strict total order $<$ with no maximal element:

$$\forall x \,.\, \neg(x < x), \tag{A1}$$

$$\forall x \forall y \forall z \,.\, x < y \land y < z \to x < z, \tag{A2}$$

$$\forall x \forall y \,.\, x < y \lor y < x \lor x = y, \tag{A3}$$

$$\forall x \exists y \,.\, x < y. \tag{A4}$$

However, the last axiom is problematic because it is not a universal sentence. (A similar idea is to axiomatise that $<$ is dense, but this also requires a non-universal sentence). By introducing a unary function symbol f, we can replace (A4) by

$$\forall x \,.\, x < f(x). \tag{A5}$$

The conjunction of (A1)–(A3) and (A5) provides the sought universal sentence φ_2. □

Statement of Problem 2.3.11 "Constructibility". Is it the case, that if $\mathfrak{A} \vDash \exists x \,.\, \varphi$, then there exists a term t in the language of $\mathfrak{A}$ s.t. $\mathfrak{A} \vDash \varphi[x \mapsto t]$? In other words, are existential witnesses *constructible*? □

Solution of Problem 2.3.11 "Constructibility". No, in general existential witnesses may not be *constructible*. Consider the trivial structure $\mathfrak{A} = (\{a\})$ (so that no element is constructible) and the formula $\exists x . x = x$. Clearly a is a witness for x, but it is not constructible in the language of $\mathfrak{A}$ (which is empty). □

2.4 Skolemisation

Statement of Problem 2.4.1. Let φ be a formula and f a unary function symbol s.t. 1) f is not used in φ, and 2) every free occurrence of variable y in φ is not under the scope of a quantifier binding variable x. Show that

$$\forall x . \exists y . \varphi \text{ is satisfiable} \quad \text{if, and only if,} \quad \forall x . \varphi[y \mapsto f(x)] \text{ is satisfiable.}$$

Is the first assumption necessary? And the second one? Find counterexamples in each case. □

Solution of Problem 2.4.1. Let $\psi \equiv \forall x \exists y . \varphi$ and $\xi \equiv \forall x . \varphi[y \mapsto f(x)]$. The "if" direction is immediate: If ξ is satisfiable, then there exists a model $\mathfrak{A} = (A, f^{\mathfrak{A}})$ with domain A and $f^{\mathfrak{A}} : A \to A$, and an evaluation $\rho : X \to A$ for the free variables of φ s.t. $\mathfrak{A}, \rho \models \xi$. By definition, $\mathfrak{A} = (A)$ (omitting $f^{\mathfrak{A}}$) is a model for ψ.

The other direction is harder. Let $\mathfrak{A} = (A)$ be a structure with domain A and let $\rho : X \to A$ be a variable valuation s.t.

$$\mathfrak{A}, \rho \models \psi.$$

For each $a \in A$, there exists $b_a \in A$ (depending on a) s.t.

$$\mathfrak{A}, \rho[x \mapsto a][y \mapsto b_a] \models \varphi.$$

Let us define a new model $\mathfrak{B} = (A, f^{\mathfrak{B}})$ by setting $f^{\mathfrak{B}}(a) = b_a$ for every $a \in A$. Since f does not occur in φ, we trivially have, for every $a \in A$,

$$\mathfrak{B}, \rho[x \mapsto a][y \mapsto b_a] \models \varphi.$$

Since $[\![f(x)]\!]^{\mathfrak{B}}_{\rho[x \mapsto a]} = f^{\mathfrak{B}}(a) = b_a$, by the "if" direction of Lemma 2.0.1 "Substitution lemma",

$$\mathfrak{B}, \rho[x \mapsto a] \models \varphi[y \mapsto f(x)].$$

Since a was arbitrary, we obtain

$$\mathfrak{B}, \rho \models \forall x \,.\, \varphi[y \mapsto f(x)].$$

Thus, $\forall x \,.\, \varphi[y \mapsto f(x)]$ is satisfiable.

The first assumption is necessary: Consider $\forall x \exists y \,.\, \varphi$ where $\varphi \equiv y \neq f(x)$, which is satisfiable, while $\forall x \,.\, \varphi[y \mapsto f(x)] \equiv \forall x \,.\, f(x) \neq f(x)$ is no longer satisfiable.

The second assumption is also necessary: Consider $\psi \equiv \forall x \exists y \,.\, \varphi$, where

$$\varphi \equiv \forall x \,.\, x = y \wedge \exists x \exists y \,.\, x \neq y.$$

(Notice that the first universal quantifier "$\forall x$" in ψ does not bind any variable.) The first conjunct of ψ says that the model has exactly one element, while the second one says that the model has at least two elements. Thus, ψ is unsatisfiable. However, $\forall x \,.\, \varphi[y \mapsto f(x)]$ equals

$$\forall x \,.\, x = f(x) \wedge \exists x \exists y \,.\, x \neq y,$$

which is clearly satisfiable by taking $f^{\mathfrak{A}}$ to be the identity function. □

Statement of Problem 2.4.2 "Skolemisation". Show that for every sentence φ there exists a *universal* sentence $\forall x_1, \ldots, x_n \,.\, \psi$ (with ψ quantifier-free) s.t.

$$\varphi \text{ satisfiable} \quad \text{if, and only if,} \quad \models \forall x_1, \ldots, x_n \,.\, \psi \text{ satisfiable.}$$

Hint: Generalise Problem 2.4.1. □

Statement of Problem 2.4.3 "Herbrandisation". Show that for every sentence φ there exists an *existential* sentence $\exists x_1, \ldots, x_n \,.\, \psi$ (with ψ quantifier-free) s.t.

$$\models \varphi \quad \text{if, and only if,} \quad \exists x_1, \ldots, x_n \,.\, \psi.$$

Hint: Use Problem 2.4.2 "Skolemisation". □

2.5 Herbrand models

Statement of Problem 2.5.2 "Herbrand's theorem". Consider a universal sentence $\varphi \equiv \forall \bar{x} \,.\, \psi$, with ψ quantifier-free. Show that φ is satisfiable if, and only if, it has a Herbrand model. Does this hold for non-universal sentences? □

Solution of Problem 2.5.2 "Herbrand's theorem". The "if" direction is trivial. For the "only if direction", let $\mathfrak{A}$ be a model. Let $\mathfrak{H}$ be the Herbrand structure uniquely defined by

$$R_i^{\mathfrak{H}}(\bar{u}) \quad \text{if, and only if,} \quad \mathfrak{A} \vDash R_i(\bar{u}).$$

We show that $\mathfrak{H}$ is a model for the sentence $\varphi \equiv \forall x_1, \ldots, x_n \,.\, \psi$ whenever $\mathfrak{A}$ is a model for φ. We proceed by induction on the number n of universal quantifiers. In the base case $n = 0$, φ is a variable-free sentence, and thus it is a Boolean combination of atomic sentences of the form $R_i(\bar{u})$. Then $R_i^{\mathfrak{H}}(\bar{u})$ holds by construction of $\mathfrak{H}$, and thus $\mathfrak{H} \vDash \varphi$, in this case. For the inductive step $n > 0$, assume $\mathfrak{A} \vDash \varphi$ with $\varphi \equiv \forall x \,.\, \psi$. For every ground term t we have $\mathfrak{A}, x : [\![t]\!] \vDash \psi$, and thus by Lemma 2.0.1 "Substitution lemma", $\mathfrak{A} \vDash \psi[x \mapsto t]$. Since $\psi[x \mapsto t]$ has $n - 1$ universal quantifiers, by the inductive assumption (applied countably many times!) $\mathfrak{H} \vDash \psi[x \mapsto t]$. Since t was arbitrary and there are no other elements in the Herbrand universe H, $\mathfrak{H} \vDash \forall x \,.\, \psi$, as required.

This fails for non-universal sentences. Consider the non-universal sentence $P(0) \wedge \exists x \,.\, \neg P(x)$, which is satisfied only in models of size ≥ 2. However, the Herbrand universe over the signature consisting of a single zero-ary constant "0" is $H = \{0\}$ and thus has size 1. □

Statement of Problem 2.5.3. Let Σ be a signature containing at least one constant symbol. Let Δ be a set of universal sentences over Σ of the form $\forall x_1, \ldots, x_n \,.\, \psi$ with ψ quantifier-free. Show that the following three conditions are equivalent:

1. Δ is satisfiable.

2. Δ has a Herbrand model.

3. The set following set of ground formulas is satisfiable in the sense of first-order logic:

$$\Gamma = \{\psi[x_1 \mapsto u_1]\cdots[x_n \mapsto u_n] \mid (\forall x_1,\ldots,x_n \,.\, \psi) \in \Delta \text{ and } u_1 \in H,\ldots,u_n \in H\}. \tag{2.1}$$

4. Let p_ψ be a fresh propositional variable for every atomic formula ψ of the form $u_1 = u_2$ or $R(u_1,\ldots,u_n)$ with $R \in \Sigma$, and let φ^{p} be the formula of propositional logic obtained from φ by replacing every atomic formula ψ as above with p_ψ. The following set of formulas of propositional logic is satisfiable in the sense of propositional logic:

$$\Gamma^{\mathrm{p}} = \{\varphi^{\mathrm{p}} \mid \varphi \in \Gamma\}. \tag{2.2}$$

□

Solution of Problem 2.5.3. The implication "1 → 2" follows immediately from Problem 2.5.2 "Herbrand's theorem": If there is a model $\mathfrak{A}$ of every sentence $\varphi \in \Delta$, then the Herbrand model $\mathfrak{H}$ constructed from $\mathfrak{A}$ is also a model of every $\varphi \in \Delta$. The implication "2 → 1" is trivial. The two implications "2 ↔ 3" hold by the definition of Herbrand models, since the domain in a Herbrand model contains precisely all terms which can be constructed from the signature Σ.

Each formula in Γ is a Boolean combination of atomic formulas of the form $u_1 = u_2$ or $R(u_1,\ldots,u_n), R \in \Sigma$, where the u_i's are terms constructed from the constants and functions of Σ. There exists a bijection between models $\mathfrak{A}$ of Γ and propositional truth assignments ρ over propositional variables p_ψ's. This shows "3 ↔ 4". □

Statement of Problem 2.5.4. Consider a universal sentence of the form $\varphi \equiv \forall \bar{x} \,.\, \psi$, with ψ quantifier-free. Show that φ is unsatisfiable if, and only if, there exist tuples of ground terms $\bar{u}_1,\ldots,\bar{u}_n$ s.t. the following is unsatisfiable:

$$\psi[\bar{x} \mapsto \bar{u}_1] \wedge \cdots \wedge \psi[\bar{x} \mapsto \bar{u}_n]. \tag{2.3}$$

Hint: Use Problem 2.5.3 and Problem 1.5.1 "Compactness theorem for propositional logic". □

Solution of Problem 2.5.4. The "if" direction is trivial. For the "only if" direction, assume that φ is unsatisfiable. By taking $\Delta = \{\varphi\}$ in Problem 2.5.3, we have that the set of all substitution instances Γ from (2.3) is unsatisfiable in the sense of first-order logic, and Γ^{p} from (2.4) is unsatisfiable in the sense of propositional logic. By Problem 1.5.1 "Compactness theorem for propositional logic", there exists a finite subset $\Gamma_0^{\mathrm{p}} \subseteq_{\mathrm{fin}} \Gamma^{\mathrm{p}}$ which is already propositionally unsatisfiable. There exists a finite subset $\Gamma_0 = \{\psi[\bar{x} \mapsto \bar{u}_1], \ldots, \psi[\bar{x} \mapsto \bar{u}_n]\} \subseteq_{\mathrm{fin}} \Gamma$ which is unsatisfiable in the sense of first-order logic, as required. □

2.6 Logical consequence

Statement of Problem 2.6.1. Consider the following two sentences:

$$\begin{aligned} \varphi &\equiv \forall x \forall y \,.\, y = f(g(x)) \to \exists u \,.\, u = f(x) \wedge y = g(u), \text{and} \\ \psi &\equiv \forall x \,.\, f(g(f(x))) = g(f(f(x))). \end{aligned}$$

Is it the case that φ logically implies ψ, in symbols $\varphi \vDash \psi$? □

Solution of Problem 2.6.1. Yes. The first sentence is logically equivalent to $\forall x \,.\, f(g(x)) = g(f(x))$, and thus the second sentence follows from this fact. □

Statement of Problem 2.6.2. Let f be a unary function symbol and, for $n \in \mathbb{N}$, denote the n-fold application of f to x by

$$f^n(x) := \underbrace{f(\cdots(f(x))\cdots)}_{n}.$$

Does the following hold?

$$\{\forall x \,.\, f^n(x) = x \mid n = 2, 3, 5, 7\} \vDash \forall x \,.\, f^{11}(x) = x.$$ □

Solution of Problem 2.6.2. Yes, because $f^{11}(x) = f^2(f^2(f^7(x)))$. □

2.6.1 Independence

Statement of Problem 2.6.4. Show that the set of axioms of equivalence relations "$\approx$" are independent:

$$\begin{aligned}\Delta = \{&\forall x\,.\,x \approx x, && \text{(reflexivity)}\\ &\forall x \forall y\,.\,x \approx y \to y \approx x, && \text{(symmetry)}\\ &\forall x \forall y \forall z\,.\,x \approx y \land y \approx z \to x \approx z\}. && \text{(transitivity)}\end{aligned} \qquad \square$$

Solution of Problem 2.6.4. Let φ be the reflexivity axiom. As a model for $\Delta \smallsetminus \{\varphi\}$ consider the one element structure $\mathfrak{A} = (\{a\}, \approx^{\mathfrak{A}})$ where $\approx^{\mathfrak{A}}$ is the empty relation.

For the symmetry axiom, consider $\mathfrak{A} = (\{a,b\}, \approx^{\mathfrak{A}})$ with $\approx^{\mathfrak{A}}= \{(a,a),(a,b),(b,b)\}$. The reflexivity and transitivity axioms are satisfied, but symmetry fails, since $a \approx^{\mathfrak{A}} b$ and $b \not\approx^{\mathfrak{A}} a$.

Finally, for the transitivity axiom, consider the structure $\mathfrak{A} = (\{a,b,c\}, \approx^{\mathfrak{A}}$) with $\approx^{\mathfrak{A}}= \{(a,a),(b,b),(c,c),(a,b),(b,a),(b,c),(c,b)\}$. The relation "$\approx^{\mathfrak{A}}$" is reflexive and symmetric, but not transitive since $a \not\approx^{\mathfrak{A}} c$. Another solution using the infinite structure of the natural numbers $\mathbb{N} = (\{0,1,\dots\}, \approx^{\mathbb{N}})$ where $(m,n) \in\approx^{\mathbb{N}}$ holds iff $|m-n| \le 1$. $\square$

Statement of Problem 2.6.5. Show that the set of axioms of linear orders "$\le$" are independent:

$$\begin{aligned}\Delta_{\text{lin}} = \{&\forall x \forall y\,.\,x \le y \land y \le x \to x = y, && \text{(antisymmetry)}\\ &\forall x \forall y \forall z\,.\,x \le y \land y \le z \to x \le z, && \text{(transitivity)}\\ &\forall x \forall y\,.\,x \le y \lor y \le x\}. && \text{(totality)}\end{aligned} \qquad \square$$

Solution of Problem 2.6.5. Antisymmetry is violated by any total preorder (i.e., a total, transitive, and reflexive relation) which is not a linear order, such as $\mathfrak{A} = (\{a,b\}, \le^{\mathfrak{A}})$ with $\le^{\mathfrak{A}}= \{(a,a),(a,b),(b,a),(b,b)\}$.

Transitivity is violated by the following antisymmetric and total relation $\mathfrak{A} = (\{a,b,c\}, \le^{\mathfrak{A}})$ with $\le^{\mathfrak{A}}= \{(a,a),(b,b),(c,c),(a,b),(b,c),(c,a)\}$.

Finally, totality is violated by any non-total partial order (i.e., a reflexive, antisymmetric, and transitive relation), such as the identity relation on a two-element set: $\mathfrak{A} = (\{a,b\}, \{(a,a),(b,b)\})$. $\square$

Statement of Problem 2.6.6. Show that the set of axioms of groups with a binary operation "$*$" and unit element "1" are independent:

$$\begin{aligned}\Delta = \{&\forall x \,.\, 1 * x = x \wedge x * 1 = x, && \text{(unit)}\\ &\forall x, y, z \,.\, (x * y) * z = x * (y * z), && \text{(associativity)}\\ &\forall x \,.\, \exists y \,.\, x * y = 1 \wedge y * x = 1\}. && \text{(inverses)}\end{aligned}$$ □

Solution of Problem 2.6.6. We begin by showing independence of the unit axiom. Consider the structure $(\{1, 2, \ldots\} \cup \{\infty\}, +, \infty)$, where "+" is the standard addition operation on the natural numbers, extended by setting the result to be ∞ if at least one argument is ∞. The addition operation is easily seen to be associative. Inverses do exist in this model, because ∞ is the inverse of any number. However, ∞ is not a unit.

Next, we show independence of the associativity axiom. Let $(\mathbb{R}, *, 1)$ be the multiplicative group of real numbers. It satisfies all three axioms. Now modify it to $\mathbb{R}'$ by setting $2 *' 2 = 5$. The axioms asserting the existence of a unit and of inverses are unaffected, because they depend only on multiplications which involve 1, either as an argument or as the result. However, associativity fails: $3 *' (2 *' 2) = 15 \neq 12 = (3 *' 2) *' 2$.

Independence of the inverses axiom can be seen by taking any monoid which is not a group, such as the free monoid $\mathfrak{A} = (\{a\}^*, \cdot, \varepsilon)$ of finite words over a single-letter alphabet. □

Statement of Problem 2.6.7. Prove that every *finite* set of sentences Δ contains a subset $\Delta' \subseteq \Delta$ s.t. Δ' is independent and $\Delta' \vDash \Delta$. Is the finiteness assumption necessary? □

Solution of Problem 2.6.7. Consider the following procedure:

$\Delta_0 := \Delta$;
$i := 0$;
while Δ_i is not independent
  choose $\varphi \in \Delta_i$ such that $\Delta_i \setminus \{\varphi\} \vDash \varphi$;
  $\Delta_{i+1} := \Delta_i \setminus \{\varphi\}$;
  $i := i + 1$;
end

The loop preserves the invariant that every sentence φ that is removed from Δ_i is a logical consequence of Δ_{i+1}. Moreover, the loop terminates at some finite index $n \leq |\Delta|$, and after it does so, Δ_n is independent.

The finiteness assumption is necessary: Any infinite set of sentences $\Delta = \{\varphi_1, \varphi_2, \dots\}$ s.t. $\varphi_{n+1} \vDash \varphi_n$ but $\varphi_n \nvDash \varphi_{n+1}$ would do. For instance, take $\varphi_n \equiv \exists x_1 \cdots \exists x_n \cdot \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$ saying that there are at least n elements in the model. If Δ' is an infinite subset of Δ, then Δ' is not independent since every $\varphi_n \in \Delta'$ is a logical consequence of some $\varphi_m \in \Delta' \setminus \{\varphi_n\}$ with $m > n$. If Δ' is a finite subset of Δ, then $\Delta' \nvDash \Delta$, since Δ' has a finite model, but Δ has only infinite models. □

Statement of Problem 2.6.8. Prove that every class of structures over a finite signature which is axiomatised by a set of first-order sentences, can be axiomatised by an *independent* set of first-order sentences. □

Solution of Problem 2.6.8. Let $\Gamma = \{\varphi_1, \varphi_2, \dots\}$ be any set of axioms, which we can assume to be countable since the signature is finite. We can assume w.l.o.g. that $\varphi_{i+1} \vDash \varphi_i$ for every $i \in \mathbb{N}$ (consider $\{\top, \varphi_1, \varphi_1 \wedge \varphi_2, \dots\}$), and by removing adjacent equivalent formulas we can also assume $\varphi_i \nvDash \varphi_{i+1}$. Consider the following set of sentences

$$\Delta = \{\varphi_1, \varphi_1 \to \varphi_2, \varphi_2 \to \varphi_3, \dots\}.$$

By compactness, it suffices to prove that each finite subset $\Delta_n = \{\varphi_1, \varphi_1 \to \varphi_2, \dots, \varphi_{n-1} \to \varphi_n\} \subseteq_{\text{fin}} \Delta$ is independent. Assume by way of contradiction that there is $1 \leq i \leq n$ s.t.

$$\Delta_n \setminus \{\varphi_{i-1} \to \varphi_i\} \vDash \varphi_{i-1} \to \varphi_i.$$

Since by assumption $\varphi_{i-1} \nvDash \varphi_i$, there exists a model $\mathcal{A}$ s.t. $\mathcal{A} \vDash \varphi_{i-1}$ and $\mathcal{A} \nvDash \varphi_i$. Consequently, $\mathcal{A} \vDash \Delta_n \setminus \{\varphi_{i-1} \to \varphi_i\}$, and thus it would follow $\mathcal{A} \vDash \varphi_i$, which is a contradiction. □

2.7 Axiomatisability

Statement of Problem 2.7.2 "Classes of finite structures are axiomatisable". Fix a finite signature Σ. Show that any countable class $\mathcal{A}$ of *finite* structures over Σ is axiomatisable. *Hint: Use the characteristic sentences from Problem 2.1.8 "Characteristic sentences".* □

Solution of Problem 2.7.2 "Classes of finite structures are axiomatisable". Let $\mathcal{A} = \{\mathfrak{A}_0, \mathfrak{A}_1, \dots\}$ be a countable class of finite structures $\mathfrak{A}_n$'s, and let $\mathcal{B}$ be the class of finite structures over Σ not in $\mathcal{A}$. The class $\mathcal{B} = \{\mathfrak{B}_0, \mathfrak{B}_1, \dots\}$ is also countable. Let φ_i be the characteristic sentence of $\mathfrak{B}_i$. Then $\mathcal{A}$ is axiomatised by

$$\{\neg\varphi_0, \neg\varphi_1, \dots\}. \qquad \square$$

Statement of Problem 2.7.3 "Universal axiomatisations". Recall that $\mathfrak{B}$ is an induced substructure of $\mathfrak{A}$ if if can obtained from the latter by taking a subset of the domain, and restricting the relations to the new domain. Show that an isomorphism-closed class $\mathcal{A}$ of finite relational structures can be axiomatised by a set of *universal* sentences of first-order logic if, and only if, $\mathcal{A}$ is closed under induced substructures. $\square$

Solution of Problem 2.7.3 "Universal axiomatisations". By Problem 2.11.3 "Fundamental property", universal sentences are preserved by induced substructures, and thus if Γ is a set of universal sentences and $\mathfrak{A} \models \Gamma$, then also $\mathfrak{B} \models \Gamma$ whenever $\mathfrak{B}$ is an induced substructure of $\mathfrak{A}$. Thus, if $\mathcal{A}$ can be axiomatised by a set of universal sentences, then it is closed under induced substructures.

On the other hand, assume $\mathcal{A} = \{\mathfrak{A}_0, \mathfrak{A}_1, \dots\}$ is a set of finite relational structures closed under induced substructures. We can use the method of Problem 2.7.2 "Classes of finite structures are axiomatisable" and construct a universal axiomatisation. The class of structures $\mathcal{B} = \{\mathfrak{B}_0, \mathfrak{B}_1, \dots\}$ over the same signature not in $\mathcal{A}$ is closed under induced superstructures, i.e., adding elements to the domain and possibly extending the relations on these new elements. The characteristic sentence φ_i of $\mathfrak{B}_i$ contains both existential and universal quantifiers. We remove the universal part "$\forall y \,.\, \bigvee_{1 \le i \le m} y = x_i$" and obtain an existential sentence $\hat{\varphi}_i$ s.t. $\mathfrak{B}_i \models \hat{\varphi}_i$, and, thanks to the closure property of $\mathcal{B}$, all models of $\hat{\varphi}_i$ are in $\mathcal{B}$. Consequently, $\{\neg\hat{\varphi}_1, \neg\hat{\varphi}_2, \dots\}$ is a universal axiomatisation for $\mathcal{A}$. $\square$

2.8 Spectrum

2.8.1 Examples

Statement of Problem 2.8.2 "Finite and cofinite sets are spectra". Show that if $N \subseteq \mathbb{N}_{>0}$ is either finite or co-finite (i.e., its complement $\mathbb{N}_{>0} \setminus N$ is finite), then N is a first-order spectrum. □

Solution of Problem 2.8.2 "Finite and cofinite sets are spectra". Let $N = \{n_1, \ldots, n_k\} \subseteq \mathbb{N}_{>0}$ be a finite set of non-zero natural numbers. By using the counting sentences $\varphi_{=i} \equiv \varphi_{\leq i} \wedge \varphi_{\geq i}$ from Problem 2.1.6 "Cardinality constraints I" and Problem 2.1.7 "Cardinality constraints II", it is easily seen that N, resp., its complement $N^c := \mathbb{N}_{>0} \setminus N$, is the spectrum of the sentence

$$\varphi_N \equiv \varphi_{=n_1} \vee \cdots \vee \varphi_{=n_k}, \text{ resp., } \varphi_{N^c} \equiv \neg\varphi_{=n_1} \wedge \cdots \wedge \neg\varphi_{=n_k}.$$

(Note that φ_N is a $\exists\forall$-sentence using only relational symbols (the equality relations). Problem 2.8.23 "Spectra of $\exists^*\forall^*$-sentences" asks to show that the spectra of such sentences are always either finite or co-finite.) □

Statement of Problem 2.8.3 "Even numbers". Show that the set of all positive even numbers $\{2 \cdot n \mid n \in \mathbb{N}_{>0}\}$ is a first-order spectrum. *Hint: Use a unary function symbol f.* □

Solution of Problem 2.8.3 "Even numbers". Consider the following sentence:

$$\forall x \,.\, f(f(x)) = x \wedge f(x) \neq x.$$

The first conjunct enforces that f is an involutive permutation, whence its cycles are of size 1 or 2. The second conjunct guarantees that all cycles are of size 2. Consequently, the sentence has models of each even cardinality, and no models of odd cardinality. Therefore the spectrum of this sentence is the infinite set of even numbers. □

Statement of Problem 2.8.4. Show that the set of squares $\{n^2 \mid n \in \mathbb{N}_{>0}\}$ is a first-order spectrum. *Hint: Use a binary function symbol f and a unary relation symbol U.* □

Solution of Problem 2.8.4. We use a unary relation symbol U and a binary function symbol f. Consider the following sentence:

$$\begin{aligned}&\forall z \exists x \exists y \,.\, U(x) \wedge U(y) \wedge f(x,y) = z \wedge \\ &\forall x_1 \forall x_2 \forall y_1 \forall y_2 \,.\, U(x_1) \wedge U(x_2) \wedge U(y_1) \wedge U(y_2) \wedge \\ &\qquad f(x_1,y_1) = f(x_2,y_2) \to x_1 = x_2 \wedge y_1 = y_2.\end{aligned}$$

The first sentence says that f restricted to $U \times U$ is onto the whole universe, and the second one that f restricted to $U \times U$ is one-to-one. Consequently, the whole domain is of the same cardinality as $U \times U$. Again, the construction of a model with an arbitrary fixed cardinality of U is obvious. □

Statement of Problem 2.8.5. Show that the set $\{m \cdot n \mid m, n \in \mathbb{N}_{>0}\}$ of positive composite numbers is a first-order spectrum. *Hint: Use a binary function symbol f and two unary relation symbols U, V.* □

Solution of Problem 2.8.5. The solution is obtained with minor modifications from the one of Problem 2.8.4:

$$\begin{aligned}&\forall z \exists x \exists y \,.\, U(x) \wedge V(y) \wedge f(x,y) = z \wedge \\ &\forall x_1 \forall x_2 \forall y_1 \forall y_2 \,.\, U(x_1) \wedge U(x_2) \wedge V(y_1) \wedge V(y_2) \wedge \\ &\qquad f(x_1,y_1) = f(x_2,y_2) \to x_1 = x_2 \wedge y_1 = y_2.\end{aligned}$$ □

Statement of Problem 2.8.6. Show that the set of powers of two $\{2^n \mid n \in \mathbb{N}\}$ is a first-order spectrum. *Hint: Axiomatise the membership relation "$\in$".* □

Solution of Problem 2.8.6. Let U be a unary relation. We axiomatise the powerset of U. We use the relation symbol "$\in$" (written in infix form) with the intended interpretation that $u \in x$ means that u is an element of U and that u "belongs" to x. Only elements of U can be members of sets:

$$\forall u \forall x \,.\, u \in x \to U(u).$$

Sets with identical elements are equal (extensionality):

$$\forall x \forall y \,.\, (\forall u \,.\, u \in x \leftrightarrow u \in y) \to x = y.$$

There is an empty set:

$$\exists x \forall u \,.\, \neg u \in x.$$

For every set x and every element u there exists $y = x \cup \{u\}$:

$$\forall x \forall u \exists y \forall v \,.\, v \in y \leftrightarrow (v \in x \vee v = u).$$

The latter is the key new technique required in this problem: if a subset is represented, then all subsets formed by adding a new element to it are also represented. These axioms, when taken together, imply that the whole universe is indeed, in terms of the relation "$\in$", the powerset of U and has therefore $2^{|U^{\mathfrak{A}}|}$ elements. Once again, the construction of a model where U has an arbitrary cardinality is obvious.

There are other solutions of this problem. The first one is to write the axioms of fields (see the solution of Problem 2.8.9 below) and add an axiom $1 + 1 = 0$ which says that the characteristic of the field is 2. Then the finite models of the whole set of sentences are fields of cardinalities 2^n for positive n, and for every n such a field exists. Another algebraic solution is to take the axioms of Boolean algebras. It can be shown that every finite Boolean algebra has 2^n elements for a positive n, and for every n such an algebra exists. In both cases one should add an extra clause permitting a single-element model. □

Statement of Problem 2.8.7. Show that the set of self-powers $\{n^n \mid n \in \mathbb{N}_{>0}\}$ is a first-order spectrum. *Hint: Axiomatise the relation $Apply(f, u, v)$, which holds iff "$f(u) = v$".* □

Solution of Problem 2.8.7. This time we are going to express that the universe is the set of all functions $U \to U$. We use a ternary relation *Apply*, with the intended meaning that $Apply(f, u, v)$ means that function f applied to an element u of U yields an element v of U. Every element f of the universe is a binary relation on U:

$$\forall f \forall u \forall v \,.\, Apply(f, u, v) \to U(u) \wedge U(v).$$

Every element f of the universe is indeed a function $U \to U$:

$$\forall f \forall u \exists! v \,.\, Apply(f, u, v).$$

Every two elements of the universe, if they are identical as functions, then they are indeed equal (extensionality):

$$\forall f \forall g . (\forall u \forall v . Apply(f, u, v) \leftrightarrow Apply(g, u, v)) \to f = g.$$

The crucial closure property that we require is that single-point modifications of represented functions are also represented: For every function f, argument u, and value v, $g = f[u \mapsto v]$ is also a function:

$$\begin{aligned} &\forall f \forall u \forall v \exists g \forall t \forall w . Apply(g, t, w) \leftrightarrow \\ &\qquad (Apply(f, t, w) \vee t = u \wedge w = v). \end{aligned}$$ □

Statement of Problem 2.8.8. Show that the set of factorials $\{n! \mid n \in \mathbb{N}\}$ is a first-order spectrum. *Hint: Axiomatise that the universe is the set of all linear orders on U.* □

Solution of Problem 2.8.8. Consider the ternary relation $R(p, x, y)$ which intuitively holds if p is a linear order and x comes before y w.r.t. p. Let the required sentence be the conjunction of the following axioms:

$$\begin{aligned} &\forall p \forall x \forall y . R(p, x, y) \to U(x) \wedge U(y), && \text{(binary relation)} \\ &\forall p \forall x \forall y \forall z . R(p, x, y) \wedge R(p, y, z) \to R(p, x, z), && \text{(transitivity)} \\ &\forall p \forall x \forall y . R(p, x, y) \vee R(p, y, x), && \text{(linearity)} \\ &\forall p \forall q . (\forall x \forall y . R(p, x, y) \leftrightarrow R(q, x, y)) \to p = q, && \text{(extensionality)} \\ &\forall p \forall x \forall y \exists q \forall u \forall v . R(q, u, v) \leftrightarrow && \\ &\qquad (R(p, u, v) \wedge u \neq x \wedge v \neq y \vee && \\ &\qquad\quad R(p, y, x) \wedge u = x \wedge v = y). && \text{(swap)} \end{aligned}$$

The crucial property is the last one, which allows to generate all linear orders by performing single swaps. □

Statement of Problem 2.8.9. Find a first-order sentence φ s.t. its spectrum is precisely the powers of all prime numbers:

$$\mathsf{Spec}(\varphi) = \{p^n \mid p, n \in \mathbb{N}, p \text{ prime}\}.$$ □

Solution of Problem 2.8.9. It is well known that any finite field has p^n elements, where p is a prime number, called its characteristic, and n is a positive natural number. Therefore it suffices to consider the sentence φ_{field} over two constant symbols "0", "1" and two binary functions "+", "·" expressing the classical axioms of fields:

$$\begin{aligned}
\varphi_{\text{field}} \equiv\ & \forall a \forall b \forall c \,.\, a + (b + c) = (a + b) + c \wedge && \text{(associativity of +)}\\
& \forall a \,.\, a + 0 = a \wedge && \text{(neutral element of +)}\\
& \forall a \exists b \,.\, a + b = 0 \wedge && \text{(inverse w.r.t. +)}\\
& \forall a \forall b \,.\, a + b = b + a \wedge && \text{(commutativity of +)}\\
& \forall a \forall b \forall c \,.\, a \cdot (b \cdot c) = (a \cdot b) \cdot c \wedge && \text{(associativity of $\cdot$)}\\
& \forall a \,.\, a \cdot 1 = a \wedge && \text{(neutral element of $\cdot$)}\\
& \forall a \,.\, a \neq 0 \rightarrow \exists b \,.\, a \cdot b = 1 \wedge && \text{(inverse w.r.t. $\cdot$)}\\
& \forall a \forall b \,.\, a \cdot b = b \cdot a \wedge && \text{(commutativity of $\cdot$)}\\
& \forall a \forall b \forall c \,.\, a \cdot (b + c) = (a \cdot b) + (a \cdot c) \wedge && \text{(distributivity)}\\
& 0 \neq 1. && \square
\end{aligned}$$

2.8.2 Closure properties

Statement of Problem 2.8.10 "Spectra are closed under union". Show that spectra of first-order logic sentences are closed under finite union. □

Solution of Problem 2.8.10 "Spectra are closed under union". We can rephrase the spectrum as $\mathsf{Spec}(\varphi) = \mathsf{Card}(\mathsf{Mod}(\varphi))$, where $\mathsf{Card}(\mathcal{A}) = \{|A| \mid (A, \dots) \in \mathcal{A}, A \text{ finite}\}$ is the set of cardinalities of the set of models in $\mathcal{A}$. Since φ, ψ are sentences (i.e., no free variables), we have $\mathsf{Mod}(\varphi) \cup \mathsf{Mod}(\psi) = \mathsf{Mod}(\varphi \vee \psi)$ (disjunctive property) directly from the definition of the satisfaction relation "$\models$". Moreover, $\mathsf{Card}(\mathcal{A} \cup \mathcal{B}) = \mathsf{Card}(\mathcal{A}) \cup \mathsf{Card}(\mathcal{B})$ holds in general. It immediately follows

$$\begin{aligned}
\mathsf{Spec}(\varphi \vee \psi) &= \mathsf{Card}(\mathsf{Mod}(\varphi \vee \psi))\\
&= \mathsf{Card}(\mathsf{Mod}(\varphi) \cup \mathsf{Mod}(\psi))\\
&= \mathsf{Card}(\mathsf{Mod}(\varphi)) \cup \mathsf{Card}(\mathsf{Mod}(\psi))\\
&= \mathsf{Spec}(\varphi) \cup \mathsf{Spec}(\psi). \qquad \square
\end{aligned}$$

Statement of Problem 2.8.11 "Spectra are closed under intersection". Show that spectra of first-order logic sentences are closed under finite intersection. $\square$

Solution of Problem 2.8.11 "Spectra are closed under intersection". Let $M = \mathsf{Spec}(\varphi)$ and $N = \mathsf{Spec}(\psi)$. First of all, by the definition of satisfaction relation "$\vDash$" since φ, ψ are sentences, $\mathsf{Mod}(\varphi \wedge \psi) = \mathsf{Mod}(\varphi) \cap \mathsf{Mod}(\psi)$. The inclusion $\mathsf{Card}(\mathcal{A} \cap \mathcal{B}) \subseteq \mathsf{Card}(\mathcal{A}) \cap \mathsf{Card}(\mathcal{B})$ holds in general, and thus

$$\begin{aligned}\mathsf{Spec}(\varphi \wedge \psi) &= \mathsf{Card}(\mathsf{Mod}(\varphi \wedge \psi))\\ &= \mathsf{Card}(\mathsf{Mod}(\varphi) \cap \mathsf{Mod}(\psi))\\ &\subseteq \mathsf{Card}(\mathsf{Mod}(\varphi)) \cap \mathsf{Card}(\mathsf{Mod}(\psi))\\ &= \mathsf{Spec}(\varphi) \cap \mathsf{Spec}(\psi).\end{aligned}$$

However the reverse inclusion $\mathsf{Card}(\mathcal{A}) \cap \mathsf{Card}(\mathcal{B}) \subseteq \mathsf{Card}(\mathcal{A} \cap \mathcal{B})$ does not hold in general, since $n \in \mathsf{Card}(\mathcal{A}) \cap \mathsf{Card}(\mathcal{B})$ is witnessed by *two* distinct models $\mathfrak{A} \in \mathcal{A}$ and $\mathfrak{B} \in \mathcal{B}$ of cardinality n, which in general will not yield a model $\mathfrak{C} \in \mathfrak{A} \cap \mathfrak{B}$ of the same cardinality. The difficulty lies in the fact that symbols in the signature may be given different interpretations by $\mathfrak{A}$ and $\mathfrak{B}$. This needs not be.

Let φ' be the sentence obtained from φ by replacing every relation and function symbols in the signature of φ in such a way that φ' and ψ have no common symbol in their signature. This operation preserves the spectrum $M = \mathsf{Spec}(\varphi')$, and since the signatures of φ', ψ are now disjoint, we can prove the missing inclusion

$$\mathsf{Card}(\mathsf{Mod}(\varphi')) \cap \mathsf{Card}(\mathsf{Mod}(\psi)) \subseteq \mathsf{Card}(\mathsf{Mod}(\varphi') \cap \mathsf{Mod}(\psi)).$$

Let $\mathfrak{A} = (A, R_1^{\mathfrak{A}}, \ldots, R_n^{\mathfrak{A}}) \in \mathsf{Mod}(\varphi')$ be a model of φ' of size $|A| = m$ let $\mathfrak{B} = (B, S_1^{\mathfrak{B}}, \ldots, S_k^{\mathfrak{B}}) \in \mathsf{Mod}(\psi)$ be a model of ψ of the same size $|A| = m$, and let $\pi : A \to B$ be any bijection between the two domains. Since φ' and ψ have no common symbol in their signature, we obtain a common model $\mathfrak{C} = (A, \mathcal{R}_1^{\mathfrak{C}}, \ldots, R_n^{\mathfrak{C}}, S_1^{\mathfrak{C}}, \ldots, S_k^{\mathfrak{C}})$ where $R_i^{\mathfrak{C}} = R_i^{\mathfrak{A}}$ and $S_j^{\mathfrak{C}}$ is obtained from $S_j^{\mathfrak{B}}$ by composition with π: $(a_1, \ldots, a_l) \in S_j^{\mathfrak{C}}$ iff $(\pi(a_1), \ldots, \pi(a_l)) \in S_j^{\mathfrak{B}}$. We have $\mathfrak{C} \vDash \varphi'$ and $\mathfrak{C} \vDash \psi$ and thus $m \in \mathsf{Card}(\mathsf{Mod}(\varphi') \cap \mathsf{Mod}(\psi))$ as required. $\square$

Statement of Problem 2.8.12 "Spectra are closed under addition". Show that spectra of first-order logic sentences are closed under addition "+". □

Solution of Problem 2.8.12 "Spectra are closed under addition". Let $M = \mathsf{Spec}(\varphi)$ and $N = \mathsf{Spec}(\psi)$ and assume w.l.o.g. that the signatures of φ and ψ are disjoint and contain only relation symbols. Let us assume they are equal to $\{R_1, \ldots, R_p\}$, resp., $\{S_1, \ldots, S_q\}$. If either φ or ψ is unsatisfiable in finite models, then $M + N = \varnothing$ and we are done by taking the sentence to be $\bot$. Assume both φ and ψ are satisfiable, i.e., M and N are nonempty. Add a fresh unary relational symbol U not already present either in φ, or in ψ. Intuitively, U partitions the model into two disjoint components, one of which is a model of φ, and the other a model of ψ. Let $[\varphi]_U$ be obtained from φ by relativising the quantifiers to U. This is formally defined using the following inductive definition (omitting the trivial cases for the Boolean connectives):

$$[\exists x \,.\, \xi]_U \;\equiv\; \exists x \,.\, U(x) \wedge [\xi]_U \quad \text{and} \quad [\forall x \,.\, \xi]_U \;\equiv\; \forall x \,.\, U(x) \to [\xi]_U.$$

Consider the sentence

$$\xi \;\equiv\; [\varphi]_U \wedge [\psi]_{\neg U}.$$

We claim that $\mathsf{Spec}(\xi) = M + N$. For the "$\supseteq$" inclusion, let $m \in M$ and $n \in N$. There is a model $\mathfrak{A} \models \varphi$ of cardinality m and a model $\mathfrak{B} \models \psi$ of cardinality n. By a suitable renaming, we can assume that $\mathfrak{A}, \mathfrak{B}$ have disjoint domains. Thus, the (disjoint) union $\mathfrak{C} = \mathfrak{A} \cup \mathfrak{B}$ is a model of ξ, where we interpret $U^{\mathfrak{C}}$ as the domain of $\mathfrak{A}$.

For the "$\subseteq$" inclusion, assume $l \in \mathsf{Spec}(\xi)$. There is a model $\mathfrak{C} \models \xi$ of the form

$$\mathfrak{C} = (C, U^{\mathfrak{C}}, R_1^{\mathfrak{C}}, \ldots, R_p^{\mathfrak{C}}, S_1^{\mathfrak{C}}, \ldots, S_q^{\mathfrak{C}})$$

with a domain of cardinality $|C| = l$. Consider the two structures

$$\mathfrak{A} = (A, R_1^{\mathfrak{C}}, \ldots, R_p^{\mathfrak{C}}) \qquad \text{and} \qquad \mathfrak{B} = (B, S_1^{\mathfrak{C}}, \ldots, S_q^{\mathfrak{C}}),$$

where $A = U^{\mathfrak{C}}$ and $B = C \setminus U^{\mathfrak{C}}$. Then, $\mathfrak{A} \models \varphi$ and $\mathfrak{B} \models \psi$, and thus $l = |A| + |B| \in M + N$. □

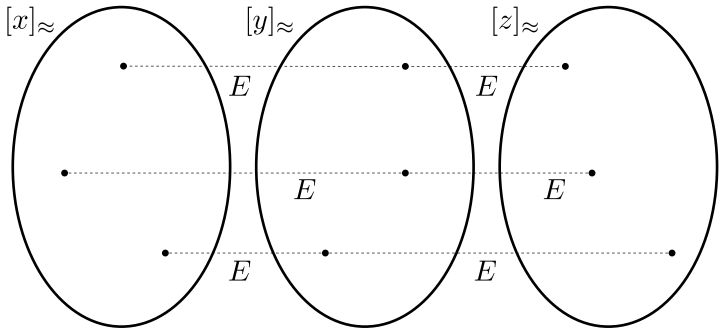


Figure for Problem 2.8.13 "Spectra are closed under multiplication".

Statement of Problem 2.8.13 "Spectra are closed under multiplication". Show that spectra of first-order logic sentences are closed under multiplication "$\cdot$". □

Solution of Problem 2.8.13 "Spectra are closed under multiplication". Let $M = \mathsf{Spec}(\varphi)$ and $N = \mathsf{Spec}(\psi)$. We assume that the signatures of φ, ψ are disjoint. We use a binary relation symbol "$\approx$" to axiomatise an equivalence relation s.t. 1) all equivalence classes have the same cardinality, 2) each equivalence class is a model of φ, and 3) the set of equivalence classes is a model of ψ (i.e., $\approx$ is interpreted as equality in ψ).

Regarding 1), we first axiomatise that $\approx$ is an equivalence relation:

$$\forall x \,.\, x \approx x, \qquad \text{(reflexivity)}$$
$$\forall x \forall y \,.\, x \approx y \to y \approx x, \qquad \text{(symmetry)}$$
$$\forall x \forall y \forall z \,.\, x \approx y \land y \approx z \to x \approx z. \qquad \text{(transitivity)}$$

In order to ensure that every equivalence class of $\approx$ has the same number of elements, we introduce a second equivalence relation E "perpendicular to $\approx$" (we skip the axioms of E being an equivalence relation):

$$\forall x \forall y \,.\, x \neq y \land x \approx y \to \neg E(x, y),$$
$$\forall x \forall y \exists! \hat{y} \,.\, y \approx \hat{y} \land E(x, \hat{y}).$$

Let ξ_1 be the conjunction of all the formulas above.

Regarding 2), let $\hat{x}$ be a fresh variable intuitively denoting a distinguished element used to select an equivalence class. Let $[\varphi]_{\approx,\hat{x}}$ be obtained by relativising the quantifiers of φ as follows:

$$[\exists x \,.\, \xi]_{\approx,\hat{x}} \;\equiv\; \exists x \,.\, x \approx \hat{x} \wedge [\xi]_{\approx,\hat{x}}, \text{ and}$$
$$[\forall x \,.\, \xi]_{\approx,\hat{x}} \;\equiv\; \forall x \,.\, x \approx \hat{x} \rightarrow [\xi]_{\approx,\hat{x}}.$$

The fact that each equivalence class of $\approx$ is a model of φ is expressed by $\xi_2 \;\equiv\; \forall \hat{x} \,.\, [\varphi]_{\approx,\hat{x}}$.

Finally, regarding 3) we construct a formula ξ_3 expressing the fact that all functions and relations in the signature of φ are invariant under $\approx$. Formally, if R is a relation symbol of arity k in the signature of ψ, then ξ_3 has a conjunct of the form (and similarly for function symbols)

$$\forall x_1 \cdots x_k \forall y_1 \cdots y_k \,.\, x_1 \approx y_1 \wedge \cdots \wedge x_k \approx y_k \rightarrow$$
$$(R(x_1, \ldots, x_k) \leftrightarrow R(y_1, \ldots, y_k)).$$

Consider the conjunction $\xi \;\equiv\; \xi_1 \wedge \xi_2 \wedge \xi_3$. We omit the details of checking $\mathsf{Spec}(\xi) = M \cdot N$. □

Statement of Problem 2.8.15 "Semilinear sets are spectra". Show that any semilinear set not containing 0 is the spectrum of a sentence of first-order logic. □

Solution of Problem 2.8.15 "Semilinear sets are spectra". Since spectra are closed under finite union by Problem 2.8.10 "Spectra are closed under union", it suffices to show that a linear set L with base b and non-zero periods $p_1, \ldots, p_n > 0$ is a spectrum. Since spectra are closed under "+" by Problem 2.8.12 "Spectra are closed under addition", it suffices to consider the case when $b = 0$ and there is only one period $p > 0$. Let f be a unary function symbol, and let φ axiomatise the fact that f is injective, the p-th iterate of f is the identity (this implies surjectivity), and no lower iterate has a fixed point

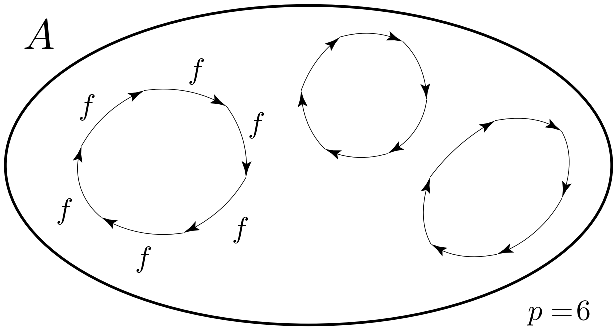


Figure for Problem 2.8.15 "Semilinear sets are spectra".

:

$$\begin{aligned}
\varphi \equiv\ & \forall x, y \,.\, f(x) = f(y) \to x = y \land && \text{(injective)}\\
& \forall x \,.\, \underbrace{f(f(\cdots f(x)\cdots))}_{p \text{ times}} = x \land && \text{(orbits of size } p\text{)}\\
& \bigwedge_{q<p} \forall x \,.\, \underbrace{f(f(\cdots f(x)\cdots))}_{q \text{ times}} \neq x. && \text{(no smaller orbits)}
\end{aligned}$$

This implies that the domain of any model of φ splits into some number of orbits, each one of size p. Consequently, $\mathsf{Spec}(\varphi)$ contains all non-zero multiples of p. If there are more periods $p_1, \ldots, p_n$, it suffices to consider n disjoint bijections $f_1, \ldots, f_n$ of the corresponding periodicities. □

Statement of Problem 2.8.16 "Spectra and Kleene iteration". Are spectra of first-order logic sentences closed under the iteration operation "$(\_)^+$"? □

Solution of Problem 2.8.16 "Spectra and Kleene iteration". The answer is affirmative and it follows from the arithmetical fact that, for any subset $N \subseteq \mathbb{N}$, N^+ is a semilinear set, to which we can apply Problem 2.8.15 "Semilinear sets are spectra". □

Statement of Problem 2.8.17 "Doubling". Given a first-order logic sentence φ, construct a sentence ψ s.t.

$$\mathsf{Spec}(\psi) \; = \; \{2 \cdot n \mid n \in \mathsf{Spec}(\varphi)\}. \qquad \square$$

Solution of Problem 2.8.17 "Doubling". W.l.o.g. we assume that φ does not include functional symbols. We choose one unary relational symbol U and one unary function symbol f, neither of them occurring in φ. Let $[\varphi]_U$ be obtained from φ by relativising all its quantifiers to U, similarly as in the solution of Problem 2.8.12 "Spectra are closed under addition". We express the fact that f is a permutation where every orbit has size two and in each orbit exactly one of the two elements belongs to U:

$$\psi \;\equiv\; [\varphi]_U \wedge \forall x \,.\, f(f(x)) = x \wedge f(x) \neq x \wedge (U(x) \leftrightarrow \neg U(f(x))).$$

Thus, $[\varphi]_U$ expresses the fact that the substructure consisting of the elements in U satisfies φ and f guarantees that the whole model has twice as many elements as those in U, as required. $\square$

2.8.3 Restricted formulas

Statement of Problem 2.8.18 "Spectra with only unary relations". Consider a sentence φ containing only unary relational symbols. Prove that $\mathsf{Spec}(\varphi)$ is either finite or cofinite. $\square$

Solution of Problem 2.8.18 "Spectra with only unary relations". Suppose that the quantifier rank of φ is k and let $U_1, \ldots, U_\ell$ be all unary relation symbols occurring in φ. Let $\mathfrak{A}$ be a model of φ of size $|A| \geq k \cdot 2^\ell$. We show that φ has arbitrary large models, and thus $\mathsf{Spec}(\varphi)$ is infinite. For every set of elements $X \subseteq A$, let $X^1 = X$ and $X^{-1} = A \setminus X$. The domain A is partitioned by all intersections of the form

$$U^\varepsilon = \bigcap_{i=1}^{\ell} U_i^{\varepsilon_i}, \quad \text{with } \varepsilon = \varepsilon_1 \cdots \varepsilon_\ell \in \{1, -1\}^\ell.$$

Since there are 2^ℓ such intersections, at least one such intersection U^ε has cardinality $|U^\varepsilon| \geq k$. Consider a new structure $\mathfrak{A}'$ obtained from $\mathfrak{A}$ by introducing arbitrarily many copies of elements in U^ε. An application of Ehrenfeucht-Fraïssé games shows that $\mathfrak{A} \equiv_k \mathfrak{A}'$ (c.f. Section 2.12), i.e., they satisfy the same sentences of rank $\leq k$, and thus $\mathfrak{A}' \models \varphi$. $\square$

Statement of Problem 2.8.19 "Spectra with a unary function". Find a sentence φ with only one unary *function* symbol f s.t. neither $\mathsf{Spec}(\varphi)$ nor its complement is finite. □

Solution of Problem 2.8.19 "Spectra with a unary function". We have seen in Problem 2.8.3 "Even numbers" an example of a sentence φ using only a single unary function f whose spectrum is the set of even numbers, which is infinite. Its complement is the set of odd numbers, which is also infinite. □

Statement of Problem 2.8.20. Give an example of a sentence of first-order logic φ s.t. $\mathsf{Spec}(\varphi) = \mathsf{Spec}(\neg\varphi)$ using only a single unary relation symbol U. Does such an example exists using only a unary function symbol f? □

Solution of Problem 2.8.20. Let $\varphi \equiv \exists x \,.\, U(x)$. Then $\mathsf{Spec}(\varphi) = \mathsf{Spec}(\neg\varphi) = \mathbb{N}_{>0}$. If only a unary function symbol f is allowed, then such a sentence does not exist. Indeed, up to isomorphism there is only one structure $\mathfrak{A}$ of cardinality 1 over a single unary function symbol. Therefore 1 belongs to exactly one of the sets $\mathsf{Spec}(\varphi), \mathsf{Spec}(\neg\varphi)$. □

Statement of Problem 2.8.21 "Spectra of existential sentences". Show that the spectrum of an existential first-order sentence φ is *upward closed*, in the sense that $m \in \mathsf{Spec}(\varphi)$ and $n \geq m$ imply $n \in \mathsf{Spec}(\varphi)$. *Hint: C.f. Problem 2.3.9, and also Problem 2.11.3 "Fundamental property" (point 3).* □

Solution of Problem 2.8.21 "Spectra of existential sentences". This is an easy consequence of the fact that we can add any number of fresh elements to the domain of a model of an existential first-order sentence (without changing the meaning of relations) and still obtain a model thereof. This works even in the presence of function symbols in the signature, since their interpretation can be extended arbitrarily on the fresh elements preserving the original satisfying assignment. □

Statement of Problem 2.8.22 "Spectra of universal sentences". Prove that for every first-order sentence φ there exists a universal first-order sentence ψ, perhaps over a larger signature, having the same spectrum $\mathsf{Spec}(\varphi) =$

$\mathsf{Spec}(\psi)$. What if we require that ψ uses only relational symbols? *Hint: Use Problem 2.4.2 "Skolemisation".* ☐

Solution of Problem 2.8.22 "Spectra of universal sentences". Thanks to Problem 2.4.2 "Skolemisation", we can convert φ to an equisatisfiable universal formula ψ by adding new functional symbols. It suffices to observe that skolemisation preserves and reflects not only satisfiability, but also the size of models.

If we restrict ψ to use only relational symbols, then, dually to Problem 2.8.21 "Spectra of existential sentences", $\mathsf{Spec}(\psi)$ is downward closed. ☐

Statement of Problem 2.8.23 "Spectra of $\exists^*\forall^*$-sentences". Show that the spectrum of a $\exists^*\forall^*$-sentence of first-order logic (i.e., in the so called *Bernays-Schönfinkel-Ramsey* class) using only relational symbols is either finite or cofinite. Does this hold for $\forall\exists^*$-sentences? *Hint: Use Problem 2.11.4 "Preservation for $\exists^*\forall^*$-sentences".* ☐

Solution of Problem 2.8.23 "Spectra of $\exists^*\forall^*$-sentences". Thanks to the characterisation in Problem 2.11.4 "Preservation for $\exists^*\forall^*$-sentences", if φ is an $\exists^n\forall^*$-sentence and $\mathfrak{A} \models \varphi$ has size $|A| = m$, then there are models of all cardinalities $n \leq k \leq m$. Thus, if φ has arbitrarily large models its spectrum is cofinite (and its complement has size at most n), and otherwise its spectrum is finite.

We can write a $\forall\exists$-sentence over a relational alphabet having infinite and co-infinite spectrum. Consider the solution from Problem 2.8.3 "Even numbers". It is a $\forall\exists$-sentence having as spectrum precisely the even numbers. However, it uses a unary function f. We replace f with a binary relation F and add an $\forall\exists$ axiom that F is functional.

$$\forall x \,.\, \exists y \,.\, F(x,y) \wedge \forall x,y,z \,.\, F(x,y) \wedge F(x,z) \rightarrow y = z,$$

we replace $U(f(x))$ with $\exists y \,.\, F(x,y) \wedge U(y)$, and expressions of the form $f(x) = y$ with $F(x,y)$. The resulting formula uses only a relational signature and it is in the $\forall\exists$-class, as required. ☐

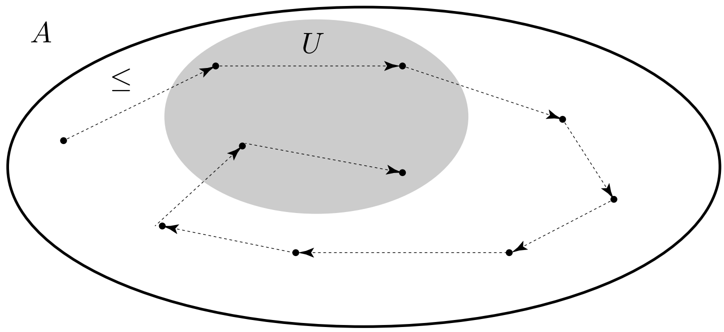


Figure for Problem 2.8.26.

2.8.4 Counting models

Statement of Problem 2.8.25. Show that the sequence $a_n = n$ is the counting spectrum of a sentence of first-order logic. □

Solution of Problem 2.8.25. Let the signature Σ consist of a single unary relation symbol U, and let φ be $\exists x\,.\,U(x)$. Each isomorphism class of models of cardinality n over Σ is uniquely determined by the number of elements in U. Therefore, there are $n+1$ such structures, and φ excludes the model with empty U, so there remain precisely n such models. □

Statement of Problem 2.8.26. Show that the sequence $a_n = 2^n$ is the counting spectrum of a sentence of first-order logic. □

Solution of Problem 2.8.26. Let the signature Σ consist of a unary relation symbol U and a binary relation symbol $\leq$, and let φ axiomatise that $\leq$ is a linear order (cf. Problem 2.6.5). Each isomorphism class of models of cardinality n over Σ is determined by selecting which elements are in U. The linear order $\leq$ is used to distinguish different elements. Therefore there are 2^n such structures. □

Statement of Problem 2.8.27. Let k be a fixed constant. Show that the sequence a_n defined as $\binom{n}{k}$ for $n \geq k$ and 0 for $n < k$ is the counting spectrum of a sentence of first-order logic. □

Solution of Problem 2.8.27. The signature Σ consists of a single unary relation symbol U and binary relation symbol $\leq$. The sentence φ is the conjunction of the axioms of linear orders and the following extra condition saying that there are precisely k elements satisfying U:

$$\exists x_1 \ldots \exists x_k \,. \bigwedge_{1 \leq i < j \leq k} x_i \neq x_k \wedge \bigwedge_{1 \leq i \leq k} U(x_i) \wedge \forall x \,. U(x) \to \bigvee_{1 \leq i \leq k} x = x_i.$$

□

Statement of Problem 2.8.28. Show that the sequence $a_n = n!$ is the counting spectrum of a sentence of first-order logic. □

Solution of Problem 2.8.28. Let φ axiomatise two linear orders $\leq_1, \leq_2$. Each isomorphism class of models of cardinality n is determined by sorting the elements according to $\leq_1$ and then describing the permutation which gives their order according to $\leq_2$. There are $n!$ such structures, as required. □

2.8.5 Characterisation

The following problem shows a complexity upper bound for spectra of first-order logic.

Statement of Problem 2.8.29 "Spectra are in NEXPTIME". Show that the following decision problem is in the complexity class NEXPTIME:

SPECTRUM MEMBERSHIP.
Input: A sentence of first-order logic φ and a number $n \in \mathbb{N}$ encoded in binary.
Output: Is it the case that $n \in \mathsf{Spec}(\varphi)$? □

Solution of Problem 2.8.29 "Spectra are in NEXPTIME". We show an NPTIME algorithm for the case when n is encoded in unary, from which the claim follows. We guess a relational model $\mathfrak{A} = (A, a_1^{\mathfrak{A}}, \ldots, a_n^{\mathfrak{A}}, R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}})$ of size $|A| = n$ together with interpretations $R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}}$ for all the relational symbols in the signature of φ (functional symbols can be treated as relations).

We transform φ into an equivalent (w.r.t. $\mathfrak{A}$) quantifier-free formula ψ by applying the following two expansion rules for quantifiers:

$$\begin{array}{lll} \exists x\,.\,\xi & \text{becomes} & \xi[x \mapsto a_1] \vee \cdots \vee \xi[x \mapsto a_n], \text{ and} \\ \forall x\,.\,\xi & \text{becomes} & \xi[x \mapsto a_1] \wedge \cdots \wedge \xi[x \mapsto a_n]. \end{array}$$

Since n is presented in unary, ψ is of size polynomial in the size if φ. Finally, we can check $\mathfrak{A} \models \psi$ in PTIME. □

2.9 Compactness

Statement of Problem 2.9.1 "Compactess theorem". Prove that if $\Gamma \models \varphi$, then there exists a finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ s.t. $\Gamma_0 \models \varphi$. *Hint: Use Gödel's completeness theorem.* □

Solution of Problem 2.9.1 "Compactess theorem". By completeness, $\Gamma \models \varphi$ implies $\Gamma \vdash \varphi$, and since proofs are finite, there are finitely many hypotheses $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ s.t. $\Gamma_0 \vdash \varphi$. By soundness, $\Gamma_0 \models \varphi$, as required. □

Statement of Problem 2.9.2 "Compactness theorem (w.r.t. satisfiability)". Sometimes the compactness theorem is stated in the following form: If every finite subset of Γ is satisfiable, then Γ is also satisfiable. Show that this alternative form is equivalent to Problem 2.9.1 "Compactess theorem". □

Solution of Problem 2.9.2 "Compactness theorem (w.r.t. satisfiability)". If Γ is unsatisfiable, then by definition $\Gamma \models \bot$, and thus by Problem 2.9.1 "Compactess theorem" there exists a finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ s.t. $\Gamma_0 \models \bot$, i.e., Γ_0 is also unsatisfiable. For the other direction, if $\Gamma \models \varphi$, then $\Gamma \cup \{\neg\varphi\}$ is unsatisfiable, and thus there exists a finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ s.t. $\Gamma_0 \cup \{\neg\varphi\}$ is unsatisfiable, i.e., $\Gamma_0 \cup \{\neg\varphi\} \models \bot$. By Problem 1.1.3 "Semantic deduction theorem", $\Gamma_0 \models \varphi$, as required. □

Statement of Problem 2.9.3 "Compactness in finite structures?" Establish whether the following variant of compactness for finite structures holds: If every *finite* model of Γ is also a model of φ, then there is a finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ with the same property. □

Solution of Problem 2.9.3 "Compactness in finite structures?" The finite variant does not hold. For instance, consider $\Gamma = \{\varphi_{\geq 1}, \varphi_{\geq 2}, \dots\}$, where $\varphi_{\geq n}$ is the sentence from Problem 2.1.6 "Cardinality constraints I" expressing that there are at least n elements in the model, and $\varphi \equiv \bot$. The set Γ has no finite models and thus it trivially satisfies the premise of the finite variant of compactness. However, every finite subset $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ admits finite models, which is a contradiction since φ has no models. □

Statement of Problem 2.9.4. Prove that if a class $\mathcal{A}$ of structures over a signature Σ and its complement $\mathsf{Mod}(\Sigma) \setminus \mathcal{A}$ are both axiomatisable by a set of first-order sentences, then each of them is definable by a first-order sentence. □

Solution of Problem 2.9.4. Assume $\mathcal{A} = \mathsf{Mod}(\Delta)$ and $\mathsf{Mod}(\Sigma) \setminus \mathcal{A} = \mathsf{Mod}(\Gamma)$. Since $\Delta \cup \Gamma$ is unsatisfiable, by compactness there are finite subsets $\Delta_0 \subseteq_{\text{fin}} \Delta$ and $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ s.t. also $\Delta_0 \cup \Gamma_0$ is unsatisfiable. We show that Δ_0 and Δ have exactly the same models, i.e., $\mathsf{Mod}(\Delta_0) = \mathsf{Mod}(\Delta)$. If $\mathfrak{A} \models \Delta_0$, then $\mathfrak{A} \not\models \Gamma_0$, which implies $\mathfrak{A} \not\models \Gamma$, and, therefore, $\mathfrak{A} \models \Delta$. The converse implication is obvious. Consequently, $\varphi \equiv \bigwedge \Delta_0$ defines $\mathcal{A}$, i.e., $\mathcal{A} = \mathsf{Mod}(\varphi)$, and similarly $\psi \equiv \bigwedge \Gamma_0$ defines $\mathsf{Mod}(\Sigma) \setminus \mathcal{A}$. □

Statement of Problem 2.9.5 "Definable separability of axiomatisable classes". We say that two disjoint classes of structures $\mathcal{A}, \mathcal{B}$ are *separated* by a class $\mathcal{C}$ if $\mathcal{A} \subseteq \mathcal{C}$ and $\mathcal{C} \cap \mathcal{B} = \varnothing$. Show that two disjoint first-order axiomatisable classes are separable by a first-order definable class. Why does this generalise Problem 2.9.4? □

Solution of Problem 2.9.5 "Definable separability of axiomatisable classes". Assume $\mathcal{A} = \mathsf{Mod}(\Delta)$ and $\mathcal{B} = \mathsf{Mod}(\Gamma)$ are disjoint. Since $\Delta \cup \Gamma$ is unsatisfiable, by compactness there are finite subsets $\Delta_0 = \{\varphi_1, \dots, \varphi_m\} \subseteq_{\text{fin}} \Delta$ and $\Gamma_0 = \{\psi_1, \dots, \psi_n\} \subseteq_{\text{fin}} \Gamma$ s.t. $\Delta_0 \cup \Gamma_0$ is already unsatisfiable. Consider the sentence

$$\varphi \equiv \varphi_1 \wedge \dots \wedge \varphi_m \wedge (\neg\psi_1 \vee \dots \vee \neg\psi_n),$$

and let $\mathcal{C} = \mathsf{Mod}(\varphi)$. We clearly have $\mathcal{C} \cap \mathcal{B} = \varnothing$, since structures in $\mathcal{B}$ satisfy all the ψ_i's. Let $\mathfrak{A} \in \mathcal{A}$. Thus, all the φ_i's are satisfied. Since $\Delta_0 \cup \Gamma_0$

is unsatisfiable, there exists some ψ_i which fails in $\mathfrak{A}$. Consequently, $\mathfrak{A}$ satisfies φ, as required. □

2.9.1 Nonaxiomatisability

Statement of Problem 2.9.6 "Finiteness is not axiomatisable". Show that there is no set of first-order sentences Δ s.t. $\mathfrak{A} \models \Delta$ if, and only if, $\mathfrak{A}$ is finite. □

Solution of Problem 2.9.6 "Finiteness is not axiomatisable". Towards reaching a contradiction, assume Δ axiomatises finiteness, and consider the set

$$\Gamma = \Delta \cup \{\varphi_{\geq 0}, \varphi_{\geq 1}, \dots\},$$

where $\varphi_{\geq n}$ is the sentence from Problem 2.1.6 "Cardinality constraints I" expressing that there are at least n elements in the model. Every finite $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ is satisfiable, since there are finite structures of arbitrarily large cardinality. By the compactness theorem, Γ is satisfiable, which is a contradiction because Γ has only infinite models. □

Statement of Problem 2.9.7 "Finite diameter is not axiomatisable". The *diameter* of a graph is the smallest $n \in \mathbb{N} \cup \{\infty\}$ s.t. any two vertices are connected by a path of length at most n. Prove that the class of graphs of finite diameter is not axiomatisable by any set of first-order logic sentences. □

Solution of Problem 2.9.7 "Finite diameter is not axiomatisable". Towards reaching a contradiction, let Δ be a purported axiomatisation. Consider the set $\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \dots\}$, where φ_n expresses that there are two vertices x, y at distance $> n$:

$$\varphi_n \equiv \exists x, y \,.\, \neg \exists x_1 \cdots x_{n-1} \,.\, E(x, x_1) \wedge E(x_1, x_2) \wedge \cdots \wedge E(x_{n-1}, y).$$

Every finite subset of Γ is satisfiable, for example by considering sufficiently long paths. By compactness, Γ is satisfiable, and thus it has a model of infinite diameter, contradicting the assumption on Δ. □

Statement of Problem 2.9.8 "Finite colourability is not axiomatisable". A *finite colouring* of a graph $\mathfrak{G} = (V, E)$ is a mapping $c : V \to C$, where C is a finite set of colours, s.t. every two vertices connected by an edge get a different colour: $(u, v) \in E$ implies $c(u) \neq c(v)$. Show that the class of finitely colourable graphs cannot be axiomatised by any set of sentences of first-order logic. □

Solution of Problem 2.9.8 "Finite colourability is not axiomatisable". Assume that Δ is the required axiomatisation, and let

$$\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \dots\},$$

where $\varphi_n \equiv \exists x_1 \dots \exists x_n \cdot \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n} E(x_i, x_j)$ expresses the existence of a n-clique in the graph. Any finite set $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ is satisfiable, since any finite clique is finitely colourable. By the compactness theorem, Γ has a model, which by definition contains arbitrarily large cliques, and thus there is no finite number of colours sufficient to colour it, which is a contradiction. □

Statement of Problem 2.9.9 "Finitely many equivalence classes is not axiomatisable". Show that the class of equivalence relations $\sim \subseteq A \times A$ containing finitely may equivalence classes (i.e., of finite index) is not axiomatisable. □

Solution of Problem 2.9.9 "Finitely many equivalence classes is not axiomatisable". We extend a purported axiomatisation Δ of being finite index as $\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \dots\}$, where φ_n says that there are at least n equivalence classes:

$$\varphi_n \equiv \exists x_1 \cdots x_n \cdot \bigwedge_{i \neq j} x_i \not\sim x_j.$$

A standard application of compactness concludes the argument, since 1) every finite subset of Γ is satisfied by an equivalence relation with sufficiently large index, and 2) all models of Γ have infinite index. □

Statement of Problem 2.9.10 "Finite equivalence classes is not axiomatisable". We want to show that the class of equivalence relations $\sim \subseteq A \times A$ where every class is finite is not axiomatisable.

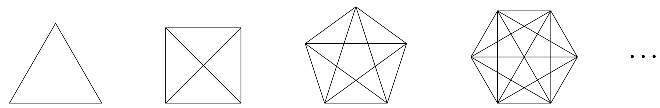


Figure for Problem 2.9.10 "Finite equivalence classes is not axiomatisable".

1. A standard way of reasoning is to extend a purported axiomatisation Δ as $\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \dots\}$, where φ_n says that there is an equivalence class containing at least n elements:

$$\varphi_n \equiv \exists x_1 \cdots \exists x_n \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge x_i \sim x_j.$$

   Do models of Γ have an infinite equivalence class?

2. If not, how can we amend the φ_n's in order to ensure that Γ has only models with an infinite equivalence class? □

Solution of Problem 2.9.10 "Finite equivalence classes is not axiomatisable". A model of Γ is only required to have arbitrarily large equivalence classes, but not necessarily an infinite one, as shown in the figure. The problem is that the equivalence classes mentioned by the φ_n's are in general different. This can be fixed by adding a new constant c to the signature, and by requiring that the same c to appear in those unbounded classes:

$$\varphi_n \equiv \exists x_1 \cdots \exists x_n \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge x_i \sim c.$$

In this way, the equivalence class of c in a model of Γ is infinite, and we can conclude by a standard application of compactness. □

Statement of Problem 2.9.11 "Finitely generated monoids are not axiomatisable". A *monoid* is a structure

$$\mathfrak{M} = (M, \circ, e),$$

where $\circ : M \times M \to M$ is an associative binary operation with neutral element $e \in M$. A monoid $\mathfrak{M}$ is *finitely generated* if there exist finitely many elements $a_1, \ldots, a_n \in M$ s.t. every $a \in M$ is a product of the a_i's. (For example, $(A^*, \cdot, \varepsilon)$ is finitely generated iff the alphabet A is finite.) Prove that the class of finitely generated monoids is not axiomatisable. □

Solution of Problem 2.9.11 "Finitely generated monoids are not axiomatisable". It suffices to add to a purported axiomatisation Δ of finitely generate monoids the sentences $\Gamma = \{\varphi_1, \varphi_2, \ldots\}$, where φ_n says that there are at least n distinct generators:

$$\varphi_n \;\equiv\; \exists x_1 \cdots x_n \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge_{i} \neg \exists y, z \,.\, y \neq e \wedge z \neq e \wedge x_i = y \cdot z.$$

Each finite subset of $\Delta \cup \Gamma$ is satisfiable by, e.g., $(\{a_1, \ldots, a_n\}^*, \cdot, \varepsilon)$, and thus we conclude by a standard application of compactness. □

Statement of Problem 2.9.12 "Cycles are not axiomatisable". Prove that the class $\mathcal{C}$ of graphs containing a cycle is not axiomatisable by any set of first-order logic sentences. □

Solution of Problem 2.9.12 "Cycles are not axiomatisable". By way of contradiction, let Δ axiomatise the existence of a cycle, and consider the set

$$\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \ldots\},$$

where $\varphi_n \;\equiv\; \neg \exists x_1 \cdots x_n \,.\, E(x_1, x_2) \wedge \cdots \wedge E(x_{n-1}, x_n) \wedge E(x_n, x_1)$ expresses that there are no cycles of length n. Every finite subset of Γ is satisfiable, since there are graphs with cycles of length n but no shorter cycle. By compactness, Γ is satisfiable, and thus it has a model without cycles of any length, contradicting the assumption on Δ. □

Statement of Problem 2.9.13 "Unions of cycles are not axiomatisable". Prove that the class $\mathcal{C}$ of graphs where every vertex belongs to a cycle is not axiomatisable by any set of first-order logic sentences. □

Solution of Problem 2.9.13 "Unions of cycles are not axiomatisable". Towards a contradiction, assume that such a set Δ of sentences exists, and consider the set

$$\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \ldots\},$$

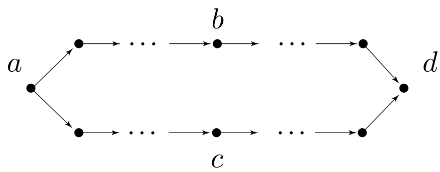


Figure for Problem 2.9.14 “The Church-Rosser property is not axiomatisable (via compactness)”.

where $\varphi_n \equiv \neg\exists x_1 \cdots x_n . E(c, x_1) \wedge \cdots \wedge E(x_{n-1}, x_n) \wedge E(x_n, c)$ for a new constant c expressing that c does not belong to a cycle of length n. Every finite subset of Γ is satisfiable, since there are models where c is on a cycle of length n but on no shorter cycle. By compactness, Γ is satisfiable, and thus it has a model where c does not belong to a cycle of any length, which contradicts the assumption on Δ. □

Statement of Problem 2.9.14 “The Church-Rosser property is not axiomatisable (via comp
A binary relation $\to \subseteq A \times A$ has the *Church-Rosser property* (CR) if, whenever $a \to^* b$ and $a \to^* c$, there exists d s.t. $b \to^* d$ and $c \to^* d$. Prove that CR is not axiomatisable by any set of first-order logic sentences. □

Solution of Problem 2.9.14 “The Church-Rosser property is not axiomatisable (via compac
Assume that Δ axiomatises CR. We add three constants a, b, c to the signature. Consider the set of sentences

$$\Gamma = \Delta \cup \{a \to b, a \to c, a \neq b, a \neq c, b \neq c\} \cup \{\varphi_1, \varphi_2, \ldots\},$$

where φ_n says that there is no d reachable from b and c in less than n steps:

$$\varphi_n \equiv \neg\exists d . \bigvee_{1 \leq i \leq n} b \to^i d \wedge \bigvee_{1 \leq j \leq n} c \to^j d.$$

Each finite subset of Γ is satisfiable, e.g., by the structure in the picture. We conclude by a standard application of compactness, since in any model of Γ no d is reachable from b and c. □

Statement of Problem 2.9.15 "Strong normalisation is not axiomatisable (via compactness)"
A binary relation $\rightarrow \subseteq A \times A$ is *strongly normalising* (SN) if there is no infinite path

$$a_1 \rightarrow a_2 \rightarrow \cdots \quad (a_1, a_2, \cdots \in A)$$

Prove that SN is not axiomatisable in first-order logic. □

Solution of Problem 2.9.15 "Strong normalisation is not axiomatisable (via compactness)"
Let Δ be a purported axiomatisation of SN. We add countably many constant symbols $a_1, a_2, \ldots$ to the signature. Consider the extension

$$\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \ldots\},$$

where φ_n says that there is a path $a_1 \rightarrow a_2 \rightarrow \cdots \rightarrow a_n$ of length n. Every finite subset of Γ is satisfiable by a sufficiently long but finite path, however every model of Γ fails SN because it contains an infinite path $a_1 \rightarrow a_2 \rightarrow \cdots$.

It is possible to avoid adding infinitely many constants at the price of introducing quantifiers: Consider the extension $\Gamma' = \Delta \cup \{\psi_1, \psi_2, \ldots\}$ where ψ_n says that there exist unique elements $x_1, \ldots, x_n$ s.t. $x_1 \rightarrow \cdots \rightarrow x_n$ and x_1 does not have a $\rightarrow$-predecessor. □

Statement of Problem 2.9.16 "Well-orders are not axiomatisable". A *well-order* is a strict total order $<$ not containing an infinite descending chain $a_0 > a_1 > \cdots$. Prove that well-orders are not axiomatisable. □

Solution of Problem 2.9.16 "Well-orders are not axiomatisable". Towards a contradiction, let Δ axiomatise a well-order. Let $C = \{c_0, c_1, \ldots\}$ be a countable set of fresh constant symbols, and consider the set of formulas

$$\Gamma = \Delta \cup \{c_0 > c_1, c_1 > c_2, \ldots\}.$$

Since there are strict total orders with arbitrarily long finite descending chains, each finite subset of Γ is satisfiable, and by compactness Γ is satisfiable, too. Its model is also a model of Δ, but it is not a well-order. □

Statement of Problem 2.9.17. Consider the class $\mathcal{A}$ of partial orders $(A, \sqsubseteq)$ with infinitely many minimal elements s.t. every non-minimal element $a \in A$ is a supremum $a = \bigsqcup B$ of finitely many minimal elements $B = \{a_1, \dots, a_n\}$. Prove that $\mathcal{A}$ is not axiomatisable by any set of sentences of first-order logic. □

Solution of Problem 2.9.17. Suppose that Δ is an axiomatisation of $\mathcal{A}$. Add a constant c to the signature and consider the extension

$$\Gamma = \Delta \cup \{\varphi_1, \varphi_2, \dots\},$$

where φ_n expresses that c is not the supremum of n minimal elements:

$$\forall x_1 \dots x_n \,.\, (\bigwedge_{1 \le i \le n} \forall y \,.\, y \not\sqsubseteq x_i) \to \neg \bigwedge_{1 \le i \le n} x_i \sqsubseteq c \wedge \forall y \,.\, (\bigwedge_{1 \le i \le n} x_i \sqsubseteq y) \to c \sqsubseteq y.$$

Every finite subset of Γ is satisfiable, e.g., by the set of finite subsets of natural numbers ordered by inclusion $(\mathcal{P}_{\text{fin}}(\mathbb{N}), \subseteq)$, by choosing the constant c to be a sufficiently large set of numbers. We conclude by a standard application of compactness, since in every model of Γ, c is not a supremum of any finite set of minimal elements. □

Statement of Problem 2.9.18. Prove that if Δ is a set of sentences s.t. $\mathsf{Spec}(\neg\varphi)$ is finite for every $\varphi \in \Delta$, and $\Delta \vDash \psi$, then $\mathsf{Spec}(\neg\psi)$ is also finite. □

Solution of Problem 2.9.18. By compactness (in the form of Problem 2.9.1 "Compactess theorem"), there exists a finite $\Delta_0 = \{\varphi_1, \dots, \varphi_n\} \subseteq_{\text{fin}} \Delta$ s.t. $\Delta_0 \vDash \psi$. Since Δ_0 is finite, this is the same as $\varphi_1 \wedge \dots \wedge \varphi_n \vDash \psi$, which in turn is equivalent to $\neg\psi \vDash \neg\varphi_1 \vee \dots \vee \neg\varphi_n$. Consequently, $\mathsf{Spec}(\neg\psi) \subseteq \mathsf{Spec}(\neg\varphi_1) \cup \dots \cup \mathsf{Spec}(\neg\varphi_n)$. The latter set is a finite union of finite sets, and hence itself finite. □

Statement of Problem 2.9.19. Consider structures $\mathfrak{A}$ over a signature consisting of binary operations $+, -, *$, constants $0, 1$, and an additional unary operation f. We say that f is *expressible* if there is a term $\tau(x)$ with one free variable x not containing f s.t.

$$\mathfrak{A} \vDash \forall x \,.\, \tau(x) = f(x).$$

(For example, if $A = \mathbb{R}$ with the usual interpretation of $+, -, *, 0, 1$, then f if expressible if it is a polynomial of one variable with integer coefficients.) Prove that the class of structures $\mathfrak{A}$ where f is expressible is not axiomatisable. □

Solution of Problem 2.9.19. Suppose that the set Δ satisfies the requirements above. Let $\tau_1(x), \tau_2(x), \ldots$ be the list of all terms no using the symbol f, and consider the extended set of axioms

$$\bar{\Delta} = \Delta \cup \{\exists x \,.\, f(x) \neq \tau_i(x) \mid i \in \mathbb{N}\}.$$

Every finite subset $\Delta_0 \subseteq_{\text{fin}} \bar{\Delta}$ contains finitely many of the additional formulas not in Δ, and thus it has a model where the arithmetic part is the standard field of real numbers and f is interpreted as some polynomial of degree higher than all degrees of all terms τ_i appearing in Δ_0. Thus Δ_0 is satisfiable, and by compactness $\bar{\Delta}$ is also satisfiable. This is, however, a contradiction because f cannot be expressible in any model of $\bar{\Delta}$. □

Statement of Problem 2.9.20. We say that a structure $\mathfrak{A}$ over signature Σ has *property F* if for any two terms s, t with one free variable x, the set of elements $a \in A$ satisfying the equation

$$\mathfrak{A}, x : a \models s = t$$

is either finite or the whole A. (For example, the field of real numbers $(F, +, *, 0, 1)$ has property F, since terms define polynomial functions, and the latter are either identically 0 or have finitely many roots.) Prove that:

1. If Σ contains only constant symbols and relation symbols, then property F is axiomatisable.

2. If Σ contains at least one unary function symbol, then property F is not axiomatisable. □

Solution of Problem 2.9.20. If the signature Σ contains only constant symbols $\{c_1, \ldots, c_n\}$ and no function symbols, then the only terms which can be constructed in this language are the c_i's or variable x. The only equations one can write in this case are $c_i = c_j$ (which has 0 solutions if $c_i^{\mathfrak{A}} = c_j^{\mathfrak{A}}$, and any element of A is a solution otherwise), $c_i = x$ (which always has 1 solution), and $x = x$ (every element of A is a solution). Therefore, $\Gamma = \varnothing$ is an axiomatisation.

If the signature Σ contains at least one unary function symbol f, then we can already build all terms of the form $f^i(x)$. By way of contradiction, assume that Γ axiomatises property F, and consider the extended set of axioms

$$\Delta = \Gamma \cup \{\varphi_1, \varphi_2, \dots\},$$

where φ_i says that there are at least i solutions to the equation $f(x) = x$ (number of fixpoints of f). Clearly Δ is finitely satisfiable, since we can build models where f has arbitrarily many fixpoints. By Problem 2.9.1 "Compactess theorem", Δ is satisfiable, and thus it has a model where f has infinitely many fixpoints, contradicting that Γ axiomatises property F. □

Statement of Problem 2.9.21 "Periodicity is not axiomatisable". Consider structures of the form $\mathfrak{A} = (A, +, s, f, 0)$, where $+$ is a binary operation, s and f are unary functions, and 0 is a constant. The function f is *periodic* if there exists $k \in A$, $k \neq 0$, s.t. $f(x + k) = f(x)$ for every $x \in A$, and *standard periodic* if k is additionally of the form $k = s^k(0)$. Consider the classes of structures where

1. f is periodic;
2. f is standard periodic;
3. f is *not* standard periodic.

For each of the classes above, determine whether it is a) definable by a single sentence; b) axiomatisable by a set of sentences, but not definable by a single sentence; c) not axiomatisable by any set of sentences. □

Solution of Problem 2.9.21 "Periodicity is not axiomatisable". Periodicity is definable by directly translating the informal prose into the single first-order logic sentence

$$\exists k \,.\, k \neq 0 \wedge \forall x \,.\, f(x + k) = x.$$

Standard periodicity, on the other hand, is not axiomatisable: By a standard compactness argument (c.f.Problem 2.9.1 "Compactess theorem"), it suffices to enlarge a purported axiomatisation Δ by the set of formulas $\Gamma = \{\varphi_1, \varphi_2, \dots\}$, where φ_n expresses that $s^n(0)$ is not a period:

$$\varphi_n \;\equiv\; \exists x\,.\, f(x + s^n(0)) \neq f(x).$$

Finally, not being standard periodic is axiomatisable by Γ above. $\square$

Statement of Problem 2.9.22. Let f be a unary function symbol, and consider the class of structures

$$\mathcal{A} = \bigcup_{n \in \mathbb{N} \setminus \{0\}} \mathsf{Mod}(\varphi_n),$$

where $\varphi_n \;\equiv\; \forall x\,.\, f^n(x) = x$ expresses that the n-th iterate of f, defined as $f^n(x) = \underbrace{f(\dots f(x)\dots)}_{n}$, is the identity function.

1. Prove that $\mathcal{A}$ cannot be axiomatised by any set of first-order sentences.
2. Can $\mathsf{Mod}(\{f\}) \setminus \mathcal{A}$ be axiomatised by *a set* of first-order sentences?
3. Prove that $\mathsf{Mod}(\{f\}) \setminus \mathcal{A}$ cannot be defined with *a single* first-order sentence. $\square$

Solution of Problem 2.9.22. By way of contradiction, let Δ be a purported axiomatisation for $\mathcal{A}$, and consider the set

$$\Gamma = \Delta \cup \{\neg\varphi_1, \neg\varphi_2, \dots\}.$$

Every finite subset of Γ is satisfiable, since there are models where f^n is the identity but no previous iterate $f^1, \dots, f^{n-1}$ is the identity. By compactness, Γ is satisfiable, and thus it has a model where no iterate of f is the identity, which is a contradiction.

The complement of $\mathcal{A}$ equals

$$\mathcal{B} = \mathsf{Mod}(\{f\}) \setminus \mathcal{A} = \bigcap_{n \in \mathbb{N} \setminus \{0\}} \mathsf{Mod}(\neg\varphi_n),$$

and thus can be axiomatised by $\{\neg\varphi_1, \neg\varphi_2, \dots\}$.

The class of structures $\mathsf{Mod}(\{f\}) \setminus \mathcal{A}$ cannot be defined with a single first-order sentence φ, because then $\neg\varphi$ would define $\mathcal{A}$, which we have just demonstrated to be impossible. $\square$

2.9.2 Extensions

Statement of Problem 2.9.23. Let A be an infinite set. Show using Problem 2.9.1 "Compactess theorem" that every partial order $\sqsubseteq\, \subseteq A \times A$ can be extended to a total order $\leq\, \subseteq A \times A$ (in the sense that $\sqsubseteq\, \subseteq\, \leq$). □

Solution of Problem 2.9.23. Let the domain be A and consider the signature consisting of a binary relation R and a constant k_a for every $a \in A$. Consider the infinite set of sentences Δ which 1) axiomatises that R is a partial order, 2) requires $R(k_a, k_b)$ whenever $a \sqsubseteq b$, and moreover 3) for every pair of elements $a, b \in A$, contains the sentence $R(k_a, k_b) \vee R(k_b, k_a)$. Every finite subset $\Gamma \subseteq_{\text{fin}} \Delta$ is satisfiable, since one can show by induction that a partial order can be extended to be total on a *finite* subset of the domain. By Problem 2.9.1 "Compactess theorem", Δ is satisfiable and thus it has a model $\mathfrak{A} = (A, R^{\mathfrak{A}})$. Then $R^{\mathfrak{A}}$ is the required total order extending $\sqsubseteq$. □

Statement of Problem 2.9.24 "Non-Archimedean reals". Consider the first-order theory $\mathsf{Th}(\mathbb{R})$ of the real numbers $(\mathbb{R}, \Sigma)$ over the signature $\Sigma = \{0, 1, +, \cdot\}$ (i.e., the set of all first-order formulas φ s.t. $\mathbb{R} \models \varphi$). The reals satisfy the following important *Archimedean property*: For all positive real numbers $a, b > 0$, there is a natural number n s.t. $n \cdot a > b$.

1. Show that the real numbers can be conservatively extended to a non-Archimedean field $\mathbb{R}^*$ in the sense that $\mathsf{Th}(\mathcal{R}) \subseteq \mathsf{Th}(\mathbb{R}^*)$ (possibly enlarging the signature). *Hint: Force an arbitrarily large element.*

2. Is it possible that $\mathbb{R}^*$ satisfies a formula over the common signature Σ not satisfied by $\mathbb{R}$, i.e., that $\mathsf{Th}(\mathcal{R}) \neq \mathsf{Th}(\mathbb{R}^*) \cap \mathsf{Th}(\Sigma)$?

□

Solution of Problem 2.9.24 "Non-Archimedean reals". Consider a new constant symbol suggestively written as "∞" and consider the infinite set of axioms

$$\Gamma = \mathsf{Th}(\mathbb{R}) \cup \{0 < \infty, 1 < \infty, 1 + 1 < \infty, \dots\}.$$

Clearly, Γ is finitely satisfiable, since we can choose ∞ to be a sufficiently large (standard) real number $c \in \mathbb{R}$. By Problem 2.9.2 "Compactness theorem (w.r.t. satisfiability)", Γ is satisfiable, i.e., it has a model $(\mathbb{R}^*, 0, 1, +, \cdot, \infty)$ s.t. $\mathbb{R}^* \vDash \Gamma$. We have the following chain of inclusions:

$$\mathsf{Th}(\mathbb{R}) \subseteq \Gamma \subseteq \mathsf{Th}(\Gamma) \subseteq \mathsf{Th}(\mathbb{R}^*), \tag{2.4}$$

where the last inclusion holds since $\mathbb{R}^* \vDash \mathsf{Th}(\Gamma)$. If we now take $a = 1$ and $b = \infty$ we have:

- $\mathbb{R}^* \vDash a > 0$ since $0 < 1 \in \mathsf{Th}(\mathbb{R}) \subseteq \mathsf{Th}(\mathbb{R}^*)$,
- $\mathbb{R}^* \vDash b > 0$ since $0 < \infty \in \Gamma \subseteq \mathsf{Th}(\mathbb{R}^*)$, and
- there is no natural number n s.t. $\mathbb{R}^* \vDash a \cdot n > b$ because $n < \infty \in \Gamma$, and thus $\mathbb{R}^* \vDash 1 \cdot n < \infty$.

Thus $\mathbb{R}^*$ is non-Archimedean.

Since the theory of a structure is always complete, then over the common signature $\mathbb{R}$ and $\mathbb{R}^*$ satisfy the same first-order properties. Indeed, by way of contradiction assume $\varphi \in \mathsf{Th}(\mathbb{R}^*) \cap \mathsf{Th}(\Sigma)$ (i.e., without the symbol "∞") but $\varphi \notin \mathsf{Th}(\mathbb{R})$. Since $\mathsf{Th}(\mathbb{R})$ is complete (like the theory of any structure), $\neg\varphi \in \mathsf{Th}(\mathbb{R})$, and since $\mathsf{Th}(\mathbb{R}^*)$ is consistent (like the theory of any structure), $\neg\varphi \notin \mathsf{Th}(\mathbb{R}^*)$, which is a contradiction to (2.4). $\square$

Statement of Problem 2.9.25. The compactness theorem is a purely semantic statement. Its proof in Problem 2.9.1 "Compactess theorem" using completeness, and thus referring to proofs can be considered unsatisfactory. Prove the compactness theorem for first-order logic by using Problem 2.5.3 and Problem 1.5.1 "Compactness theorem for propositional logic". $\square$

Solution of Problem 2.9.25. Fix a signature Σ and let $\Xi = \{\xi_0, \xi_1, \dots\} \subseteq \mathsf{Th}(\Sigma)$ be a finitely satisfiable set of first-order sentences over Σ. We need to show that Ξ is satisfiable. Apply skolemisation to every sentence in Ξ according to Problem 2.4.2 "Skolemisation" to obtain the following set of *universal* sentences

$$\Delta = \{\varphi_i \mid \varphi_i \text{ is the skolemisation of } \xi_i\}$$

over an extended signature $\Sigma' \supseteq \Sigma$. Since each ξ_i is equisatisfiable with φ_i and skolemisation commutes with conjunction (finite or infinite), we have that Δ is finitely satisfiable (since Ξ is) and moreover it is equisatisfiable with Ξ. It thus suffices to show that Δ is satisfiable. We can assume w.l.o.g. that $\varphi_i \equiv \forall \bar{x} \,.\, \psi_i$ is in PNF with ψ_i quantifier-free.

Consider now Γ from (2.3). (For this step to go through we need that Σ' contains at least one constant symbol. This can be assumed w.l.o.g. since we consider only non-empty structures and thus adding a constant symbol preserves satisfiability.) By the implication "3 → 2" of Problem 2.5.3, it suffices to show that Γ is satisfiable.

Notice that Γ is finitely satisfiable. Let $\Gamma_0 \subseteq_{\text{fin}} \Gamma$ be a finite subset thereof. There exists a finite subset $\Delta_0 \subseteq_{\text{fin}} \Delta$ s.t.

$$\Gamma_0 \subseteq \{\psi_i[x_1 \mapsto u_1]\cdots[x_n \mapsto u_n] \mid (\forall x_1, \ldots, x_n \,.\, \psi_i) \in \Delta_0 \text{ and } u_1 \in U, \ldots, u_n \in U\}.$$

Since Δ is finitely satisfiable, Δ_0 is satisfiable and thus has a model $\mathfrak{A}$. By the inclusion above, $\mathfrak{A}$ is also a model for Γ_0, and thus Γ_0 is satisfiable, as required.

Consider now Γ^{p} from (2.4). Since Γ is finitely satisfiable in the sense of first-order logic, by the same reasoning as in the proof of "3 → 4" of Problem 2.5.3 Γ^{p} is finitely satisfiable in the sense of propositional logic. By Problem 1.5.1 "Compactness theorem for propositional logic", Γ^{p} is satisfiable in the sense of propositional logic, and thus by the implication "4 → 3" of Problem 2.5.3, Γ it is satisfiable in the sense of first-order logic, as required. □

2.10 Skolem-Löwenheim theorems

2.10.1 Going upwards

Statement of Problem 2.10.2 "Hessenberg theorem". Show that for each infinite cardinal $\mathfrak{m}$, we have $\mathfrak{m}^2 = \mathfrak{m}$. *Hint: Express that the cardinality of the universe is not smaller than the cardinality of its Cartesian square. Show that the sentence has an infinite model and use Theorem 2.10.1 "Upward Skolem-Löwenheim theorem".* □

Solution of Problem 2.10.2 "Hessenberg theorem". We extend the signature with a functional symbol $f : A^2 \to A$. We express that f is a bijection, and thus $|A|^2 = |A|$, with the sentence

$$\begin{aligned}\varphi \equiv\ & \forall x, y, x', y' \,.\, ((x \neq x' \vee y \neq y') \to f(x,y) \neq f(x',y')) \wedge \\ & \forall z \,.\, \exists x, y \,.\, f(x,y) = z.\end{aligned}$$

This sentence has an infinite countable model, such as $\aleph_0 = \aleph_0^2$. By Theorem 2.10.1 "Upward Skolem-Löwenheim theorem", for any infinite cardinal $\mathfrak{m}$, φ has a model $\mathfrak{B}$ of cardinality $\mathfrak{m}$. In particular, $f^{\mathfrak{B}} : B^2 \to B$ is a bijection, hence $\mathfrak{m}^2 = \mathfrak{m}$. □

Statement of Problem 2.10.3. Is there a set of first-order logic sentences over a finite signature, which has finite models of every even cardinality, but has no model of the continuum cardinality $\mathfrak{c}$? □

Solution of Problem 2.10.3. This is not possible. The described collection of sentences should have an infinite model, by a standard application of compactness. Then, according to Theorem 2.10.1 "Upward Skolem-Löwenheim theorem", it should have a model of cardinality $\mathfrak{c}$. □

Statement of Problem 2.10.4 "Infinite axiomatisability?" We want to extend Problem 2.1.8 "Characteristic sentences" to deal with countable structures over a countable signature

$$\mathfrak{A} = (\{a_1, a_2, \ldots\}, R_1^{\mathfrak{A}}, R_2^{\mathfrak{A}}, \ldots)$$

Is it possible to find a countable set of sentences $\Delta_{\mathfrak{A}}$ s.t., for every structure $\mathfrak{B}$,

$$\mathfrak{B} \vDash \Delta_{\mathfrak{A}} \qquad \text{if, and only if,} \qquad \mathfrak{B} \cong \mathfrak{A}?$$ □

Solution of Problem 2.10.4 "Infinite axiomatisability?" This is not possible. By Theorem 2.10.1 "Upward Skolem-Löwenheim theorem", any countable set of sentences over a countable signature (such as $\Delta_{\mathfrak{A}}$) which has a countable model (such as $\mathfrak{A}$), must have an uncountable model $\mathfrak{B}$ as well, contradicting $\mathfrak{B} \cong \mathfrak{A}$ by a cardinality argument. □

Statement of Problem 2.10.5 "Nowhere dense orders". A strict linear order $\mathfrak{A} = (A, <)$ is *nowhere dense* if for any two elements $x, y \in A$ with $x < y$, there are only finitely many elements $z \in A$ s.t. $x < z < y$. Show that nowhere dense linear orders cannot be axiomatised in first-order logic. □

First solution (via compactness) of Problem 2.10.5 "Nowhere dense orders". Assume that Δ is the required axiomatisation, and add two new constants c, d to the signature. Consider the set of sentences

$$\bar{\Delta} = \Delta \cup \{\exists x_1, \ldots, x_n \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge_{i=1}^{n} c < x_i < d \mid n \in \mathbb{N}\}.$$

We show that $\bar{\Delta}$ satisfies the assumptions of the compactness theorem. Let $\Delta_0 \subseteq_{\text{fin}} \bar{\Delta}$ be an arbitrary finite subset of $\bar{\Delta}$, and let N be the maximum number of quantifiers in sentences in $\Delta_0 \setminus \Delta$. Then Δ_0 has a model $(\mathbb{Z}, <, c, d)$ where we interpret c and d as two elements of distance larger than N, such as 0 and $N + 1$. By virtue of the compactness theorem, $\bar{\Delta}$ has a model, and, by the definition of $\bar{\Delta}$, it contains infinitely many elements between the interpretations of c and d, so it is not nowhere dense, leading to a contradiction. □

Second solution (via Skolem-Löwenheim) of Problem 2.10.5 "Nowhere dense orders". Let $\mathfrak{A} = (a, <)$ be any nowhere dense order, and fix an element $a \in A$. Let $d(x, y) = 1 + |\{z \in A \mid x < z < y \text{ or } y < z < x\}|$. Then A can be expressed as a countable union of finite sets $\bigcup_{n \in \mathbb{N}} \{x \in A \mid d(x, a) \leq n\}$, and thus it is itself countable. (Indeed, if some $b \in A$ had not belonged to the union, then the number of elements between b and a would have been infinite, which is impossible in a nowhere dense order.) It follows that there is no uncountable nowhere dense order, and there is a countable nowhere dense order $(\mathbb{Z}, <)$. This contradicts Theorem 2.10.1 "Upward Skolem-Löwenheim theorem". □

2.10.2 Going downwards

Statement of Problem 2.10.7. Let $\mathcal{A}$ be an axiomatisable class of structures over a countable signature Σ. Show that if there is an infinite structure not in $\mathcal{A}$, then there is a countable structure not in $\mathcal{A}$. □

Solution of Problem 2.10.7. Let Γ be an axiomatisation for $\mathcal{A}$, and assume $\mathfrak{A} \notin \mathcal{A}$. The set of sentences $\mathsf{Th}(\mathfrak{A})$ satisfied by $\mathfrak{A}$ contains at least one sentence not in Γ: $\mathsf{Th}(\mathfrak{A}) \nsubseteq \Gamma$. By Theorem 2.10.6 "Downward Skolem-Löwenheim theorem", the theory $\mathsf{Th}(\mathfrak{A})$ has a countable model $\mathfrak{B}$ s.t. $\mathfrak{B} \not\models \Gamma$, as required. □

Statement of Problem 2.10.8. Let A be a fixed set. Consider the class $\mathcal{A}$ of structures isomorphic to $(A^{\mathbb{N}}, R)$, where $A^{\mathbb{N}}$ is the set of all infinite sequences of elements of A and $R(x, y)$ holds if, and only if, the set of positions at which x and y differ is finite. Prove that $\mathcal{A}$ is axiomatisable in first-order logic if, and only if, $|A| = 1$. □

Solution of Problem 2.10.8. If $A = \{a\}$, then there is only one element in the model $A^{\mathbb{N}} = \{aa\cdots\}$ and R is the identity, yielding the axiomatisation:

$$\{\exists x \,.\, \forall y \,.\, y = x \wedge \forall x, y \,.\, R(x, y) \leftrightarrow x = y\}.$$

Now assume $|A| > 1$. Since $A^{\mathbb{N}}$ is uncountable, the class $\mathcal{A}$ contains only uncountable structures. If $\mathcal{A}$ were axiomatisable by a set of first-order sentences Γ, then Γ would have a model of at most countable cardinality by the Theorem 2.10.6 "Downward Skolem-Löwenheim theorem", contradicting that $\mathcal{A}$ contains only uncountable structures. □

Statement of Problem 2.10.9. Prove that the class of all algebras $\mathfrak{A} = (A, f)$, where f is a unary function symbol, s.t. $|f(A)| < |A|$ (the cardinality of the codomain of f is strictly smaller than the cardinality of the universe), is not axiomatisable in first-order logic. □

Solution of Problem 2.10.9. Assume that Γ axiomatises the class and consider the extended set

$$\Delta = \Gamma \cup \{\exists x_1, \dots, x_n \,.\, \bigwedge_{i \neq j} f(x_i) \neq f(x_j) \mid n \in \mathbb{N}\}.$$

Every finite subset of Δ has a model where $|f(A)| > n$, and thus by compactness Δ has an infinite model where $|f(A)|$ is infinite. Since the signature is finite, by the Skolem-Löwenheim theorem Δ has a countable model $\mathfrak{A}$. Since $|f(A)|$ is countable in $\mathfrak{A}$, we have $|f(A)| = |A|$, which is a contradiction. □

Statement of Problem 2.10.10 "Function semigroups". Consider a signature with a binary operation $\circ$ and a constant symbol id. A model $\mathfrak{F}$ over this signature is called a *function semigroup* if its carrier is the set of all functions $f : A \to A$ on some set A, $\circ$ is function composition, and id is the identity function. Prove that the class of function semigroups cannot be axiomatised in first-order logic. □

Solution of Problem 2.10.10 "Function semigroups". Since there are infinite function semigroups and the signature is finite, if it were axiomatisable by a set of first-order sentences, then by Theorem 2.10.6 "Downward Skolem-Löwenheim theorem" it should also contain a countable structure. However the set of functions $A \to A$ is never countable when A is infinite. □

Statement of Problem 2.10.11. Prove that the class of all structures isomorphic to $\mathfrak{A} = (\mathcal{P}(A), \cup, \cap, \subseteq)$, where $\cup, \cap$ are the binary operations of union, resp., intersection, and $\subseteq$ is the set containment relation, is not axiomatisable in first-order logic. □

Solution of Problem 2.10.11. The class contains infinite structures, and the signature is finite. If the class were axiomatisable with a set of first-order sentences, then by Theorem 2.10.6 "Downward Skolem-Löwenheim theorem" it would also contain a countable structure. But such a structure does not exist, because the cardinality of $\mathcal{P}(A)$ is never countable when A is infinite. □

Statement of Problem 2.10.12. Prove that there are three isomorphism closed classes $\mathcal{A} \subseteq \mathcal{B} \subseteq \mathcal{C}$ of structures over the same finite signature, such that:

- $\mathcal{B}$ is not axiomatisable even though $\mathcal{A}$ and $\mathcal{C}$ are.
- $\mathcal{B}$ is axiomatisable even though $\mathcal{A}$ and $\mathcal{C}$ are not. □

Solution of Problem 2.10.12.

- Take $\mathcal{B}$ to be any nonaxiomatisable class of structures. It is sandwiched between the empty class defined by $\bot$ and the complete class defined by $\top$.

- Let $\mathcal{B}$ be an axiomatisable class of structures over a finite signature s.t. there is an infinite structure in the class $\mathfrak{A} \in \mathcal{B}$ and an infinite structure not in the class $\mathfrak{B} \notin \mathcal{B}$.

  We can assume that $\mathfrak{A}$ is countable by Theorem 2.10.6 "Downward Skolem-Löwenheim theorem", and that $\mathfrak{B}$ is countable by Problem 2.10.7 By Theorem 2.10.1 "Upward Skolem-Löwenheim theorem" there exist uncountable structures elementarily equivalent to $\mathfrak{A}$, resp., $\mathfrak{B}$. Let $\mathcal{A}$ be $\mathcal{B}$ with all uncountable structures elementarily equivalent to $\mathfrak{A}$ removed, and let $\mathcal{C}$ be $\mathcal{B}$ with all uncountable structures elementarily equivalent to $\mathfrak{B}$ added. Neither $\mathcal{A}$ nor $\mathcal{B}$ is axiomatisable because they do not satisfy the Skolem-Löwneheim theorem. □

2.11 Relating models

2.11.1 Relational homomorphisms

Statement of Problem 2.11.2. Show that a relational homomorphism R preserves the meaning of terms, in the sense that, for any term t,

$$(\varrho, \sigma) \in R \quad \text{implies} \quad (\llbracket t \rrbracket^{\mathfrak{A}}_{\varrho}, \llbracket t \rrbracket^{\mathfrak{B}}_{\sigma}) \in R.$$

Additionally equality of terms is preserved when R is injective:

$$\llbracket u \rrbracket^{\mathfrak{A}}_{\varrho} = \llbracket v \rrbracket^{\mathfrak{A}}_{\varrho} \quad \text{implies} \quad \llbracket u \rrbracket^{\mathfrak{B}}_{\sigma} = \llbracket v \rrbracket^{\mathfrak{B}}_{\sigma}. \qquad \square$$

Solution of Problem 2.11.2. This follows by a straightforward induction on the structure of terms, where $(\varrho, \sigma) \in R$ is used to prove the base case of variables. □

Statement of Problem 2.11.3 "Fundamental property". Let R be a relational homomorphism between $\mathfrak{A}$ and $\mathfrak{B}$, and consider formulas without equality. Show that

1. All positive quantifier-free formulas are preserved.
2. If R is (left) total, then it preserves all positive existential formulas.
3. If R is total and faithful, then it preserves all existential formulas.

4. If R is surjective (right total), then it preserves all positive universal formulas.

5. If R is surjective and faithful, then it preserves all universal formulas.

6. If R is total and surjective, then it preserves all positive formulas.

7. If R is total, surjective, and faithful, then it preserves all formulas.

8. If R is injective, then it preserves formulas with equality. □

Solution of Problem 2.11.3 "Fundamental property". We assume that the formula φ is in NNF, and thus negations (if any) appear only in front of atomic formulas. We prove (2.6) by structural induction on φ. Assume $(\varrho, \sigma) \in R$. The base case is handled directly by the definition of relational homomorphism and Problem 2.11.2:

$$\mathfrak{A}, \varrho \models R_j(\bar{t}) \quad \text{implies} \quad \mathfrak{B}, \sigma \models R_j(\bar{t}).$$

The positive inductive cases involving "$\vee$" and "$\wedge$" are immediate. This proves the first point. The other points are proved by a combination of the following observations.

If R is faithful, then the induction goes through negation (applied to atomic formulas):

$$\mathfrak{A}, \varrho \models \neg R_j(\bar{t}) \quad \text{implies} \quad \mathfrak{B}, \sigma \models \neg R_j(\bar{t}).$$

If R is total, then the induction goes through existential formulas:

$$\mathfrak{A}, \varrho \models \exists x \,.\, \varphi \quad \text{implies} \quad \mathfrak{B}, \sigma \models \exists x \,.\, \varphi.$$

Indeed, take $a \in A$ s.t. $\mathfrak{A}, \varrho[x \mapsto a] \models \varphi$. Since R is total, there is $b \in B$ s.t. $(a, b) \in R$, and thus $(\varrho[x \mapsto a], \sigma[x \mapsto b]) \in R$ too. By the inductive assumption, $\mathfrak{B}, \sigma[x \mapsto b] \models \varphi$, and thus $\mathfrak{B}, \sigma \models \exists x \,.\, \varphi$, as required.

If R is surjective, then we can handle universal formulas as well:

$$\mathfrak{A}, \varrho \models \forall x \,.\, \varphi \quad \text{implies} \quad \mathfrak{B}, \sigma \models \forall x \,.\, \varphi.$$

Indeed, let $b \in B$ be arbitrary. Since R is surjective, there is $a \in A$ s.t. $(a, b) \in R$. Thus, $\mathfrak{A}, \varrho[x \mapsto a] \models \varphi$, and since $(\varrho[x \mapsto a], \sigma[x \mapsto b]) \in R$, by the inductive hypothesis we get $\mathfrak{B}, \sigma[x \mapsto b] \vDash \varphi$. Since b was arbitrary, we have $\mathfrak{B}, \sigma \vDash \forall x . \varphi$, as required.

Regarding the last point, assume that R is injective. This suffices to show that R preserves equalities:

$$\mathfrak{A}, \varrho \vDash u = v \quad \text{implies} \quad \mathfrak{B}, \sigma \vDash u = v.$$

Indeed, by Problem 2.11.2 applied twice we get $([\![u]\!]^{\mathfrak{A}}_{\varrho}, [\![u]\!]^{\mathfrak{B}}_{\sigma}) \in R$ and $([\![v]\!]^{\mathfrak{A}}_{\varrho}, [\![v]\!]^{\mathfrak{B}}_{\sigma}) \in R$. Since $[\![u]\!]^{\mathfrak{A}}_{\varrho} = [\![v]\!]^{\mathfrak{A}}_{\varrho}$ by assumption, thanks to injectivity we get $[\![u]\!]^{\mathfrak{B}}_{\sigma} = [\![v]\!]^{\mathfrak{B}}_{\sigma}$, as required. □

Statement of Problem 2.11.4 "Preservation for $\exists^* \forall^*$-sentences". Show that for every $\exists^n \forall^*$-sentence of first-order logic φ over a signature without function symbols, if $\mathfrak{A} \vDash \varphi$, then there exists a *core* $C \subseteq A$ of at most n elements s.t. every induced substructure $\mathfrak{B}$ of $\mathfrak{A}$ containing $C \subseteq B$ is also a model $\mathfrak{B} \vDash \varphi$. □

Solution of Problem 2.11.4 "Preservation for $\exists^* \forall^*$-sentences". Let $\varphi \equiv \exists x_1, \ldots, x_n . \psi$ with ψ universal and assume $\mathfrak{A} \vDash \varphi$. There exists a variable valuation $\varrho = (x_1 \mapsto a_1, \ldots, x_n \mapsto a_n)$ s.t. $\mathfrak{A}, \varrho \vDash \psi$. Let the core be $C = \{a_1, \ldots, a_n\}$. Since ψ is universal, the rest of the argument is analogous to the easy direction of Problem 2.13.13 "Łoś-Tarski's theorem". □

2.11.2 Isomorphisms

Statement of Problem 2.11.6 "Isomorphism theorem". Show that $\mathfrak{A} \cong_h \mathfrak{B}$ implies that, for every formula φ and for every valuation ϱ of $\mathfrak{A}$,

$$\mathfrak{A}, \varrho \vDash \varphi \quad \text{if, and only if} \quad \mathfrak{B}, \varrho \circ h^{-1} \vDash \varphi. \qquad \square$$

Solution of Problem 2.11.6 "Isomorphism theorem". We apply Problem 2.11.3 "Fundamental property" since an isomorphism is a relational homomorphism which is total, injective, surjective, and faithful. □

Statement of Problem 2.11.7. Are $(\mathbb{R}, +)$ and $(\mathbb{R}_+, *)$ isomorphic? □

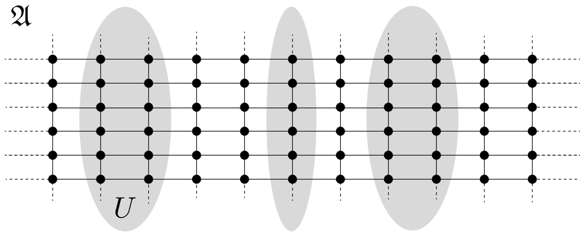


Figure for Problem 2.11.8.

Solution of Problem 2.11.7. Yes, each exponential function $\lambda x.a^x$, with $a > 0$, is an isomorphism. □

Statement of Problem 2.11.8. Consider the coloured graph $\mathfrak{A} = (\mathbb{Z}\times\mathbb{Z}, E, U)$, where the edge relation E is defined as

$$(x, y, x', y') \in E \text{ iff } (x = x' \text{ and } |y - y'| = 1) \text{ or } (|x - x'| = 1 \text{ and } y = y'),$$

and $U \subseteq \mathbb{Z} \times \mathbb{Z}$ is a unary relation. Is it possible to define in first-order logic that U is a union of complete columns? □

Solution of Problem 2.11.8. No, this is not possible since being a union of complete columns is not invariant under isomorphism. Take $\mathfrak{A} = (\mathbb{Z} \times \mathbb{Z}, E, U^{\mathfrak{A}})$ and $\mathfrak{B} = (\mathbb{Z} \times \mathbb{Z}, E, U^{\mathfrak{B}})$, where

$$U^{\mathfrak{A}} = \{(x, 0) \mid x \in \mathbb{Z}\} \quad \text{and} \quad U^{\mathfrak{B}} = \{(0, y) \mid y \in \mathbb{Z}\}.$$

The mapping $h : (x, y) \mapsto (y, x)$ from $\mathbb{Z} \times \mathbb{Z}$ into itself is an isomorphism $\mathfrak{A} \cong_h \mathfrak{B}$, but $\mathfrak{A}$ satisfies the considered property and $\mathfrak{B}$ does not. □

Statement of Problem 2.11.9. Construct a set Δ of first-order sentences s.t. every two *countable* models thereof are isomorphic (i.e., Δ is $\aleph_0$-categorical), but there exist two uncountable nonisomorphic models of Δ of the same cardinality (i.e., Δ is not κ-categorical for some $\kappa > \aleph_0$). □

Solution of Problem 2.11.9. Let Δ be the set of axioms of dense linear orders without maximal and minimal elements. Every two countable orders of this kind are isomorphic thanks to Problem 2.12.12 "Countable EF-games". On the other hand, there exist two such nonisomorphic orders of cardinality of the continuum. One of them is $(\mathbb{R}, \leq)$, and the other is the same with another copy of itself appended to the right. Both structures are dense and without endpoints. It remains to observe that every bounded subset of the former has a supremum, while there are bounded subsets of the latter without a supremum. Suprema are preserved by isomorphisms, hence the two are not isomorphic. □

2.11.3 Elementary equivalence

Statement of Problem 2.11.11. Show that isomorphic structures are elementarily equivalent: $\mathfrak{A} \cong \mathfrak{B}$ implies $\mathfrak{A} \equiv \mathfrak{B}$. □

Solution of Problem 2.11.11. This follows immediately from Problem 2.11.6 "Isomorphism theorem", since isomorphisms preserve and reflect valid sentences. □

Statement of Problem 2.11.12. Is it the case that $(\mathbb{R}, +, *) \equiv (\mathbb{Q}, +, *)$? □

Solution of Problem 2.11.12. This is not the case, since the sentence

$$\exists x\,.\,(\forall y\,.\,x * y = y) \wedge \exists y\,.\,y * y = x + x$$

expresses that $\sqrt{1+1}$ exists, which is true in the first structure, and false in the second. □

2.12 Ehrenfeucht-Fraïssé games

2.12.1 Equivalent structures

Statement of Problem 2.12.3. Is it the case that

$$(\mathbb{Q}, <) \equiv (\mathbb{R}, <)?$$

Are the two structures above isomorphic? □

Solution of Problem 2.12.3. The rationals and the reals are not isomorphic due to a trivial counting argument—the reals are uncountable while the rationals are countable. Nonetheless, they are elementarily equivalent. This can be proved by showing that Player II wins $G_k((\mathbb{Q},<),(\mathbb{R},<))$ for every $k \in \mathbb{N}$. We prove that she even wins the infinite game $k = \infty$. Player II maintains the following invariant: Let $a_1,\dots,a_m \in \mathbb{Q}$ and $b_1,\dots,b_m \in \mathbb{R}$ be the elements selected so far. Then, for every $i,j \in \{1,\dots,m\}$,

$$a_i < a_j \quad \text{if, and only if,} \quad b_i < b_j.$$

The invariant above ensures that Player II wins the game. In the first round, Player II can establish the invariant by an arbitrary choice. At round $m+1$, if Player I plays $a_{m+1} \in \mathbb{Q}$, then Player II has the obvious reply $b_{m+1} = a_{m+1} \in \mathbb{R}$, thus establishing the invariant. If Player I plays $b_{m+1} \in \mathbb{R}$ instead, then there are three cases to consider.

1. If b_{m+1} is larger than any other b_i's, then Player II can pick $a_{m+1} \in \mathbb{Q}$ larger than any other a_i's.

2. The case when b_{m+1} is the new least element is analogous.

3. Finally, let $b_i < b_{m+1} < b_j$ with b_i maximal and b_j minimal. Then Player II replies with $a_{m+1} = \frac{a_i+a_j}{2} \in \mathbb{Q}$, thus establishing the invariant as required. □

Statement of Problem 2.12.4. Prove that the structures $(\mathbb{Q}\times\mathbb{Z},\leq)$ and $(\mathbb{R}\times\mathbb{Z},\leq)$, ordered lexicographically using the natural orders on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, are elementarily equivalent. □

Solution of Problem 2.12.4. An argument very similar as in Problem 2.12.3 can be used. Whenever Player I plays in the first component in one structure, then Player II replies in the same component in the other structure as in Problem 2.12.3. Whenever Player I plays in the second component in one structure, then Player II replies with the same element in the same component in the other structure. □

Statement of Problem 2.12.5. Consider a finite directed cycle $\mathfrak{A}_n$ of size 2^n (number of vertices) and a path infinite in both directions $\mathfrak{B}$. From a trivial counting argument, $\mathfrak{A}_n$ and $\mathfrak{B}$ can be distinguished by a sentence of rank $2^n + 1$ using only the equality symbol (c.f. Problem 2.1.6 "Cardinality constraints I"). However, if we additionally allow the edge relation "E" sentences of smaller rank suffice. What is the smallest k s.t. Player I wins $G_k(\mathfrak{A}_n, \mathfrak{B})$? □

Solution of Problem 2.12.5. Player II wins for $k = n$ and loses for any larger value. Player II ensures that the distance of close vertices is preserved while far vertices need to remain far, but the exact distance is unimportant. Let $h \in \mathbb{N}$ be a threshold. We say that two integers $x, y \in \mathbb{Z}$ are *h-threshold equivalent*, written $x \approx_h y$, if the following condition holds:

$$x \approx_h y \quad \text{if, and only, if} \quad \text{either } x = y, \text{ or } x, y \geq h.$$

Player II maintains the following invariant: Let $a_1, \ldots, a_m \in A$ and $b_1, \ldots, b_m \in B$ be the elements selected up to and including round m. For every $i, j, k \in \{1, \ldots, m\}$,

$$\begin{aligned}&(1)\ d(a_i, a_j) \approx_{2^{n-m+1}} d(b_i, b_j), \text{ and}\\ &(2)\ K(a_i, a_j, a_k) \text{ iff } K(b_i, b_j, b_k),\end{aligned}$$

where the distance $d(a, b) \in \mathbb{N} \cup \{\infty\}$ is the length of the shortest path from a to b, and $K(a_i, a_j, a_k)$ is the *cyclic order* relation saying that a_j is visited when going clockwise from a_i to a_k (we interpret $\mathfrak{B}$ as a cyclic order too). First of all, this is winning since after the last round $m = n$, we have $d(a_i, a_j) \approx_2 d(b_i, b_j)$, which means precisely $E(a_i, a_j)$ iff $E(b_i, b_j)$, as required. The invariant can be established at the first round by an arbitrary response of Player II.

At round $m + 1$, let Player I select $b_{m+1} \in B$. Let b_i be the rightmost (largest) point and b_j the leftmost (smallest) point s.t. $K(b_i, b_{m+1}, b_j)$ holds. By the invariant (2), it follows that there is no a_k visited when going clockwise from a_i to a_j, i.e., $K(a_i, a_k, a_j)$. Player II replies with some point a_{m+1} s.t. $K(a_i, a_{m+1}, a_j)$ holds (thus satisfying condition (2)) to be determined as follows. If $d(b_i, b_j) < 2^{n-m+1}$, then by the inductive hypothesis we have $d(a_i, a_j) = d(b_i, b_j)$ and Player two selects the unique

a_{m+1} s.t.

$$d(a_i, a_{m+1}) = d(b_i, b_{m+1}) \text{ and } d(a_{m+1}, d_j) = d(b_{m+1}, d_j),$$

thus satisfying condition (1). If $d(b_i, b_j) \geq 2^{n-m+1}$ (including the case when $d(b_i, b_j) = \infty$), then $d(a_i, a_j) \geq 2^{n-m+1}$ by the inductive assumption. There are three sub-cases to consider.

1. If $d(b_i, b_{m+1}) < 2^{n-(m+1)+1}$, then Player II (necessarily) selects a_{m+1} as the unique point satisfying

$$d(a_i, a_{m+1}) = d(b_i, b_{m+1}).$$

2. The case $d(b_{m+1}, d_j) < 2^{n-(m+1)+1}$ is analogous.

3. Finally, assume $d(b_i, b_{m+1}), d(b_{m+1}, b_j) \geq 2^{n-(m+1)+1}$. By assumption, $d(a_i, a_j) \geq 2^{n-m+1}$, and thus Player II can pick some a_{m+1} in the middle between a_i and a_j satisfying $d(a_i, a_{m+1}), d(a_{m+1}, a_j) \geq 2^{n-(m+1)+1}$.

The construction when Player I plays $a_{m+1} \in A$ is very similar. The only modification is in 3. above in the case that b_i is to the right of b_j: In this case, Player II needs to break symmetry and will select b_{m+1} to be at any distance $\geq 2^{n-(m+1)+1}$ to the right of b_i (the symmetric choice to the left of b_j would work too). □

Statement of Problem 2.12.6. Show that the following two structures cannot be distinguished by any sentence of first-order logic (c.f. problem figure):

$$\begin{aligned} \mathfrak{A} &= (\mathbb{N}, \leq), \text{ and} \\ \mathfrak{B} &= (\{1 - \tfrac{1}{n} \mid n > 0\} \cup \{1 + \tfrac{1}{n} \mid n > 0\} \cup \{3 - \tfrac{1}{n} \mid n > 0\}, \leq). \end{aligned}$$ □

Solution of Problem 2.12.6. We show that Player II wins $G_k(\mathfrak{A}, \mathfrak{B})$ for every $k \in \mathbb{N}$. Let $B_1 = \{1 - \frac{1}{n} \mid n > 0\}$ be the copy of $\mathbb{N}$ in $\mathfrak{B}$, and let $B_2 = \{1 + \frac{1}{n} \mid n > 0\} \cup \{3 - \frac{1}{n} \mid n > 0\}$ be the copy of $\mathbb{Z}$ in $\mathfrak{B}$. For two points a, b, let $d(a, b) \in \mathbb{N} \cup \{\infty\}$ be the number of steps necessary to reach b from a. Player II plays as to guarantee the following invariant: If at round m

the selected elements are $a_1, \dots, a_m \in \mathbb{N}$ and $b_1, \dots, b_m \in B = B_1 \cup B_2$, then, for every $i, j \in \{1, \dots, m\}$,

$$\begin{aligned} &(1)\ d(a_i, a_j) \approx_{2^{n-m+1}} d(b_i, b_j), \text{ and} \\ &(2)\ a_i \le a_j \text{ iff } b_i \le b_j, \end{aligned}$$

where $\approx_{2^{n-m+1}}$ is the threshold equivalence relation as defined in Problem 2.12.5. We assume w.l.o.g. that Player I initially plays $a_1 = 0$, to which Player II responds with $b_1 = 0$. At round $m+1$, assume Player I plays $a_{m+1} \in \mathbb{N}$. There are two cases to consider. If a_{m+1} is a new maximal element, then let a_i be the largest element s.t. $a_i < a_{m+1}$, and by the invariant b_i is the largest element played so far in B. Player II replies with the unique $b_{m+1} \in B$ s.t. $d(b_i, b_{m+1}) = d(a_i, a_{m+1})$ and $b_i < b_{m+1}$, thus establishing the invariant. Otherwise, let $a_i < a_{m+1} < a_j$ with a_i maximal and a_j minimal with this property. By the invariant, there is no b_k s.t. $b_i < b_k < b_j$, and Player II replies with some b_{m+1} s.t. $b_i < b_{m+1} < b_j$, to be established as follows. There are two cases to consider.

1. If $d(a_i, a_j) < 2^{n-m+1}$, then by the invariant $d(a_i, a_j) = d(b_i, b_j)$ (in particular b_i, b_j are either both in B_1 or in B_2), and Player II replies with the unique b_{m+1} s.t. $d(b_i, b_{m+1}) = d(a_i, a_{m+1})$ (and thus $d(b_{m+1}, b_j) = d(a_{m+1}, a_j)$), which clearly preserves the invariant.

2. If $d(a_i, a_j) \ge 2^{n-m+1}$, then $d(b_i, b_j) \ge 2^{n-m+1}$ as well (including the case where $d(b_i, b_j) = \infty$). There are three sub-cases to consider.

   (a) If $d(a_i, a_{m+1}) < 2^{n-(m+1)+1}$, then Player II is obliged to choose the unique b_{m+1} s.t. $d(b_i, b_{m+1}) = d(a_i, a_{m+1})$.

   (b) The case $d(a_{m+1}, a_j) < 2^{n-(m+1)+1}$ is similar.

   (c) Finally, if $d(a_i, a_{m+1}), d(a_{m+1}, a_j) \ge 2^{n-(m+1)+1}$, then Player II replies with any b_{m+1} s.t. $d(b_i, b_{m+1}), d(b_{m+1}, b_j) \ge 2^{n-(m+1)+1}$, which is chosen in B_1 if $a_i, a_j \in B_1$ and in B_2 otherwise.

The argument if Player I plays $b_{m+1} \in B$ is similar. □

Statement of Problem 2.12.7. Assume that Player II has a winning strategy in $G_4(\mathfrak{A}, \mathfrak{B})$, where $\mathfrak{A}$ is shown in the problem figure and $\mathfrak{B}$ is an unspecified undirected graph with n vertices. How many edges can $\mathfrak{B}$ have? □

Solution of Problem 2.12.7. If player II wins $G_4(\mathfrak{A}, \mathfrak{B})$, then $\mathfrak{A} \equiv_4 \mathfrak{B}$ by Theorem 2.12.2 "Finite EF-games". The following are sentences of quantifier rank ≤ 4, which are true in $\mathfrak{A}$ and thus must be true in $\mathfrak{B}$.

1. There are precisely three distinct vertices s.t. every other vertex is incident to one of them:

$$\exists x_1 \exists x_2 \exists x_3 \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge$$
$$\forall y \,.\, E(x_1, y) \vee E(x_2, y) \vee E(x_3, y) \vee x_1 = y \vee x_2 = y \vee x_3 = y,$$

2. There are no two such vertices:

$$\neg \exists x_1 \exists x_2 \,.\, \bigwedge_{i \neq j} x_i \neq x_j \ \wedge \forall y \,.\, E(x_1, y) \vee E(x_2, y) \vee x_1 = y \vee x_2 = y$$

   Thus, $\mathfrak{B}$ consists of three "central" vertices s.t. all other vertices are connected to them.

3. We forbid triangles and paths of length three:

$$\neg \exists x_1 \exists x_2 \exists x_3 \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge E(x_1, x_2) \wedge E(x_2, x_3) \wedge E(x_3, x_1), \text{ and}$$
$$\neg \exists x_1 \exists x_2 \exists x_3 \exists x_4 \,.\, \bigwedge_{i \neq j} x_i \neq x_j \wedge E(x_1, x_2) \wedge E(x_2, x_3) \wedge E(x_3, x_4).$$

Thus, $\mathfrak{B}$ is the disjoint union of three stars with a total of n vertices, and thus it has $n - 3$ edges. ☐

Statement of Problem 2.12.8. Consider the graph $\mathfrak{G}$ in the problem figure. Prove that any graph $\mathfrak{H}$ s.t. $\mathfrak{H} \equiv_3 \mathfrak{G}$ has an odd number of ≥ 3 vertices. ☐

Solution of Problem 2.12.8. Note that $G_3(\mathfrak{G}, \mathfrak{H})$ is equivalent to the same game played on the complement graphs $G_3(\overline{\mathfrak{G}}, \overline{\mathfrak{H}})$, since partial isomorphisms are the same in both cases. The complement of $\mathfrak{G}$ consists of two edges and an isolated vertex. Any graph $\mathfrak{H}$ satisfying $\mathfrak{H} \equiv_3 \mathfrak{G}$ consists of an isolated vertex and at least two isolated edges. From this observation the thesis follows. ☐

Statement of Problem 2.12.9. For a partial order $\mathfrak{A} = (A, \leq)$, let $\widetilde{\mathfrak{A}} = (\widetilde{A}, \widetilde{\leq})$ be obtained from $\mathfrak{A}$ by adding a new largest and smallest element $\widetilde{A} = A \cup \{\bot, \top\}$.

1. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two partial orders. Prove that

$$\mathfrak{A} \equiv_n \mathfrak{B} \quad \text{implies} \quad \widetilde{\mathfrak{A}} \equiv_n \widetilde{\mathfrak{B}}.$$

2. What about the converse implication? □

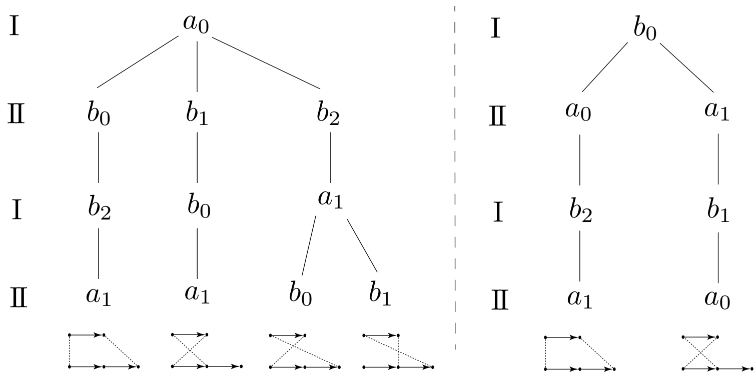
Solution of Problem 2.12.9. Regarding the first point, assume Player II wins $G_n(\mathfrak{A}, \mathfrak{B})$. The winning strategy for Player II in $G_n(\widetilde{\mathfrak{A}}, \widetilde{\mathfrak{B}})$ consists in mimicking her moves in the $G_n(\mathfrak{A}, \mathfrak{B})$ whenever Player I plays elements different from $\bot_{\mathfrak{A}}, \top_{\mathfrak{A}}, \bot_{\mathfrak{B}}, \top_{\mathfrak{B}}$. If Player I plays any of the new elements, then Player II plays the corresponding element in the other structure.

The converse implication does not hold. Consider finite total orders $\mathfrak{A}, \mathfrak{B}$ of different lengths $> 2^n$. As in Problem 2.12.5, one can show that $\mathfrak{A} \equiv_n \mathfrak{B}$. "Removing" a tilde means reducing the length by two and thus we would eventually produce two distinct short orders $\mathfrak{A}', \mathfrak{B}'$ s.t. $\mathfrak{A} \not\equiv_n \mathfrak{B}$, which is a contradiction. □

2.12.2 Distinguishing sentences

Statement of Problem 2.12.10 "Distinguishing chains". Let the signature consist of a single binary relation $\Sigma = \{E\}$, and let $\mathfrak{A}$ and $\mathfrak{B}$ be two directed paths of length 1, resp., 2 (c.f. problem figure). Show that Player I wins $G_k(\mathfrak{A}_1, \mathfrak{B}_1)$ with $k = 2$ and construct the distinguishing formula corresponding to her winning strategy. □

Solution of Problem 2.12.10 "Distinguishing chains". A winning strategy tree for Player I is shown on the left in the solution figure. Player I is always able to ensure an edge $E(a_0, a_1)$ in the first structure and never a matching edge $E(h(a_0), h(a_1))$ in the second structure; thus in each leaf the distinguishing quantifier-free formula is $E(a_0, a_1)$. Moves of Player I in the first structure correspond to existential quantifiers, while when she moves in the second structure it corresponds to universal quantifiers. The



Two solutions for Problem 2.12.10 "Distinguishing chains".

distinguishing formula directly corresponding to Player's I winning strategy is

$$\begin{aligned}\exists x_0 \,.\, (&\forall x_1 \,.\, x_0 \neq x_1 \to E(x_0, x_1) \wedge \\ &(\forall x_1 \,.\, x_0 \neq x_1 \to E(x_0, x_1) \wedge \\ &(\exists x_1 \,.\, x_0 \neq x_1 \wedge E(x_0, x_1) \wedge E(x_0, x_1)),\end{aligned}$$

which is logically equivalent to $\exists x_0 \,.\, \forall x_1 \,.\, x_0 \neq x_1 \to E(x_0, x_1)$, also a distinguishing formula of rank 2.

This needs not be the only winning strategy for Player I, and different strategies yield different distinguishing formulas. For example, consider the strategy tree on the right in the solution figure. The corresponding distinguishing formula (of rank 2) is $\forall x_0 \,.\, (\forall x_1 \,.\, x_0 \neq x_1 \to E(x_0, x_1)) \vee (\forall x_1 \,.\, x_0 \neq x_1 \to E(x_1, x_0))$. □

Statement of Problem 2.12.11 "The hypercube". Let $\mathfrak{H}_n = (\{0,1\}^n, E)$ be the hypercube graph, i.e., $E(x, y)$ holds iff $x, y \in \{0,1\}^n$ differ on exactly one position. Find two sentences of smallest quantifier rank distinguishing:

- $\mathfrak{H}_4$ and $\mathfrak{H}_3$;
- $\mathfrak{H}_3$ and $\mathfrak{H}_3^-$, where the latter graph is obtained by removing one edge from $\mathfrak{H}_3$. □

Solution of Problem 2.12.11 "The hypercube". Regarding the first point, we are looking for the least k s.t. Player I has a winning strategy in $G_k(\mathfrak{H}_4, \mathfrak{H}_3)$, and a sentence of rank k describing her strategy. We present a Player I's winning strategy for $k = 3$. In the first two rounds she marks vertices $(0,0,0)$ and $(1,1,1)$ of $\mathfrak{H}_3$. No matter how Player II responds, there is always a vertex in $\mathfrak{H}_4$ which is neither selected nor incident to any previously selected vertex, and this what Player I selects next. (Indeed, the degree of vertices in $\mathfrak{H}_4$ is 4, hence there are 2 selected vertices and no more than 8 additional vertices incident to them, a total of 10, while there are 16 vertices in the whole graph.) Every Player II's answer is now losing, since every vertex of $\mathfrak{H}_3$ either has been already selected or is incident to a selected one. The following sentence, extracted from the argument above, is true in $\mathfrak{H}_4$ and false in $\mathfrak{H}_3$:

$$\forall x \forall y \exists z \,.\, z \neq x \wedge z \neq y \wedge \neg E(x,z) \wedge \neg E(y,z).$$

The value $k = 3$ is optimal, since Player II has an obvious winning strategy for in game with $k = 2$ rounds.

Regarding the second point, Player I has the following winning strategy in $G_3(\mathfrak{H}_3, \mathfrak{H}_3^-)$:

1. Select a vertex x degree 2 in $\mathfrak{H}_3^-$. By symmetry, we can w.l.o.g. assume that Player II answers with $h^{-1}(x) = (0,0,0)$ in $\mathfrak{H}_3$.
2. Select vertex $y = (1,1,1)$ in $\mathfrak{H}_3$, and let $h(y)$ be Player II's response in $\mathfrak{H}_3^-$.
3. In $\mathfrak{H}_-^3$, the first selected vertex x has degree 2 and the second one $h(y)$ has degree at most 3. Those two selected vertices and all those incident to them make a total of at most 7 vertices, while there are 8 vertices in the graph. Player I now chooses the remaining vertex z in $\mathfrak{H}_3^-$. Player II has no winning answer, because in $\mathfrak{H}_3$ all vertices are either selected or incident to one of the selected vertices.

This strategy of Player II translates into the sentence

$$\forall x \exists y \forall z \,.\, z \neq x \wedge z \neq y \rightarrow E(z,x) \vee E(z,y),$$

which is true in $\mathfrak{H}^3$ and false in $\mathfrak{H}_-^3$.

There is another solution:

1. In the first two moves, Player I selects both vertices of degree 2 in $\mathfrak{H}^3_-$. Her final winning move depends on the answers of Player II in $\mathfrak{H}^3$.
   (a) If the vertices chosen by Player II are equal or connected by an edge, he loses immediately, even before the third round.
   (b) If the vertices chosen by Player II are on two ends of a diagonal of a common face (e.g. $(0,0,0)$ and $(0,1,1)$), then Player II wins by choosing $(0,1,0)$ in $\mathfrak{H}_3$, which is connected by an edge to both selected vertices, while there is no such vertex in $\mathfrak{H}_3^-$.
   (c) If the vertices chosen by Player II are on two ends of a diagonal of the cube (e.g. $(0,0,0)$ and $(1,1,1)$), then Player II wins by choosing a vertex in $\mathfrak{H}_3^-$ which is not connected to any already selected one. Player II has no answer, because every vertex in $\mathfrak{H}_3$ which in neither $(0,0,0)$ nor $(1,1,1)$, is incident to one of them.

This strategy translates into the distinguishing sentence

$$\begin{aligned}\forall x \forall y \,.\, & x = y \vee E(x,y) \vee \\ & \exists z \,.\, E(x,z) \wedge E(y,z) \vee \\ & \forall z \,.\, x = z \vee y = z \vee E(x,z) \vee E(y,z).\end{aligned}$$ □

2.12.3 Infinite EF-games

Let the infinite EF-game $G_\infty(\mathfrak{A}, \mathfrak{B})$ be played for a countable number of rounds. The following problem shows that countable EF-games capture isomorphism of countable structures.

Statement of Problem 2.12.12 "Countable EF-games". Fix a signature Σ and two *countable* structures $\mathfrak{A}$ and $\mathfrak{B}$ over Σ.

$$\text{Player II wins } G_\infty(\mathfrak{A}, \mathfrak{B}) \quad \text{if, and only if,} \quad \mathfrak{A} \cong \mathfrak{B}.$$ □

Solution of Problem 2.12.12 "Countable EF-games". For the "if" direction, assume $\mathfrak{A} \cong_h \mathfrak{B}$. Player II's winning strategy consists in using h in order to reply to Player I: If at round i Player I selects $a_i \in \mathfrak{A}$, then Player II replies with $b_i = h(a_i) \in \mathfrak{B}$, and if Player I selects $b_i \in \mathfrak{B}$, then Player II replies with $a_i = h^{-1}(b_i)$. It is easy to see that this strategy is winning.

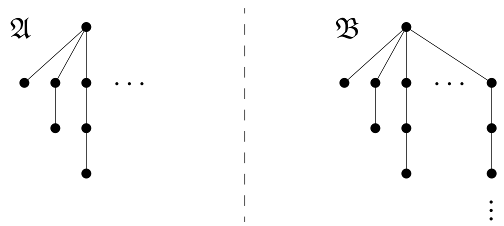


Figure for Problem 2.12.13.

For the "only if" direction, assume that Player II has a winning strategy in $G_\infty(\mathfrak{A}, \mathfrak{B})$. We let Player I select an element of $\mathfrak{A}$ at even rounds and one of $\mathfrak{B}$ at odd rounds, in such a way that in the limit the whole domains $X = A$ and $Y = B$ are selected. □

Statement of Problem 2.12.13. Construct two structures $\mathfrak{A}$ and $\mathfrak{B}$ s.t. Player II wins $G_m(\mathfrak{A}, \mathfrak{B})$ for every finite number of rounds $m \in \mathbb{N}$ but loses the infinite game $G_\infty(\mathfrak{A}, \mathfrak{B})$. □

Solution of Problem 2.12.13. Consider the two infinite trees $\mathfrak{A}$ and $\mathfrak{B}$ in the figure, where the latter is obtained from the former by adding an infinite branch. For every finite $n \in \mathbb{N}$, Player II wins $G_n(\mathfrak{A}, \mathfrak{B})$ by mapping the infinite branch of $\mathfrak{B}$ into any fixed branch branch of length $\geq 2^n$ of $\mathfrak{A}$. However, Player II loses with $n = \infty$, since Player I can play on the infinite branch of $\mathfrak{B}$, which has no counterpart in $\mathfrak{A}$ (and indeed, $\mathfrak{A}$ and $\mathfrak{B}$ are not isomorphic). □

2.12.4 No equality

Statement of Problem 2.12.14. Find two structures $\mathfrak{A}, \mathfrak{B}$ which can be distinguished by a sentence using equality, but cannot be distinguished by any sentence not using equality. □

Solution of Problem 2.12.14. It suffices to consider the empty vocabulary $\Sigma = \varnothing$ and two structures $\mathfrak{A}$ consisting of just one element, and $\mathfrak{B}$ consisting of two elements. Then the sentence $\exists x \,.\, \forall y \,.\, y = x$ is satisfied in $\mathfrak{A}$ but not in $\mathfrak{B}$. If equality is not available, then no formula can be written at all over the empty signature. $\square$

Statement of Problem 2.12.18. Let $\mathfrak{A}, \mathfrak{B}$ be two relational structures over a common signature Σ. Propose a modification $\mathfrak{A}'$ of $\mathfrak{A}$ and $\mathfrak{B}'$ of $\mathfrak{B}$ s.t. Player I wins $H_k(\mathfrak{A}, \mathfrak{B})$ if, and only if, she wins $G_k(\mathfrak{A}', \mathfrak{B}')$. $\square$

Solution of Problem 2.12.18. Let $\mathfrak{A}'$ be obtained from $\mathfrak{A}$ by replacing every element $a \in A$ by k identical copies thereof $a_1, \dots, a_k$, and similarly for $\mathfrak{B}'$. Relations are updated in such a way as to make the new elements behave like the original ones. For instance, for binary relations we have $(a, a') \in R^{\mathfrak{A}}$ iff $(a_i, a'_j) \in R^{\mathfrak{A}'}$ for every $i, j \in \{1, \dots, k\}$. It remains to check that Player II wins $H_k(\mathfrak{A}, \mathfrak{B})$ iff she wins $G_k(\mathfrak{A}', \mathfrak{B}')$.

For the "only if" direction, assume she has a winning strategy against Player I in $G_k(\mathfrak{A}', \mathfrak{B}')$. In order to show that Player II wins in $H_k(\mathfrak{A}, \mathfrak{B})$, we play the two games in parallel, as follows: If at round i Player I picks element $a_i \in A$ for the j-th time in $H_k(\mathfrak{A}, \mathfrak{B})$, then she picks the corresponding j-th copy $a_{i,j} \in A'$ in $G_k(\mathfrak{A}', \mathfrak{B}')$, and when Player II subsequently replies with $b_{i,j'} \in B'$ in $G_k(\mathfrak{A}', \mathfrak{B}')$, then Player II copies this move in $H_k(\mathfrak{A}, \mathfrak{B})$ by choosing $b_i \in B$. The construction when Player I picks an element in B is analogous. Assume $a_1, \dots, a_k \in A$ and $b_1, \dots, b_k \in B$ are the two sequences constructed at the end of the game $H_k(\mathfrak{A}, \mathfrak{B})$, and let $X = \{a_{1,j_1}, \dots, a_{k,j_k}\} \subseteq A'$ and $Y = \{b_{1,h_1}, \dots, b_{k,h_k}\} \subseteq B'$ be the corresponding sets in $G_k(\mathfrak{A}', \mathfrak{B}')$. Since Player II is playing according to a winning strategy in $G_k(\mathfrak{A}', \mathfrak{B}')$, $\mathfrak{A}'|_X \cong h\, \mathfrak{B}'|_Y$. It's immediate to check that $\sim = \{(a_1, b_1), \dots, (a_k, b_k)\} \subseteq A \times B$ is a $\mathfrak{A}, \mathfrak{B}$-invariant, and thus Player II wins $H_k(\mathfrak{A}, \mathfrak{B})$, as required.

The construction for the "if" direction is symmetric: When Player I picks $a_{i,j} \in A'$, then she picks $a_i \in A$, and then Player II replies by selecting element $b_i \in B$ for the j-th time, then she replies with the j-th copy $b_{i,j} \in B'$. Since Player II plays a winning strategy in $H_k(\mathfrak{A}, \mathfrak{B})$, $\sim = \{(a_1, b_1), \dots, (a_k, b_k)\} \subseteq A \times B$ is an $\mathfrak{A}, \mathfrak{B}$-invariant. It follows that $\mathfrak{A}'|_X \cong_h \mathfrak{B}'|_Y$ for the isomorphism $h(a_{i,j_i}) = b_{i,h_i}$ for every $1 \leq i \leq k$. $\square$

2.12.5 One-sided EF-games

Statement of Problem 2.12.20. Show that Player I wins the standard game $G_4(\mathfrak{A}, \mathfrak{B})$, with $\mathfrak{A}, \mathfrak{B}$ as in the problem figure. Is there a winning strategy for Player I in the one-sided variant $G_4^{\mathsf{one}}(\mathfrak{A},\mathfrak{B})$? $\square$

Solution of Problem 2.12.20. In the first three moves Player I chooses the centres of the stars in $\mathfrak{B}$, and in the fourth move she chooses any element of $\mathfrak{A}$ in a star where Player II has not chosen any element so far.

Player I cannot win without switching sides. If Player I always plays in $\mathfrak{B}$, then Player II has a trivial copy-cat counter-strategy. If Player I always plays in $\mathfrak{A}$, then Player II copies her moves until the first time Player I has selected three different stars. At this point, Player II selects a node not at the centre of the remaining unselected star in $\mathfrak{B}$. Now, whatever Player I does in her last move, Player II can mimic it successfully. $\square$

Statement of Problem 2.12.21. Give an example of two structures $\mathfrak{A}_0, \mathfrak{A}_1$ s.t. Player II wins $G_k^{\mathsf{one}}(\mathfrak{A}_0,\mathfrak{A}_1)$ for every $k \in \mathbb{N}$, even though she loses the standard game $G_m(\mathfrak{A}_0,\mathfrak{A}_1)$ for some m. What is the smallest such m? $\square$

Solution of Problem 2.12.21. The optimal value is $m = 2$. Let $\mathfrak{A}_1 = (\mathbb{Z}, \leq)$ and $\mathfrak{A}_2 = (\mathbb{N}, \leq)$. In the standard game, Player I wins in two rounds: She first marks 0 in $\mathbb{N}$, and in the second round she marks in $\mathbb{Z}$ the predecessor of the element specified by Player II in the first round.

Consider now the one-sided game with k rounds. If in the first round Player I plays in $\mathbb{N}$, then Player II has an obvious strategy to mimic in $\mathbb{Z}$ the consecutive choices of Player I (indeed $\mathbb{N}$ can be embedded in $\mathbb{Z}$).

If Player I initially plays a_1 in $\mathbb{Z}$, then Player II answers in $\mathbb{N}$ with an element sufficiently far from the origin; distance $\geq 2^k$ suffices. The subsequent moves of Player I to the left of a_1 are answered by Player II as in Problem 2.12.5, and moves to the right of a_1 are mimicked precisely by Player II in $\mathbb{N}$. $\square$

2.12.6 Inexpressibility: Non-definability and non-axiomatisability

Statement of Problem 2.12.22 "Non-definability via EF-games". Show that, in order to prove that a class of structures $\mathcal{A}$ cannot be defined by a single sentence, it suffices to construct two sequences of structures $\mathfrak{A}_1, \mathfrak{A}_2, \dots \in \mathcal{A}$ and $\mathfrak{B}_1, \mathfrak{B}_2, \dots \notin \mathcal{A}$ s.t., for every $m \in \mathbb{N}$, $\mathfrak{A}_m \equiv_m \mathfrak{B}_m$. $\square$

Solution of Problem 2.12.22 "Non-definability via EF-games". By way of contradiction, let φ be a sentence s.t. $\mathcal{A} = \mathsf{Mod}(\varphi)$. If $m = \mathsf{rank}(\varphi)$ is the rank of φ, by assumption $\mathfrak{A}_m \vDash \varphi$ and thus $\mathfrak{B}_m \vDash \varphi$, implies $\mathfrak{B}_m \in \mathcal{A}$, which is a contradiction. □

Statement of Problem 2.12.23 "Eulerian cycles are not definable". An *Eulerian cycle* in a simple graph is a cycle visiting every edge exactly once. Prove that the existence of an Eulerian cycle in *finite* simple graphs is not definable by a sentence of first-order logic. *Hint: Use Problem 2.12.22 "Non-definability via EF-games".* □

Solution of Problem 2.12.23 "Eulerian cycles are not definable". A simple graph has an Euler cycle if, and only if, every vertex is of even degree. Therefore a clique K_n has an Eulerian cycle iff n is odd. An application of EF-games shows that sentences of quantifier rank $\leq n$ cannot distinguish K_n and K_{n+1}. □

Statement of Problem 2.12.24 "Hanf". Consider the cylinder $\mathfrak{C}_n$ and the Möbius $\mathfrak{M}_n$ graph shown in the problem figure, both with $2 \cdot n$ vertices. Is there a single first-order sentence φ distinguishing $\mathfrak{C}_n$ from $\mathfrak{M}_n$ for every $n \in \mathbb{N}$? □

Solution of Problem 2.12.24 "Hanf". There is no such formula. The intuition is that $\mathfrak{C}_n$ and $\mathfrak{D}_n$ locally look the same. Formally, $\mathfrak{C}_{2^n} \equiv_n \mathfrak{D}_{2^n}$ for every $n \in \mathbb{N}$. For two vertices u, v, let the *distance* $d(u, v)$ be the length of the shortest path connecting them. Player II plays as to preserve the following invariant: If at round m the two players have selected vertices $A_m = \{a_1, \ldots, a_m\} \subseteq C_{2^n}$ and $B_m = \{b_1, \ldots, b_m\} \subseteq D_{2^n}$ (corresponding to the partial isomorphism $h(a_1) = b_1, \ldots, h(a_m) = b_m$), then for every index $i \in \{1, \ldots, m\}$, letting $A = \{a_j \mid d(a_i, a_j) < 2^{n-m}\}$ and $B = \{b_j \mid d(b_i, b_j) < 2^{n-m}\}$ be the corresponding neighbourhoods, h extends to a partial isomorphism $\mathfrak{C}_n|_A \cong_h \mathfrak{M}_n|_B$. □

Statement of Problem 2.12.25 "Non-axiomatisability via EF-games". Show that, in order to prove non-axiomatisability by a set of sentences, it suffices to construct a sequence of structures $\mathfrak{A}_1, \mathfrak{A}_2, \dots \in \mathcal{A}$ and a single structure $\mathfrak{B} \notin \mathcal{A}$ s.t., for every $m \in \mathbb{N}$, $\mathfrak{A}_m \equiv_m \mathfrak{B}$. □

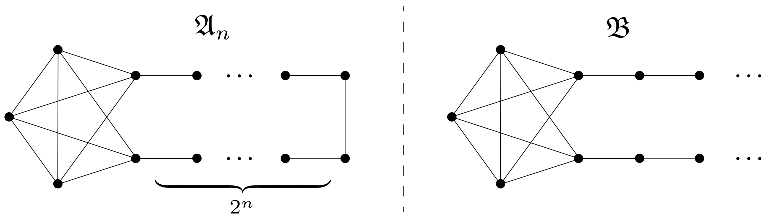


Figure for Problem 2.12.26 "Planarity is not axiomatisable".

Solution of Problem 2.12.25 "Non-axiomatisability via EF-games". By way of contradiction, assume that a class of structures $\mathcal{A}$ is axiomatisable by a set of sentences Γ. Consider an arbitrary sentence $\varphi \in \Gamma$. If $m = \mathsf{rank}(\varphi)$ is the rank of φ, then by assumption $\mathfrak{A}_m \models \varphi$ and thus $\mathfrak{B} \models \varphi$. Since φ was chosen arbitrarily, $\mathfrak{B} \models \Gamma$, i.e., $\mathfrak{B} \in \mathcal{A}$, which is a contradiction. □

Statement of Problem 2.12.26 "Planarity is not axiomatisable". A simple graph is *planar* if it can be drawn on the plane without crossing edges. Prove that the class of graphs in which each finite subgraph is planar is not axiomatisable. *Hint: Use Problem 2.12.25 "Non-axiomatisability via EF-games".* □

Solution of Problem 2.12.26 "Planarity is not axiomatisable". Let $n \in \mathbb{N}$. Consider the graphs in the figure $\mathfrak{A}_n$ (left) and $\mathfrak{B}$ (right). The graph $\mathfrak{A}_n$ contains the complete graph of five vertices K_5 as a minor, and thus by Wagner's theorem it is not planar. The graph $\mathfrak{B}$ is planar, and thus all of its finite subgraphs are planar as well. By playing the EF-game $G_n(\mathfrak{A}_n, \mathfrak{B})$, one can show that $\mathfrak{A}_n \equiv_n \mathfrak{B}$ (Problem 2.12.5). By □

Statement of Problem 2.12.27 "The Church-Rosser property is not axiomatisable (via EF- We showed in Problem 2.9.14 "The Church-Rosser property is not axiomatisable (via compactness)" using compactness that the Church-Rosser property CR is not axiomatisable. Prove the same using EF games. □

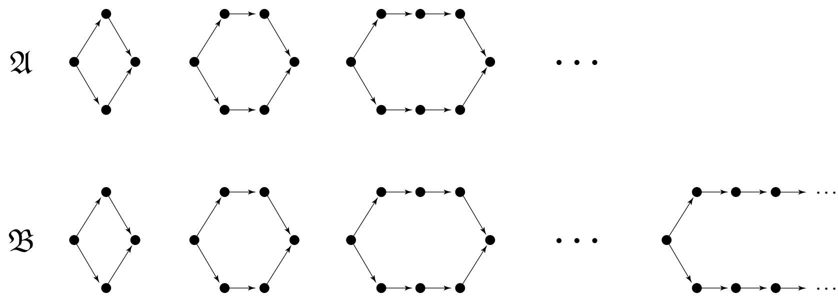


Figure for Problem 2.12.27 "The Church-Rosser property is not axiomatisable (via EF-games)".

Solution of Problem 2.12.27 "The Church-Rosser property is not axiomatisable (via EF-ga
Consider the two structures $\mathfrak{A}$ and $\mathfrak{B}$ from the figure. Structure $\mathfrak{A}$ has the Church-Rosser property, while $\mathfrak{B}$ does not. Player II has a winning strategy in $G_k(\mathfrak{A}, \mathfrak{B})$ for any number of moves k. Player I's moves in the infinite component of $\mathfrak{B}$ are simulated in a sufficiently large component of $\mathfrak{A}$. □

2.12.7 Complexity

Statement of Problem 2.12.28 "Solving EF-games in PSPACE". Show that the following problem can be solved in PSPACE.

THE EF-GAME PROBLEM.
Input: Two structures $\mathfrak{A}$ and $\mathfrak{B}$ over a common vocabulary Σ and $k \in \mathbb{N}$.
Output: YES iff Player II wins $G_k(\mathfrak{A}, \mathfrak{B})$. □

Solution of Problem 2.12.28 "Solving EF-games in PSPACE". Let $\mathfrak{A}, \mathfrak{B}$ have size n. We can assume w.l.o.g. that $k \le n$, because we cannot play an EF-game for more rounds than the number of elements in the two structures. Consider the following alternating polynomial time algorithm: Each position of the game is a pair of elements (a_i, b_i), where $a_i \in A$ and $b_i \in B$. At the end of the game we must check whether $\mathfrak{A}|_{\{a_1,\dots,a_k\}} \cong_h \mathfrak{B}|_{\{b_1,\dots,b_k\}}$ for the partial isomorphism $h(a_1) = b_1, \dots, h(a_k) = b_k$, which can be done in PTIME. The result follows since APTIME = PSPACE [6]. □

Statement of Problem 2.12.29 "Fixed-length EF-games". Fix a number of rounds $k \in \mathbb{N}$. Show that the following problem can be solved in LOGSPACE:

FIXED-LENGTH EF-GAME.
Input: Two structures $\mathfrak{A}$ and $\mathfrak{B}$ over a common vocabulary Σ.
Output: YES iff Player II wins $G_k(\mathfrak{A}, \mathfrak{B})$. □

Solution of Problem 2.12.29 "Fixed-length EF-games". Let $\mathfrak{A}$ and $\mathfrak{B}$ have size n. Traverse the game tree using a min-max algorithm. Each node can be represented by $O(\log n)$ bits using a binary encoding of the elements in A and B. The tree has constant depth $2 \cdot k$, since there are k rounds with two moves in each and k is fixed, and thus the memory sufficient to store an entire branch is also $O(\log n)$. In a leaf, checking for the winner amounts to testing whether vertex pairs in the branch leading to this leaf define a partial isomorphism. The latter can be done with an additional $O(\log n)$ space, by checking for every tuple in $R^{\mathfrak{A}}$ whether the corresponding tuple is in $R^{\mathfrak{B}}$, and vice-versa. We thus obtain a LOGSPACE algorithm. □

2.12.8 Complete theories

Statement of Problem 2.12.32 "Łoś-Vaught test". Let κ be an infinite cardinality. Show that every set of sentences Γ over a signature Σ of cardinality $|\Sigma| \leq \kappa$, which has no finite models and is κ-categorical, must be complete. □

Solution of Problem 2.12.32 "Łoś-Vaught test". If Γ is not consistent (i.e., it has no model), then it is trivially complete. Thus, assume that Γ is consistent. By way of contradiction, assume that Γ is not complete, and thus there is a sentence φ such that $\Gamma \nvDash \varphi$ and $\Gamma \nvDash \neg\varphi$. Consequently, $\Gamma_0 = \Gamma \cup \{\neg\varphi\}$ and $\Gamma_1 = \Gamma \cup \{\varphi\}$ are both consistent and have infinite models, because Γ has no finite models itself. By Theorem 2.10.1 "Upward Skolem-Löwenheim theorem", there are two models $\mathfrak{A}_0 \vDash \Gamma_0$ and $\mathfrak{A}_1 \vDash \Gamma_1$ of cardinality κ, and in particular $\mathfrak{A}_0, \mathfrak{A}_1$ are also models of Γ. Since $\mathfrak{A}_0 \vDash \neg\varphi$ and $\mathfrak{A}_1 \vDash \varphi$, by Problem 2.11.6 "Isomorphism theorem" $\mathfrak{A}_0, \mathfrak{A}_1$ are not isomorphic, contradicting κ-categoriciy of Γ. □

Statement of Problem 2.12.33 "Theory completeness and decidability". A theory Γ is *recursive* if it is decidable whether $\varphi \in \Gamma$ (membership), and *de-*

cidable if it is decidable whether $\Gamma \vDash \varphi$ (logical consequence). Show that a complete recursive theory over a finite signature Σ is decidable. □

Solution of Problem 2.12.33 "Theory completeness and decidability". Let φ be an input sentence. Since Γ is complete, $\Gamma \vDash \varphi$ (logical consequence) if, and only if, $\varphi \in \Gamma$ (membership). The latter problem is decidable by assumption. □

Statement of Problem 2.12.34. How many complete theories over a finite signature can exist? Find a finite signature Σ s.t. there are continuum-many complete theories over Σ. □

Solution of Problem 2.12.34. Since there are countably many sentences over any finite signature, there can be at most continuum-many complete theories over a finite signature. In order to show that this maximum cardinality can be attained, consider the finite signature $\Sigma = \{0, s, U\}$, where "0" is a constant, "s" is a unary function, and "U" is a unary (i.e., monadic) relation. Let us consider structures of the form $(\mathbb{N}, 0^{\mathbb{N}}, s^{\mathbb{N}}, U^{\mathbb{N}})$, where $0^{\mathbb{N}}$ is the constant 0, "$s^{\mathbb{N}}$" is the successor function over the natural numbers, and $U^{\mathbb{N}} \subseteq \mathbb{N}$ is a unary relation. There is a structure of this form for any choice of $U^{\mathbb{N}}$, and thus continuum-many. Every two such structures $(\mathbb{N}, 0^{\mathbb{N}}, +1^{\mathbb{N}}, U^{\mathbb{N}})$ and $(\mathbb{N}, 0^{\mathbb{N}}, +1^{\mathbb{N}}, V^{\mathbb{N}})$ with $U^{\mathbb{N}} \neq V^{\mathbb{N}}$ can be distinguished by a sentence $U(s^n(0))$ for some n s.t. $n \in U^{\mathbb{N}}$ and $n \notin V^{\mathbb{N}}$. Consequently, the respective (complete) theories are different: $\mathsf{Th}(\mathbb{N}, 0^{\mathbb{N}}, +1^{\mathbb{N}}, U^{\mathbb{N}}) \neq \mathsf{Th}(\mathbb{N}, 0^{\mathbb{N}}, +1^{\mathbb{N}}, V^{\mathbb{N}})$. We conclude that there are continuum-many complete theories over Σ. □

2.13 Interpolation

2.13.1 No equality

Statement of Problem 2.13.2 "Interpolation for quantifier-free ground formulas". Assume that $\vDash \varphi \to \psi$, where φ, ψ are quantifier-free, ground, and do not contain the equality symbol "=". Construct a quantifier-free ground formula ξ interpolating φ, ψ. □

Solution of Problem 2.13.2 "Interpolation for quantifier-free ground formulas". Let φ' be obtained from φ by replacing each subformula $\gamma \equiv R(t_1, \dots, t_k)$

thereof by a corresponding propositional variable p_γ, and similarly for ψ. Since there is no equality, each propositional variable behaves completely independently from other propositional variable. By Problem 1.7.2 "Propositional interpolation", there exists a propositional interpolant ξ'. We can thus reconstruct an interpolant ξ for φ, ψ by undoing the substitution above. Since ξ' contains only propositional variables p_γ's which are used both in φ' and ψ', ξ contains only relation and function symbols which are used in φ and ψ. □

Statement of Problem 2.13.3 "Preinterpolation for $\forall/\exists$ *sentences".* Assume

$$\vDash (\forall \bar{x} \,.\, \varphi) \to \exists \bar{y} \,.\, \psi,$$

with φ, ψ quantifier-free, not containing the equality symbol "=". Show how to construct a quantifier-free ground preinterpolant ξ for the two sentences above. *Hint: Use Problem 2.5.4 and Problem 2.13.2 "Interpolation for quantifier-free ground formulas".* □

Solution of Problem 2.13.3 "Preinterpolation for $\forall/\exists$ *sentences".* By assumption, $(\forall \bar{x} \,.\, \varphi) \to \exists \bar{y} \,.\, \psi$ is a tautology, and thus $(\forall \bar{x} \,.\, \varphi) \land \forall \bar{y} \,.\, \neg\psi$ is unsatisfiable. By Problem 2.5.4, there are tuples of ground terms $\bar{u}_1, \ldots, \bar{u}_m$ and $\bar{v}_1, \ldots, \bar{v}_n$ s.t. already the following quantifier-free ground formula is unsatisfiable:

$$\varphi[\bar{x} \mapsto \bar{u}_1] \land \cdots \land \varphi[\bar{x} \mapsto \bar{u}_m] \;\land\; \neg\psi[\bar{y} \mapsto \bar{v}_1] \land \cdots \land \neg\psi[\bar{y} \mapsto \bar{v}_n],$$

and thus the following quantifier-free ground formula is a tautology

$$\underbrace{\varphi[\bar{x} \mapsto \bar{u}_1] \land \cdots \land \varphi[\bar{x} \mapsto \bar{u}_m]}_{\varphi'} \to \underbrace{\psi[\bar{y} \mapsto \bar{v}_1] \lor \cdots \lor \psi[\bar{y} \mapsto \bar{v}_n]}_{\psi'}.$$

By Problem 2.13.2 "Interpolation for quantifier-free ground formulas", there exists a quantifier-free ground interpolant ξ s.t.

$$\vDash \varphi' \to \xi \quad \text{and} \quad \vDash \xi \to \psi'.$$

Since ξ contains only atomic formulas $R(\bar{t})$ which appear both in φ' and ψ', and the latter are obtained by replacing free variables in φ, resp., ψ, by ground terms, the symbol R necessarily appears in φ and ψ. By first-order reasoning, ξ is a preinterpolant for the original φ, ψ, since $\models \forall \bar{x} . \varphi \to \varphi[\bar{x} \mapsto \bar{u}_1] \wedge \cdots \wedge \varphi[\bar{x} \mapsto \bar{u}_m]$ and $\models \psi[\bar{y} \mapsto \bar{v}_1] \vee \cdots \vee \psi[\bar{y} \mapsto \bar{v}_n] \to \exists \bar{y} . \psi$.

Note that the application of Problem 2.5.4 above yields ground terms u_i's and v_j's over the *union* of the vocabularies of φ, ψ, and thus ξ could possibly use unshared function symbols. This issue will be solved in the next problem. $\square$

Statement of Problem 2.13.4 "Interpolation for $\forall/\exists$ sentences". Show how to transform a quantifier-free ground preinterpolant ξ,

$$\models \forall \bar{x} . \varphi \to \xi \quad \text{and} \quad \models \xi \to \exists \bar{y} . \psi,$$

into a ground interpolant (i.e., a sentence). $\square$

Solution of Problem 2.13.4 "Interpolation for $\forall/\exists$ sentences". We proceed by repeatedly applying the following transformation. Let $f(\bar{t})$ be a *maximal* ground subterm of ξ s.t. f is not a shared function symbol, and let z be a fresh variable. There are two cases to consider.

1. If f appears in φ but not in ψ, then

$$\models \forall \bar{x} . \varphi \to \xi' \text{ and } \models \xi' \to \exists \bar{y} . \psi, \text{ where } \xi' \equiv \exists z . \xi[f(\bar{t}) \mapsto z].$$

2. If f appears in ψ, but not in φ, then

$$\models \forall \bar{x} . \varphi \to \xi' \text{ and } \models \xi' \to \exists \bar{y} . \psi, \text{ where } \xi' \equiv \forall z . \xi[f(\bar{t}) \mapsto z].$$

Both cases are easily proved. Repeatedly applying the procedure above will preserve ξ being a preinterpolant and eventually remove all unshared function symbols. (Maximality is only needed in order to be able to iterate the procedure above. Correctness of a single step only requires that $f(\bar{t})$ is ground.) $\square$

Statement of Problem 2.13.5 "Interpolation for sentences". Let $\models \varphi \to \psi$, where φ, ψ are two sentences not containing the equality symbol. Show that there exists a sentence ξ interpolating φ, ψ. *Hint: Use Problem 2.4.3 "Herbrandisation" and Problem 2.13.4 "Interpolation for $\forall/\exists$ sentences".* $\square$

Solution of Problem 2.13.5 "Interpolation for sentences". Let's assume φ, ψ are in PNF (c.f. Problem 2.2.2 "Prenex normal form"). By assumption, $\varphi \to \psi$ is a tautology, and thus, by suitable renaming of quantified variables to avoid conflicts, we can have it in the form

$$\vDash Q_1 x_1 \cdots Q_m x_m \,.\, Q'_1 y_1 \cdots Q'_n y_n \,.\, \varphi' \to \psi',$$

where φ' is quantifier-free with free variables $\mathsf{fv}(\varphi') = \{x_1, \dots, x_m\}$, and similarly $\mathsf{fv}(\psi') = \{y_1, \dots, y_n\}$. By Problem 2.4.3 "Herbrandisation" we obtain a tautology

$$\vDash \exists x_{i_1}, \dots, x_{i_p} \,.\, \exists y_{j_1}, \dots, y_{j_q} \,.\, \varphi'' \to \psi'',$$

where $x_{i_1}, \dots, x_{i_p}$ are precisely the existentially quantified variables in $\{x_1, \dots, x_m\}$ and φ'' is the quantifier-free formula obtained from φ' by herbrandisation; similarly for $y_{j_1}, \dots, y_{j_q}$ and ψ''. The new formula φ'' contains fresh function symbols f_i's corresponding to the eliminated universal variables x_i's, and similarly for ψ''; we assume that all such function symbols are different. By a simple reshuffling of quantifiers, we obtain the tautology

$$\vDash (\forall x_{i_1}, \dots, x_{i_p} \,.\, \varphi'') \to \exists y_{j_1}, \dots, y_{j_q} \,.\, \psi'',$$

to which we can apply Problem 2.13.4 "Interpolation for $\forall/\exists$ sentences" and obtain a ground interpolant ξ (i.e., a sentence):

$$\vDash \exists x_{i_1}, \dots, x_{i_p} \,.\, \varphi'' \to \xi \quad \text{and} \quad \vDash \xi \to \exists y_{j_1}, \dots, y_{j_q} \,.\, \psi''.$$

By inverting the herbrandisation process (i.e., replacing newly introduced functions by universally quantified variables) and thanks to the fact that ξ has no free variables, we have

$$\vDash Q_1 x_1 \cdots Q_m x_m \,.\, \varphi' \to \xi \quad \text{and} \quad \vDash \xi \to Q'_1 y_1 \cdots Q'_n y_n \,.\, \psi',$$

thus showing that ξ is an interpolant for φ, ψ as required. □

Statement of Problem 2.13.6 "Interpolation for formulas without equality". Let $\vDash \varphi \to \psi$, where φ, ψ are two formulas (possibly containing free variables) not containing the equality symbol. Show that there exists a formula interpolating φ, ψ. *Hint: Use Problem 2.13.5 "Interpolation for sentences".* □

Solution of Problem 2.13.6 "Interpolation for formulas without equality". Replace every free variable x in φ, ψ by a fresh constant symbol c_x and let φ', ψ' be the corresponding sentences. Apply Problem 2.13.5 "Interpolation for sentences" to obtain an interpolant ξ and replace back every c_x by x. ☐

2.13.2 Extensions

Statement of Problem 2.13.7 "Interpolation with equality". Let $\models \varphi \to \psi$, where φ, ψ are two formulas possibly containing the equality relation. Show that there exists an interpolant thereof. *Hint: Use Problem 2.13.6 "Interpolation for formulas without equality".* ☐

Solution of Problem 2.13.7 "Interpolation with equality". It suffices to axiomatise equality w.r.t. the vocabulary of φ, ψ and then apply Problem 2.13.6 "Interpolation for formulas without equality". ☐

Statement of Problem 2.13.8. Let Γ be a set of formulas and ψ a formula of first-order logic and s.t. $\Gamma \models \psi$. Show that there exists a formula ξ over the common signature and common free variables of $\Gamma \cup \{\psi\}$ s.t. $\Gamma \models \xi$ and $\xi \models \psi$. *Hint: Apply Problem 2.9.1 "Compactess theorem" and Problem 2.13.7 "Interpolation with equality".* ☐

Solution of Problem 2.13.8. By the assumption, $\Gamma \cup \{\neg\psi\}$ is unsatisfiable, and by Problem 2.9.1 "Compactess theorem" there exists a finite set of formulas $\{\varphi_1, \dots, \varphi_n\} \subseteq \Gamma$ s.t. $\{\varphi_1, \dots, \varphi_n, \psi\}$ is already unsatisfiable. In other words, $\models \varphi_1 \wedge \cdots \wedge \varphi_n \to \psi$, and by Problem 2.13.7 "Interpolation with equality" there exists an interpolant ξ over the common signature and free variables s.t. $\models \varphi_1 \wedge \cdots \wedge \varphi_n \to \xi$ and $\models \xi \to \psi$. It follows at once that $\Gamma \models \xi$, $\xi \models \psi$, and ξ contains only symbols and free variables that are in common in $\Gamma \cup \{\psi\}$. ☐

Statement of Problem 2.13.9 "No interpolation for finite structures". Prove that the interpolation theorem fails for first-order logic over finite structures: Construct two sentences φ, ψ s.t.

- $\varphi \to \psi$ holds in all finite structures, and

- there is no ξ containing only relation and/or function symbols occurring in both φ and ψ s.t. $\varphi \to \xi$ and $\xi \to \psi$ holds in all finite structures.

Hint: Use Problem 2.8.18 "Spectra with only unary relations". □

Solution of Problem 2.13.9 "No interpolation for finite structures". It suffices to take any φ and ψ s.t. 1) φ is valid in any infinite models and ψ is invalid in some infinite model (thus $\varphi \not\models \psi$), 2) the finite models of φ, ψ are precisely those with even cardinality (thus $\varphi \to \psi$ over finite models), and 3) they have disjoint signature. Thanks to the conditions above, any interpolant ξ must have empty signature and express precisely the fact that its finite models have even cardinality. In particular, both $\mathsf{Spec}(\xi)$ and its complement $\mathbb{N}_{>}0 \setminus \mathsf{Spec}(\xi)$ are infinite. By Problem 2.8.18 "Spectra with only unary relations", we know that over the empty signature $\mathsf{Spec}(\xi)$ is either finite or cofinite. Consequently, no such interpolant ξ can exist. □

2.13.3 Applications of interpolation

Statement of Problem 2.13.10 "Separability of universal formulas". If two universal formulas φ, ψ over a relational signature without equality are jointly unsatisfiable $\models \varphi \wedge \psi \to \bot$, then they can be separated by a quantifier-free formula ξ: $\models \varphi \to \xi$ and $\models \xi \wedge \psi \to \bot$. □

Solution of Problem 2.13.10 "Separability of universal formulas". Let the two formulas be of the form $\varphi \equiv \forall \bar{x} \,.\, \varphi'$ and $\psi \equiv \forall \bar{y} \,.\, \psi'$, with φ', ψ' quantifier-free. We can assume that φ and ψ have the same free variables (otherwise, we can universally quantify the non-shared ones). Let's turn φ, ψ into sentences by interpreting the (common) free variables as zero-ary constant symbols. Since they are jointly unsatisfiable, $\models (\forall \bar{x} \,.\, \varphi') \to \exists \bar{y} \,.\, \neg\psi'$. By Problem 2.13.3 "Preinterpolation for $\forall/\exists$ sentences", they have a quantifier-free ground preinterpolant ξ. By interpreting back the introduced constants as free variables, we can see ξ as a quantifier-free interpolant (since the signature is relational, there are no functional symbols in ξ): $\models (\forall \bar{x} \,.\, \varphi') \to \xi$ and $\models \xi \to \exists \bar{y} \,.\, \neg\psi'$, as required. □

A *homomorphism* is a total functional logical relation.

Statement of Problem 2.13.12 "Lyndon's theorem". Show that a formula of first-order logic is preserved under surjective homomorphisms if, and only if, it is equivalent to a positive formula. *Hint: Express preservation under surjective homomorphisms as a first-order formula and apply Theorem 2.13.11 "Lyndon's interpolation theorem".* □

Solution of Problem 2.13.12 "Lyndon's theorem". The "if" direction has been proved in Problem 2.11.3 "Fundamental property".

For the "only if" direction, assume φ is preserved under surjective homomorphisms. W.l.o.g. we assume that the signature contains a single unary relational symbol R. We express that φ is preserved under surjective homomorphisms within the logic. If $h : A \to B$ is a surjective homomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$, then $\mathfrak{B}$ is obtained from $\mathfrak{A}$ by 1) introducing an equivalence relation $\approx \subseteq A \times A$ on the elements of A ($a \approx a'$ iff $h(a) = h(b)$), and 2) extending $R^{\mathfrak{A}}$ with new elements in a $\approx$-compatible manner. Let R' be a copy of R. The following the sentence axiomatises the two conditions above:

$$\begin{aligned}\psi \equiv\ & \forall x \,.\, x \approx x \wedge \\ & \forall x, y \,.\, x \approx y \to y \approx x \wedge \\ & \forall x, y, z \,.\, x \approx y \wedge y \approx z \to x \approx z \wedge \\ & \forall x \,.\, R(x) \to R'(x) \wedge \\ & \forall x, y \,.\, R'(x) \wedge x \approx y \to R'(y).\end{aligned}$$

Let $\varphi' \equiv \varphi[R \mapsto R'][= \mapsto \approx]$ be obtained from φ by replacing R with R' and equality with $\approx$.

Claim. The formula φ is preserved under surjective homomorphisms if, and only if, $\models \varphi \wedge \psi \to \varphi'$.

The common symbols between $\varphi \wedge \psi$ and φ' are only R' and $\approx$, however only R' appears positively in both. By Lyndon's interpolation theorem, there exists an interpolant ξ using only R' positively, and thus ξ is a positive formula. By definition, $\models \varphi \wedge \psi \to \xi$ and $\models \xi \to \varphi'$. By taking "R'" to be "R" and "$\approx$" to be "$=$", we obtain, as required,

$$\models \varphi \leftrightarrow \xi.$$ □

Statement of Problem 2.13.13 "Łoś-Tarski's theorem". Show that a sentence is preserved under induced substructures if, and only if, it is equivalent to a universal sentence.[1] □

Solution of Problem 2.13.13 "Łoś-Tarski's theorem". For the "if" direction, note that $\mathfrak{B}$ is an induced substructure of $\mathfrak{A}$ if, and only if, there exists an injective, surjective, and faithful logical relation between $\mathfrak{A}$ and $\mathfrak{B}$. Thanks to Problem 2.11.3 "Fundamental property", such a relation preserves all universal formulas. □

Statement of Problem 2.13.14 "Robinson's joint consistency theorem". Show that, if Γ, Δ are satisfiable sets of sentences but $\Gamma \cup \Delta$ is not satisfiable, then there exists a sentence ξ over the shared variables and vocabulary s.t. $\Gamma \vDash \xi$ and $\Delta \vDash \neg\xi$. *Hint: Apply Problem 2.9.1 "Compactess theorem" and Problem 2.13.7 "Interpolation with equality".* □

Solution of Problem 2.13.14 "Robinson's joint consistency theorem". By Problem 2.9.1 "Compactess theorem", there exist finite nonempty sets $\Gamma' = \{\varphi_1, \dots, \varphi_m\} \subseteq_{\text{fin}} \Gamma$ and $\Delta' = \{\psi_1, \dots, \psi_n\} \subseteq_{\text{fin}} \Delta$ s.t. $\Gamma' \cup \Delta'$ is unsatisfiable. It suffices to apply Problem 2.13.7 "Interpolation with equality" to $\varphi_1 \wedge \cdots \wedge \varphi_m \vDash \neg\psi_1 \vee \cdots \vee \neg\psi_n$. □

2.14 Relational algebra

Statement of Problem 2.14.1. Show how to express intersection $E\&F$ in terms of the primitives above. □

Solution of Problem 2.14.1. One solution is to use double negation $E\&F = E - (E - F)$. If negation is not available, another solution is $E\&F = \pi_{1,\dots,n}\sigma_{1=n+1,\cdots,n=n+n}(E \times F)$. □

Statement of Problem 2.14.2. Show that given any relational algebra expression E of dimension k one can write an equivalent formula of first-order

[1] Preservation under induced substructures on all finite models has been conjectured in 1958 by Scott and Suppes [27]. Tait showed that Łoś-Tarski's theorem does not hold on finite structures [31].

logic $\varphi_E(x_1, \ldots, x_k)$ with k free variables. *Hint: Proceed by structural induction on expressions.* □

Solution of Problem 2.14.2. A straightforward induction does the job:

$$
\begin{aligned}
\varphi_{\bar{a}}(\bar{x}) &\equiv x_1 = a_1 \wedge \cdots \wedge x_k = a_k,\\
\varphi_{R_i}(\bar{x}) &\equiv R_i(\bar{x}),\\
\varphi_{E+F}(\bar{x}) &\equiv \varphi_E(\bar{x}) \vee \varphi_F(\bar{x}),\\
\varphi_{E-F}(\bar{x}) &\equiv \varphi_E(\bar{x}) \wedge \neg\varphi_F(\bar{x}),\\
\varphi_{E\times F}(\bar{x},\bar{y}) &\equiv \varphi_E(\bar{x}) \wedge \varphi_F(\bar{y}),\\
\varphi_{\sigma_{i=j}(E)}(\bar{x}) &\equiv \varphi_E(\bar{x}) \wedge x_i = x_j,\\
\varphi_{\pi_{i_1,\ldots,i_k}(E)}(\bar{x}) &\equiv \exists \bar{y} \,.\, \varphi_E(\bar{y}) \wedge x_1 = y_{i_1} \wedge \cdots \wedge x_k = y_{i_k}.
\end{aligned}
$$ □

Statement of Problem 2.14.3. Show that given a formula of first-order logic with equality $\varphi(x_1, \ldots, x_k)$ with k free variables and any dimension $n \geq k$, one can write an equivalent expression of relational algebra $E_{\varphi,n}$ of dimension n. *Hint: Proceed by structural induction preserving the invariant*

$$[\![E_{\varphi,n}]\!] = \{\bar{a} \in A^n \mid \mathfrak{A}, \bar{x} : \bar{a} \vDash \varphi\}.$$ □

Solution of Problem 2.14.3. Consider a first-order formula φ over relational symbols $\Sigma = \{R_1, \ldots, R_n\}$. Let the domain of all relations be captured by the expression

$$D = \sum_{i=1}^{n} \sum_{j=1}^{k_i} \pi_j(R_i).$$

We assume w.l.o.g. that in atomic formulas $R_i(x_{i_1}, \ldots, x_{i_{k_i}})$ all the indices are distinct; for example $R_i(x_3, x_3, x_1)$ can be expressed as $R_i(x_2, x_3, x_1) \wedge x_2 = x_3$. For every formula φ with m free variables and any dimension $n \geq m$, the corresponding relational expression $E_{\varphi,n}$ of dimension n is defined inductively as follows:

$$\begin{aligned}
E_{R_i(x_{i_1},\ldots,x_{i_{k_i}}),n} &= \pi_{j_1,\ldots,j_n}(R_i \times D^{n-k_i}),\\
E_{x_i=x_j,n} &= \sigma_{i=j} D^n,\\
E_{\varphi\vee\psi,n} &= E_{\varphi,n} + E_{\psi,n},\\
E_{\neg\varphi,n} &= D^n - E_{\varphi,n},\\
E_{\exists x_i\,.\,\varphi,n} &= \pi_{1,\ldots,i-1,i+1,\ldots,n}(E_{\varphi,n+1}),
\end{aligned}$$

where $j_1,\ldots,j_n$ is obtained as follows: Consider the partial permutation $(i_1,\ldots,i_{k_i})$ from $\{i_1,\ldots,i_{k_i}\}$ to $\{1,\ldots,k_i\}$ and extend it arbitrarily to a permutation $\rho = (i_1,\ldots,i_n)$ on $\{1,\ldots,n\}$; then, $(j_1,\ldots,j_n) = \rho^{-1}$ is the inverse permutation of ρ. □

2.15 Hilbert's proof system

Statement of Problem 2.15.1. As an example, we can prove the following familiar properties of equality.

$$\vdash x = y \to y = x, \tag{2.5}$$

$$\vdash x = y \wedge y = z \to x = z. \tag{2.6}$$

□

Solution of Problem 2.15.1. We take $R(x_1,x_2) \equiv x_2 = x_1$ in the derivation below:

1. $x = x$ (by (A7))
2. $\forall x_1,x_2,y_1,y_2\,.\,x_1 = y_1 \to x_2 = y_2 \to R(x_1,x_2) \to R(y_1,y_2)$ (by (A9))
3. $x = x \to x = y \to x = x \to y = x$ (by (A6) + (MP) + 2.)
4. $x = y \to x = x \to y = x$ (by (MP) from 1. and 3.)
5. $x = x \to x = y \to y = x$ (from 4.)
6. $x = y \to\to y = x$ (by (MP) from 1. and 5.)

Equation 5. has been obtained from 4. by propositional reasoning (details omitted).

□

Statement of Problem 2.15.2 "Soundness". Let $\Delta \cup \{\varphi\}$ be a set of first-order formulas. Then,

$$\Delta \vdash \varphi \quad \text{implies} \quad \Delta \vDash \varphi.$$

Hint: Proceed by complete induction on the length of proofs. □

Solution of Problem 2.15.2 "Soundness". In the base case, it suffices to check that 1) each axiom preserves validity in the sense that for each instantiation φ of (A1)–(A9), $\vDash \varphi$, and 2) for $\varphi \in \Delta$ then clearly $\Delta \vDash \varphi$. For the inductive step, $\Delta \vdash \varphi$ is obtained by (MP) to previously established theorems $\Delta \vdash \psi \to \varphi$ and $\Delta \vdash \psi$, whose proofs are thus strictly shorter than the proof of $\Delta \vdash \varphi$. By the inductive hypothesis, $\Delta \vDash \{\psi, \psi \to \varphi\}$. It follows from the definition of logical consequence "$\vDash$" then $\Delta \vDash \varphi$, as required. □

Statement of Problem 2.15.3 "Deduction theorem". Show that for Hilbert's proof system for first-order logic,

$$\Delta \vdash \varphi \to \psi \quad \text{if, and only if,} \quad \Delta \cup \{\varphi\} \vdash \psi.$$ □

Solution of Problem 2.15.3 "Deduction theorem". The proof of Problem 1.8.4 "Deduction theorem" can be repeated identically. At some point we used provability (B0) as a propositional tautology, which is also provable as a first-order logic tautology (its proof in Problem 1.8.1 uses only axioms (A1), (A2), and the deduction rule (MP)). □

Statement of Problem 2.15.4 "Generalisation theorem". Let $x \notin \mathsf{fv}(\Delta)$ be a variable not occurring free in any formula of Δ. Then,

$$\Delta \vdash \forall x \,.\, \varphi \quad \text{if, and only if,} \quad \Delta \vdash \varphi.$$ □

Hint: Use (A4), (A5), (A6), and (MP).

Solution of Problem 2.15.4 "Generalisation theorem". The "only if" direction is easy. Assume we have a proof of $\Delta \vdash \forall x \,.\, \varphi$. We instantiate (A6) with $t \equiv x$ and obtain the axiom $\vdash \forall x \,.\, \varphi \to \varphi$ (since x is admissible for x in φ and $\varphi[x \mapsto x] \equiv \varphi$). By (MP), we have $\Delta \vdash \varphi$, as required.

For the "if" direction, we proceed by induction on the length of the proof establishing $\Delta \vdash \varphi$. In the base case, φ is either an axiom or in Δ. Either way, by (A5) we have the axiom $\varphi \to \forall x\,.\,\varphi$, and thus by (MP) we have $\Delta \vdash \forall x\,.\,\varphi$, as required. In the inductive case, φ is necessarily obtained by applying (MP) to previously established theorems $\Delta \vdash \psi \to \varphi$ and $\Delta \vdash \psi$, whose proofs are thus strictly shorter than the proof of $\Delta \vdash \varphi$. Thus, by applying the inductive hypothesis twice we have $\Delta \vdash \forall x\,.\,\psi \to \varphi$ and $\Delta \vdash \forall x\,.\,\psi$. By instantiating axiom (A4) (with φ and ψ swapped) we have $(\forall x\,.\,\psi \to \varphi) \to \forall x\,.\,\psi \to \forall x\,.\,\varphi$. By a double application of (MP) we have $\Delta \vdash \forall x\,.\,\varphi$, as required. $\square$

Statement of Problem 2.15.5 "Renaming". Consider a formula φ and two variables x, y s.t. $y \notin \mathsf{fv}(\Delta \cup \{\varphi\})$ and y is free for x in φ. Then,

$$\Delta \vdash \forall x\,.\,\varphi \quad \text{implies} \quad \Delta \vdash \forall y\,.\,\varphi[x \mapsto y]. \qquad \square$$

Hint: Use (A4)*,* (A5)*,* (A6)*, and* (MP)*.*

Solution of Problem 2.15.5 "Renaming". Since $y \notin \mathsf{fv}(\varphi)$, also $y \notin \mathsf{fv}(\forall x\,.\,\varphi)$, and thus we can instantiate (A5) as $(\forall x\,.\,\varphi) \to \forall y\,.\,\forall x\,.\,\varphi$, and by (MP) we have

$$\Delta \vdash \forall y\,.\,\forall x\,.\,\varphi.$$

On the other hand, we can instantiate (A6) as $(\forall x\,.\,\varphi) \to \varphi[x \mapsto y]$, and since $y \notin \mathsf{fv}(\Delta)$, by Problem 2.15.4 "Generalisation theorem" we have

$$\Delta \vdash \forall y\,.\,(\forall x\,.\,\varphi) \to \varphi[x \mapsto y].$$

We suitably instantiate (A4) as

$$(\forall y\,.\,(\forall x\,.\,\varphi) \to \varphi[x \mapsto y]) \to (\forall y\,.\,\forall x\,.\,\varphi) \to \forall y\,.\,\varphi[x \mapsto y],$$

and thus by two applications of (MP) we get, as required,

$$\Delta \vdash \forall y\,.\,\varphi[x \mapsto y]. \qquad \square$$

2.15.1 Completeness

Statement of Problem 2.15.6. Show that the two formulations of completeness below are equivalent.

1. For every set of formulas $\Delta \cup \{\varphi\}$, $\Delta \vDash \varphi$ implies $\Delta \vdash \varphi$.

2. For every set of formulas Γ, if Γ is consistent, then it is satisfiable (i.e., it has a model). $\square$

Solution of Problem 2.15.6. For the "$1 \to 2$" direction, assume $\Gamma \nvdash \bot$. By instantiating the first point with $\Delta = \Gamma$ and $\varphi \equiv \bot$, we have $\Gamma \nvDash \bot$, i.e., there is a structure $\mathfrak{A}$ s.t. $\mathfrak{A} \vDash \Gamma$ and $\mathfrak{A} \nvDash \bot$. The second condition is trivial, and the first one says that Γ has a model, as required.

For the "$2 \to 1$" direction, assume $\Delta \vDash \varphi$. By way of contradiction, assume $\Delta \nvdash \varphi$. We claim that $\Delta \cup \{\neg\varphi\}$ is consistent: Again by contradiction, if $\Delta \cup \{\neg\varphi\} \vdash \bot$, then by Problem 2.15.3 "Deduction theorem" $\Delta \vdash \neg\varphi \to \bot$; by the definition of "$\neg$", $\Delta \vdash \neg\neg\varphi$, and thus by (A3) and (MP) we have $\Delta \vdash \varphi$, which is a contradiction. By the second point applied to $\Gamma = \Delta \cup \{\neg\varphi\}$, the latter set is satisfiable, i.e., there is a structure $\mathfrak{A}$ and a valuation ϱ s.t. $\mathfrak{A}, \varrho \vDash \Delta \cup \{\neg\varphi\}$. This witnesses $\Delta \nvDash \varphi$, which is contradiction. $\square$

Statement of Problem 2.15.7 "Saturation". Any consistent set of sentences Δ extends to a consistent and saturated set of sentences $\Gamma \supseteq \Delta$ (over a larger signature). $\square$

Solution of Problem 2.15.7 "Saturation". We show a solution for a countable signature Σ. Let $\Delta = \{\varphi_0, \varphi_1, \dots\}$ be a consistent set of sentences over Σ. We extend Σ to a countable signature $\Sigma' = \Sigma \cup C$, where $C = \{b_0, b_1, \dots\}$ contains countably many fresh constant symbols $b_i \notin \Sigma$. The set Δ is consistent also over Σ' since no formula in Δ contains any b_i. Let $\psi_0(x), \psi_1(x), \dots \in \mathsf{Th}(\Sigma')$ be an enumeration of all formulas over Σ' s.t. ψ_i has a single free variable $\mathsf{fv}(\psi_i) = \{x\}$. We construct a sequence of constant symbols $c_0, c_1, \dots \in C$ and a nondecreasing sequence of sets of formulas

$$\Gamma_0 \subseteq \Gamma_1 \subseteq \cdots$$

as follows. For every $n \geq 0$, let c_n be the constant b_i of minimal index i not occurring previously in $\Gamma_n \cup \{\psi_n\}$. Initially, $\Gamma_0 = \Delta$, and thus $c_0 = b_0$. For every $n \geq 0$, we take

$$\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\neg\psi_n[x \mapsto c_n]\} & (\dagger) \text{ if } \Gamma_n \nvdash \forall x \,.\, \psi_n, \\ \Gamma_n & \text{otherwise.} \end{cases}$$

The Γ_{n+1} thus constructed is consistent. By contradiction, assume $\Gamma_{n+1} \vdash \bot$ and n is the least index s.t. this happens. Thus case $(\dagger)$ above holds. By Problem 2.15.3 "Deduction theorem" and the definition of negation "$\neg$", we would have $\Gamma_n \vdash \neg\neg\psi_n[x \mapsto c_n]$, and thus by (A3) even $\Gamma_n \vdash \psi_n[x \mapsto c_n]$. Let y be a globally fresh variable. We can repeat the proof of $\Gamma_n \vdash \psi_n[x \mapsto c_n]$ with c_n replaced by y and obtain a proof of $\Gamma_n \vdash \psi_n[x \mapsto y]$. Since y does not occur free in Γ_n, by Problem 2.15.4 "Generalisation theorem" we have $\Gamma_n \vdash \forall y \,.\, \psi_n[x \mapsto y]$. Since x is free for y in $\psi_n[x \mapsto y]$ and we can assume that x does not appear free in any formula of Γ_n, by Problem 2.15.5 "Renaming" we have $\Gamma_n \vdash \forall x \,.\, \psi_n[x \mapsto y][y \mapsto x]$. Since $\psi_n[x \mapsto y][y \mapsto x] \equiv \psi_n$, this contradicts $(\dagger)$.

Now let

$$\Gamma_\omega = \bigcup_{n=0}^{\infty} \Gamma_n$$

be the limit of the sequence of formulas thus constructed. Also Γ_ω is consistent, since $\Gamma_\omega \vdash \bot$ would already imply $\Gamma_n \vdash \bot$ for some finite n (since proofs have finite length and can thus use only finitely many assumptions). We show that Γ_ω is saturated (w.r.t. its signature, which is Σ'). Consider an arbitrary formula $\varphi_n \in \mathsf{Th}(\Sigma')$ of one free variable x s.t. $\Gamma_\omega \nvdash \forall x \,.\, \varphi_n$. Since $\Gamma_n \subseteq \Gamma_\omega$, in particular this means that $\Gamma_n \nvdash \forall x \,.\, \varphi_n$, and thus, by $(\dagger)$, $\Gamma_{n+1} = \Gamma_n \cup \{\neg\psi_n[x \mapsto c_n]\}$ Consequently, $\Gamma_{n+1} \vdash \neg\psi_n[x \mapsto c_n]$, and thus $\Gamma \vdash \neg\psi_n[x \mapsto c_n]$, as required. □

Let Γ be a saturated set of sentences over signature Σ. We define the following relation on the constant symbols in Σ:

$$c \sim_\Gamma d \quad \text{if, and only if,} \quad \Gamma \vdash c = d.$$

Intuitively, $c \sim_\Gamma d$ means that they are provably equal from the axioms in Γ.

Statement of Problem 2.15.8 "Congruence". Prove the following two crucial properties of $\sim_\Gamma$.

1. The relation $\sim_\Gamma$ is an equivalence: For every constants $c, d, e \in \Sigma$,

$$\begin{array}{lll} c \sim_\Gamma c, & & \\ c \sim_\Gamma d & \text{implies} & d \sim_\Gamma c, \\ c \sim_\Gamma d \text{ and } d \sim_\Gamma e & \text{implies} & c \sim_\Gamma e. \end{array}$$

2. The relation $\sim_\Gamma$ is a congruence w.r.t. the function symbols in Σ: For every n-ary function symbol $f : n \in \Sigma$ and constants $c_1, d_1, \ldots, c_n, d_n \in \Sigma$,

$$c_1 \sim_\Gamma d_1, \cdots, c_n \sim_\Gamma d_n \text{ implies } f(c_1, \ldots, c_n) \sim_\Gamma f(d_1, \ldots, d_n).$$ □

Solution of Problem 2.15.8 "Congruence". □

We are now ready to build a syntactic model. Let $\Sigma_0 \subseteq \Sigma$ be the set of constant symbols in Σ. Consider the structure $\mathfrak{A}_\Gamma = (A, \Sigma)$ over signature Σ, where the domain is the set of equivalence classes $A = \Sigma_0 / \sim_\Gamma$ of constants w.r.t. the congruence $\sim_\Gamma$, each constant $c \in \Sigma_0$ is interpreted as its equivalence class

$$c^{\mathfrak{A}_\Gamma} = [c]_{\sim_\Gamma},$$

each n-ary functional symbol $f \in \Sigma$ is interpreted as the relation $\subseteq A^n \times A$ defined as:

$$f^{\mathfrak{A}_\Gamma}([c_1]_{\sim_\Gamma}, \ldots, [c_n]_{\sim_\Gamma}) = [d]_{\sim_\Gamma} \quad \text{if, and only if,} \quad f(c_1, \ldots, c_n) \sim_\Gamma d,$$

and every n-ary relational symbol $R \in \Sigma$ is interpreted as the n-ary relation $\subseteq A^n$ defined as

$$([c_1]_{\sim_\Gamma}, \ldots, [c_n]_{\sim_\Gamma}) \in R^{\mathfrak{A}_\Gamma} \quad \text{if, and only if,} \quad \Gamma \vdash R(c_1, \ldots, c_n).$$

Thanks to the fact that $\sim_\Gamma$ is a congruence, the definition of $f^{\mathfrak{A}_\Gamma}$ does not depend on the choice of representatives and denotes indeed a partial function $A^n \to A$.

Statement of Problem 2.15.9 "Functionality". Show that the interpretation of $f^{\mathfrak{A}_\Gamma}$ above does indeed define a total function $A^n \to A$: For every $c_1, \ldots, c_n$, there is d s.t. $f(c_1, \ldots, c_n) \sim_\Gamma d$. *Hint: Use the fact that* Γ *is saturated.* □

Solution of Problem 2.15.9 "Functionality". □

Statement of Problem 2.15.10 "Terms". Show that for every term t over Σ with free variables $\mathsf{fv}(t) = \{x_1, \ldots, x_n\}$, valuation $\varrho : X \to A$ with $\varrho(x_1) = [c_1]_{\sim_\Gamma}, \ldots, \varrho(x_n) = [c_n]_{\sim_\Gamma}$, and constant d,

$$[\![t]\!]_\varrho = [d]_{\sim_\Gamma} \quad \text{if, and only if,} \quad t[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] \sim_\Gamma d.$$

Hint: Use structural induction on terms. □

Solution of Problem 2.15.10 "Terms". □

Statement of Problem 2.15.11 "Relations". Show that the interpretation of $R^{\mathfrak{A}_\Gamma}$ is well-defined, in the sense that does not depend on the chosen representatives. *Hint: Use* (A9). □

Solution of Problem 2.15.11 "Relations". □

Statement of Problem 2.15.12 "Implication". Let $\psi^* \equiv \psi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$ and $\xi^* \equiv \xi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$. Show that

$$\Gamma \vdash \psi^* \to \xi^* \quad \text{if, and only if,} \quad \Gamma \vdash \psi^* \text{ implies } \Gamma \vdash \xi^*$$

Hint: □

Solution of Problem 2.15.12 "Implication". □

Statement of Problem 2.15.13 "Universal quantification". Let $\psi^* \equiv \psi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$ Show that

$$\Gamma \vdash \forall x_0 \,.\, \psi^* \quad \text{if, and only if,} \quad \text{for all } [c_0]_{\sim_\Gamma} \in A, \Gamma \vdash \psi^*[x_0 \mapsto c_0].$$

Hint: Use the fact that Γ *is saturated and* (A6). □

Solution of Problem 2.15.13 "Universal quantification". □

Statement of Problem 2.15.14 "Formulas". Show that for every first-order formula φ over Σ with free variables $\mathsf{fv}(\varphi) = \{x_1, \dots, x_n\}$, and valuation $\varrho : X \to A$ with $\varrho(x_1) = [c_1]_{\sim_\Gamma}, \dots, \varrho(x_n) = [c_n]_{\sim_\Gamma}$,

$$\mathfrak{A}_\Gamma, \varrho \vDash \varphi \quad \text{if, and only if,} \quad \Gamma \vdash \varphi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n].$$

Hint: Use structural induction on formulas. □

Solution of Problem 2.15.14 "Formulas". Case $\varphi \equiv u = v$: We have:

$$\begin{aligned}
\mathfrak{A}_\Gamma, \varrho \vDash \varphi \quad & \text{iff} \quad \mathfrak{A}_\Gamma, \varrho \vDash u = v && \text{(by def. of } \varphi\text{)} \\
& \text{iff} \quad [\![u]\!]_\varrho = [\![v]\!]_\varrho && \text{(by def. of } \vDash\text{)} \\
& \text{iff} \quad u[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] \sim_\Gamma v[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] && \text{(by Problem 2.15.10 "} \\
& \text{iff} \quad \Gamma \vdash u[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] = v[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] && \text{(by def. of } \sim_\Gamma\text{)} \\
& \text{iff} \quad \Gamma \vdash \varphi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] && \text{(by def. of } \varphi\text{).}
\end{aligned}$$

Case $\varphi \equiv R(t_1, \dots, t_m)$: We have:

$$\begin{aligned}
\mathfrak{A}_\Gamma, \varrho \vDash \varphi \quad & \text{iff} \quad \mathfrak{A}_\Gamma, \varrho \vDash R(t_1, \dots, t_n) && \text{(by def. of } \varphi\text{)} \\
& \text{iff} \quad ([c_1]_{\sim_\Gamma}, \dots, [c_n]_{\sim_\Gamma}) \in R^{\mathfrak{A}_\Gamma} && \text{(by def. of } \vDash\text{)} \\
& \text{iff} \quad \Gamma \vdash R(c_1, \dots, c_n) && \text{(by def. of } R^{\mathfrak{A}_\Gamma}\text{)} \\
& \text{iff} \quad \Gamma \vdash \varphi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n] && \text{(by def. of } \varphi\text{).}
\end{aligned}$$

Case $\varphi \equiv \psi \to \xi$: Let $\varphi^* \equiv \psi^* \to \xi^*$, with $\psi^* \equiv \psi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$ and $\xi^* \equiv \xi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$. We have:

$$\begin{aligned}
\mathfrak{A}_\Gamma, \varrho \vDash \varphi \quad & \text{iff} \quad \mathfrak{A}_\Gamma, \varrho \vDash \psi \to \xi && \text{(by def. of } \varphi\text{)} \\
& \text{iff} \quad \mathfrak{A}_\Gamma, \varrho \vDash \psi \text{ implies } \mathfrak{A}_\Gamma, \varrho \vDash \xi && \text{(by def. of } \vDash\text{)} \\
& \text{iff} \quad \Gamma \vdash \psi^* \text{ implies } \Gamma \vdash \xi^* && \text{(by ind. hyp. } \times 2\text{)} \\
& \text{iff} \quad \Gamma \vdash \psi^* \to \xi^* && \text{(by Problem 2.15.12 "Implication")} \\
& \text{iff} \quad \Gamma \vdash \varphi^* && \text{(by def. of } \varphi\text{).}
\end{aligned}$$

Case $\varphi \equiv \forall x_0 . \psi$: Let $\mathsf{fv}(\psi) \subseteq \{x_0, x_1, \ldots, x_n\}$, $\varphi^* \equiv \forall x_0 \psi^*$, with $\psi^* \equiv \psi[x_1 \mapsto c_1]\cdots[x_n \mapsto c_n]$. Thus, $\mathsf{fv}(\psi^*) \subseteq \{x_0\}$. We have:

$$\begin{array}{lll} \mathfrak{A}_\Gamma, \varrho \vDash \varphi & \text{iff} \quad \mathfrak{A}_\Gamma, \varrho \vDash \forall x_0 . \psi & \text{(by def. of } \varphi) \\ & \text{iff} \quad \text{for all } [c_0]_{\sim_\Gamma} \in A, \mathfrak{A}_\Gamma, \varrho[x_0 \mapsto c_0] \vDash \psi & \text{(by def. of } \vDash) \\ & \text{iff} \quad \text{for all } [c_0]_{\sim_\Gamma} \in A, \Gamma \vdash \psi^*[x_0 \mapsto c_0] & \text{(by ind. hyp.)} \\ & \text{iff} \quad \Gamma \vdash \forall x_0 . \psi^* & \text{(by Problem 2.15.13 “Universal qua} \\ & \text{iff} \quad \Gamma \vdash \varphi^* & \text{(by def. of } \varphi). \end{array}$$

□

Statement of Problem 2.15.15 “Sentences”. Show that for every first-order sentence φ over Σ

$$\mathfrak{A}_\Gamma \vDash \varphi \quad \text{if, and only if,} \quad \Gamma \vdash \varphi.$$

In particular, $\mathfrak{A}_\Gamma \vDash \Gamma$. *Hint: Use Problem 2.15.14 “Formulas”.* □

Solution of Problem 2.15.15 “Sentences”. □

Statement of Problem 2.15.16 “Strong completeness theorem”. Let φ be a formula and let Δ be a set of formulas (possibly infinite). Then,

$$\Delta \vDash \varphi \quad \text{implies} \quad \Delta \vdash \varphi.$$

□

Solution of Problem 2.15.16 “Strong completeness theorem”. By Problem 2.15.6 it suffices to show that if a set of sentences Δ is consistent, then it has a model. By Problem 2.15.7 “Saturation” we can extend Δ to a consistent and saturated set of sentences $\Gamma \supseteq \Delta$. By Problem 2.15.15 “Sentences”, there is a model $\mathfrak{A}_\Gamma \vDash \Gamma$, as required. □

Chapter 3

Second-order predicate logic

3.1 Expressiveness

Statement of Problem 3.1.1 "Finiteness". Write a sentence of universal second-order logic which is satisfied precisely in finite models. Can this be done in $\forall\mathsf{MSO}$? □

Solution of Problem 3.1.1 "Finiteness". We axiomatise that every injective function on X is surjective, for every X, which is possible only in finite models (we will reuse the following definitions later):

$$\begin{aligned}
\varphi_{\text{fin}} &\equiv \forall X \,.\, \varphi_{\text{fin}}(X), \text{ where} \\
\varphi_{\text{rel}}(F, X, Y) &\equiv \forall x, y \,.\, F(x, y) \to X(x) \wedge Y(y), \\
\varphi_{\text{fun}}(F, X, Y) &\equiv \varphi_{\text{rel}}(F, X, Y) \wedge \forall x, y, z \,.\, F(x, y) \wedge F(x, z) \to y = z, \\
\varphi_{\text{inj}}(F) &\equiv \forall x, y, z \,.\, F(x, y) \wedge F(z, y) \to x = z, \\
\varphi_{\text{surj}}(F) &\equiv \forall y \,.\, \exists x \,.\, F(x, y), \\
\varphi_{\text{fin}}(X) &\equiv \forall F \,.\, \varphi_{\text{fun}}(F, X, X) \wedge \varphi_{\text{inj}}(F) \to \varphi_{\text{surj}}(F).
\end{aligned}$$

Finiteness cannot be axiomatised in $\forall\mathsf{MSO}$. Towards reaching a contradiction, fix the empty signature Σ = let $\varphi \equiv \forall X_1, \ldots, X_n \,.\, \psi$ (with ψ first-order) a purported $\forall\mathsf{MSO}$ formula axiomatising finiteness of models over Σ, and take an infinite model $\mathfrak{A}$. There are subsets $A_1, \ldots, A_n$ of the domain s.t. $\mathfrak{A}, X_1 : A_1, \ldots, X_n : A_n \models \neg\psi$. Since ψ is first-order and uses only equality, we can make the universe finite while preserving it. Let k be the rank of ψ. For every index set $I \subseteq \{1,\ldots,n\}$, consider $A_I = \bigcap_{i\in I} A_i$. The A_I's partition the domain. We construct a finite model $\mathfrak{B}$ by removing elements from $\mathfrak{A}$ in such a way that every infinite A_I has k elements in $\mathfrak{B}$. Let $B_i \subseteq A_i$ be obtained by restricting A_i to $\mathfrak{B}$. We have $\mathfrak{B}, X_1 : B_1, \ldots, B_n : B_n \vDash \neg\psi$, and thus $\mathfrak{B} \nvDash \varphi$, contradicting that φ expresses finiteness of the model. □

Statement of Problem 3.1.2 "Countability". Write a sentence of second-order logic which is satisfied precisely in countable models.

□

Solution of Problem 3.1.2 "Countability". We axiomatise that every infinite subset of the domain has the same cardinality as the domain itself (where $\varphi_{\text{inf}}(X) \equiv \neg\varphi_{\text{fin}}(X)$ is an existential formula axiomatising infiniteness of X):

$$\begin{aligned}\varphi_{count} \equiv\ & \forall X, U\,.\,(\forall x\,.\,U(x)) \wedge \varphi_{\text{inf}}(X) \rightarrow \\ & \exists F\,.\,\varphi_{\text{fun}}(F, X, U) \wedge \varphi_{\text{inj}}(F) \wedge \varphi_{\text{surj}}(F).\end{aligned}$$ □

Statement of Problem 3.1.3 "Spectrum". Show that spectra of second-order logic are closed under complement. (The analogous statement for first-order spectra is a long-standing open problem.) □

Solution of Problem 3.1.3 "Spectrum". Note that obviously

$$\mathsf{Spec}(\varphi) = \mathsf{Spec}(\psi), \quad \text{with } \psi \equiv \exists R_1, \ldots, R_n\,.\,\varphi,$$

where $R_1, \ldots, R_n$ are all the elements of the signature of φ. Since the signature of ψ is empty and over the empty signature, for every cardinality $n \in \mathbb{N}$, there exists precisely a single structure of cardinality n (up to isomorphism), it follows that, for each $n \in \mathbb{N}$,

$$n \in \mathsf{Spec}(\psi) \quad \text{if, and only if,} \quad n \notin \mathsf{Spec}(\neg\psi).$$ □

Statement of Problem 3.1.4. Construct a sentence of MSO whose spectrum is the set of prime numbers. □

Solution of Problem 3.1.4. Take the signature and axioms of set theory, and an additional sentence saying that every element except the unit generates the whole group:

$$\begin{aligned}\forall x, X\,.\,(\exists y\,.\,x \cdot y \neq y \wedge X(x) \wedge \forall y\,.\,X(y) \to X(y \cdot x))\\ \to \forall y\,.\,X(y).\end{aligned}$$

□

3.1.1 Directed graphs

Statement of Problem 3.1.5 "Reachability for directed graphs". Consider a directed graph (V, E) with edge relation $E \subseteq V \times V$. Write a universal formula of second-order logic expressing the reflexive-transitive closure E^* of E. Is it possible to express it with a monadic formula? And with an existential one (possibly non-monadic)? □

Solution of Problem 3.1.5 "Reachability for directed graphs". We express that E^* is the smallest relation including the identity and closed under composition with E:

$$\begin{aligned}\varphi_{E^*}(x,y) \;\equiv\; \forall R\,.\,(&\forall x\,.\,R(x,x) \wedge\\ &\forall x,y,z\,.\,R(x,y) \wedge E(y,z) \to R(x,z))\\ &\to R(x,y).\end{aligned}$$

In fact, we can do better and show that y belongs to the set of vertices $E^*(x)$ reachable from x. The latter is the smallest set of vertices including x and closed under application of E, thus yielding a universal monadic formula:

$$\psi_{E^*}(x,y) \;\equiv\; \forall F\,.\,(F(x) \wedge \forall x,y\,.\,F(x) \wedge E(x,y) \to F(y)) \to F(y).$$

We can also find a (nonmonadic) existential formula by guessing a path (a certain set of edges R) from x to y:

$$\begin{aligned}
\chi_{E^*}(x,y) \;\equiv\; & \exists R\,.\,x = y \vee \forall x,y\,.\,R(x,y) \rightarrow E(x,y)\ \wedge && (3.1)\\
& R(x,_) \wedge R(_,y)\ \wedge && (3.2)\\
& \forall x,y,z\,.\,R(x,y) \wedge R(x,z) \rightarrow y = z\ \wedge && (3.3)\\
& \forall x,y,z\,.\,R(x,y) \wedge R(z,x) \rightarrow x = z\ \wedge && (3.4)\\
& \forall x\,.\,x \neq y \wedge R(_,x) \rightarrow R(x,_),\ \text{where} && (3.5)
\end{aligned}$$

$$\begin{aligned}
R(_,x) &\equiv \exists y\,.\,R(y,x),\ \text{and}\\
R(x,_) &\equiv \exists y\,.\,R(x,y).
\end{aligned}$$

Line (3.1) says that R is a set of edges, (3.2) says that R selects an edge with source x and an edge with target y, (3.3) says that at most one outgoing edge is selected from every source, (3.4) says the same for incoming edges, and (3.5) says that every node with an incoming edge must also have an outgoing edge, except for the destination y. On finite graphs, $\chi_{E^*}(x,y)$ holds precisely when there exists a path from x to y.

For infinite simple graphs, reflexive-transitive closure is not definable in existential monadic logic since the latter logic has the compactness property (c.f. Problem 3.2.1 "Compactness fails for $\forall$SO"). □

Statement of Problem 3.1.6 "Connectivity for directed graphs". A finite directed graph (V,E) is *strongly connected* if every two vertices are connected by a directed path. Show how to express strong connectivity in $\forall$MSO and $\exists$SO. □

Solution of Problem 3.1.6 "Connectivity for directed graphs". From Problem 3.1.5 "Reachability for directed graphs", there is a $\forall$MSO formula $\forall R\,.\,\varphi(x,y)$, with φ first-order, expressing reachability. Thus, $\forall x,y\,.\,\forall R\,.\,\varphi(x,y)$ expresses strong connectivity, and the latter formula is equivalent to the $\forall$MSO formula $\forall R\,.\,\forall x,y\,.\,\varphi(x,y)$.

Similarly, there is an $\exists$SO formula $\exists R\,.\,\varphi(x,y)$, with φ first-order and R binary, expressing reachability. Connectivity can be expressed by $\forall x,y\,.\,\exists R\,.\,\varphi(x,y)$, which is not yet a $\exists$SO formula. We can commute the quantifiers by adding two extra arguments to R, obtaining a four-ary relation $S(\_,\_,x,y)$ effectively representing a family of binary relations indexed by pairs (x,y). This argument yields the $\exists$SO formula $\exists S\,.\,\forall x,y\,.\,\varphi'$,

directed graphs	reachability	connectivity
$\forall$MSO	✓ (3.1.5)	✓ (3.1.6)
$\exists$SO	✓ (3.1.5)	✓ (3.1.6)
$\exists$MSO	no	no [14]

Figure 3.1: Expressing reachability/connectivity in directed graphs.

where φ' is obtained from φ by replacing every atomic formula of the form $R(u,v)$ by $S(u,v,x,y)$. □

Statement of Problem 3.1.7 "Eulerian cycles in $\exists$SO". Express the existence of a Eulerian cycle (c.f. Problem 2.12.23 "Eulerian cycles are not definable") in $\exists$SO. Is it possible to write a universal sentence as well? □

Solution of Problem 3.1.7 "Eulerian cycles in $\exists$SO". Over directed graphs, it is well-known that there exists an Eulerian cycle if, and only if, the graph is connected and for every vertex the number of incoming edges (indegree) is the same as the number of outgoing ones (outdegree). The first property can be expressed in $\exists$SO thanks to Problem 3.1.6 "Connectivity for directed graphs". For the second property, we can express that $f(u, \_, \_)$ is a family of bijections (indexed by vertices u's) between the set of edges entering u and the set of edges exiting u. (Over simple graphs, the latter property boils down to the fact that the degree of every vertex is even.) The latter property can be expressed in $\exists$SO. □

Statement of Problem 3.1.8 "Hamiltonian cycles in $\exists$SO". A *Hamiltonian cycle* in a finite directed graph is a path that visits each node exactly once.

1. Show that the existence of a Hamiltonian cycle in finite directed graphs can be expressed in $\exists$SO.

2. Show that the existence of an analogous formula in $\forall$SO would imply NPTIME = coNPTIME. □

Solution of Problem 3.1.8 "Hamiltonian cycles in ∃SO". We can express the existence of an Hamiltonian cycle by guessing a total order R of vertices in the graph, which refines the edge relation:

$$\forall x, y \,.\, R(x,y) \land (\forall z \,.\, R(x,z) \land R(z,y) \to z = x \lor z = y) \to E(x,y).$$

By Fagin's theorem [13, point 1 of Theorem 6], properties expressible in $\exists\mathsf{SO}$ coincide with the complexity class NPTIME, and thus $\forall\mathsf{SO}$ coincide with coNPTIME. Since Hamiltonicity is NPTIME-complete, if it was expressible in $\forall\mathsf{SO}$, then it would be in coNPTIME, and NPTIME = coNPTIME. □

Statement of Problem 3.1.9. Show that $\exists\mathsf{MSO}$ can already define some NPTIME-complete problem. *Hint: Express 3-colourability in* $\exists\mathsf{MSO}$. □

Solution of Problem 3.1.9. We can directly define 3-colourability as:

$$\begin{aligned}
&\exists X, Y, Z \,.\, \forall x \,.\, (X(x) \lor Y(x) \lor Z(x)) \land \\
&\forall x \,.\, \neg(X(x) \land Y(x)) \land \neg(Y(x) \land Z(x)) \land \neg(X(x) \land Z(x)) \land \\
&\forall x, y \,.\, E(x,y) \to \neg(X(x) \land X(y)) \land \neg(Y(x) \land Y(y)) \land \neg(Z(x) \land Z(y)).
\end{aligned}$$

□

Statement of Problem 3.1.10 "The Church-Rosser property is MSO definable". We have seen in Problem 2.9.14 "The Church-Rosser property is not axiomatisable (via compactness)" that the Church-Rosser property is not axiomatisable in first-order logic. Show that it can be defined in $\forall\mathsf{MSO}$. □

Solution of Problem 3.1.10 "The Church-Rosser property is MSO definable". Thanks to Problem 3.1.5 "Reachability for directed graphs" there exists a $\forall\mathsf{MSO}$ formula of two free first-order variables $\varphi_{\to^*}(x,y)$ expressing that there is a path from x to y. With such a formula in hand, the Church-Rosser property can be expressed directly with the sentence

$$\varphi_{\mathsf{CR}} \;\equiv\; \forall x, y, z \,.\, \varphi_{\to^*}(x,y) \land \varphi_{\to^*}(x,z) \to \exists t \,.\, \varphi_{\to^*}(y,t) \land \varphi_{\to^*}(z,t).$$

□

Statement of Problem 3.1.11 "Strong normalisation is MSO definable". We have seen in Problem 2.9.15 "Strong normalisation is not axiomatisable (via compactness)" that strong normalisation of a binary relation $E \subseteq A \times A$ (i.e., well-foundedness of $(E^*)^{-1}$) is not axiomatisable in first-order logic. Show that it is definable in $\forall\mathsf{MSO}$. □

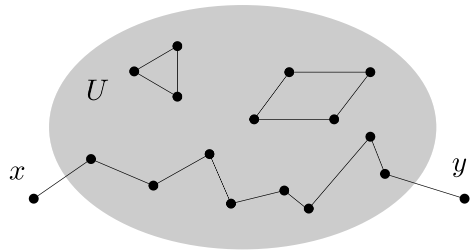


Figure for Problem 3.1.12.

Solution of Problem 3.1.11 "Strong normalisation is MSO definable". We express the fact that E is not strongly normalisable as

$$\exists X . \exists x . X(x) \wedge \forall x . X(x) \rightarrow \exists y . E(x, y) \wedge X(y). \qquad \square$$

3.1.2 Simple graphs

Statement of Problem 3.1.12. Consider simple (i.e., undirected, without self-loops) finite graphs (V, E). Find an $\exists$MSO formula expressing the transitive closure E^*. Is this possible for directed graphs? □

Solution of Problem 3.1.12. We can express that there is an undirected path from x to y by guessing a set of vertices U s.t. (3.6) x has exactly one neighbour in U, (3.7) y has exactly one neighbour in U, (3.8) every element in U has exactly two neighbours in U (c.f. figure):

$$\begin{aligned}
&\varphi_{E^*}(x, y) \equiv \exists U . \\
&\exists! z . E(x, z) \wedge U(z) \wedge && (3.6)\\
&\exists! z . E(z, y) \wedge U(z) \wedge && (3.7)\\
&\forall z . U(z) \rightarrow \exists u, v . u \neq v \wedge E(z, u) \wedge E(z, v) \wedge U(u) \wedge U(v). && (3.8)
\end{aligned}$$

Over finite simple graphs, the set U is interpreted as a undirected path from x to y, plus addionally some cycles.

An analogous formula for directed graphs fails because there may be back-edges along the directed path. In fact, there is no monadic existential formula expressing transitive closure over directed finite graphs [1]. □

simple graphs	reachability	connectivity
∀MSO	✓	✓
∃SO	✓	✓ (3.1.13)
∃MSO	✓ (!, 3.1.12)	no (3.1.13)

Figure 3.2: Expressing reachability/connectivity in simple graphs.

Statement of Problem 3.1.13 "Connectivity for simple graphs". Write a sentence φ_{conn} of MSO expressing that a simple graph is connected. Is it possible to express it in ∃MSO? □

Solution of Problem 3.1.13 "Connectivity for simple graphs". Thanks to Problem 3.1.12, let $\varphi_{E^*}(x, y)$ be an ∃MSO formula for reachability in the graph. We can express that the graph is connected as:

$$\varphi_{\text{conn}} \equiv \forall x, y \,.\, \varphi_{E^*}(x, y).$$

Notice that the formula above is not existential. Moreover, if we were to pull out the existential monadic quantifier $\exists U$ from φ_{E^*}, upon commutation with $\forall x, y$ it would give rise to an existential quantifier $\exists U'$ where U' would be a relation of arity three.

In fact, connectivity for simple graphs is not expressible in ∃MSO. It is known that connectivity for *directed graphs* cannot be expressed in ∃MSO [14]. If we had a formula ψ for connectivity, then we could relativise it to a set of vertices X by replacing all first-order quantifications $\exists x \,.\, \cdots$ with $\exists x \,.\, x \in X \wedge \cdots$, and second-order ones $\exists Y \,.\, \cdots$ with $\exists Y \,.\, Y \subseteq X \wedge \cdots$. Let $\psi(X)$ be this relativised formula. Then transitive closure can be expressed as $\varphi_{E^*}(x, y) \equiv \exists X \,.\, X(x) \wedge X(y) \wedge \psi(X)$. The latter formula is not ∃MSO, but it can be put in the existential format by pulling out the quantifiers in ψ. This contradicts the fact that reachability on simple graphs is not expressible in ∃MSO (c.f. Problem 3.1.12). □

Statement of Problem 3.1.14 "Graph minors in MSO". A graph G is a *minor* of a graph H if it can be obtained from the latter by contracting edges and removing edges and nodes. Let G be a fixed finite simple graph. Write a closed MSO formula φ_G s.t., for every simple graph H, $H \vDash \varphi_G$ holds if, and only if, H contains G as a minor. □

Solution of Problem 3.1.14 "Graph minors in MSO". Let $G = (U, E)$ have vertices $U = \{1, \dots, n \mid \}$, and let $H = (V, F)$. If G is a minor of H, then there are n pairwise disjoint nonempty sets of vertices $V_1, \dots, V_n \subseteq V$ of H s.t. each induced subgraph $H|_{V_i}$ is connected and, for every edge $(i, j) \in E$ in G, there are vertices $u \in V_i$ and $v \in V_j$ connected by an edge $(u, v) \in F$ in H. When G is fixed, we can express this condition directly in MSO. Let $\varphi_{\mathrm{conn}}(X)$ be an MSO formula of one set variable X stating that the subgraph induced by X is connected (a simple generalisation of φ_{conn} from Problem 3.1.13 "Connectivity for simple graphs"). The required formula is then

$$\begin{aligned}\varphi_G \equiv \exists V_1, \dots, V_n \,.\, & \bigwedge_i \varphi_{\mathrm{conn}}(V_i) \wedge \exists v \,.\, V_i(v) \wedge \\ & \bigwedge_{i \neq j} (\neg \exists v \,.\, V_i(v) \wedge V_j(v)) \wedge \\ & \bigwedge_{(i,j) \in E} \exists u, v \,.\, V_i(u) \wedge V_j(v) \wedge F(u, v).\end{aligned}$$ □

Statement of Problem 3.1.15 "Planarity of finite simple graphs in MSO". Express planarity of finite simple graphs (c.f. Problem 2.12.26 "Planarity is not axiomatisable") in MSO. □

Solution of Problem 3.1.15 "Planarity of finite simple graphs in MSO". By Wagner's theorem, a finite simpler graph is planar if, and only if, it has neither the complete graph K_5 (clique of 5 vertices) nor $K_{3,3}$ (complete bipartite graph of $3 + 3$ vertices) as a minor. By Problem 3.1.14 "Graph minors in MSO" there are closed MSO formulas φ_{K_5} and $\varphi_{K_{3,3}}$ expressing the existence of the respective minor. Then planarity is expressed by $\neg \varphi_{K_5} \wedge \neg \varphi_{K_{3,3}}$. □

3.1.3 MSO on trees

Statement of Problem 3.1.16. Consider the tree structure $\mathfrak{T} = (T, L, R, U)$, where the domain is the set of nodes $T = \{0, 1\}^*$, L, R are binary relations encoding the left, resp., right child ($L(w, w0)$ and $R(w, w1)$ hold for every

$w \in T$), and $U \subseteq T$ is an unspecified set of nodes. Express in MSO the existence of a path in T containing infinitely many elements of U. □

Solution of Problem 3.1.16. Let $\mathsf{path}(x, X)$ be an auxiliary formula stating that X is a path rooted at x:

$$\begin{aligned}
\mathsf{path}(x, X) \;\equiv\;& X(x) \wedge \\
& \forall y \,.\, X(y) \rightarrow \exists! z \,.\, X(z) \wedge (L(y, z) \vee R(y, z)) \wedge \\
& \forall y \,.\, X(y) \wedge y \neq x \rightarrow \exists z \,.\, X(z) \wedge (L(z, y) \vee R(z, y)).
\end{aligned}$$

Then, the required formula is

$$\begin{aligned}
& \exists x, X \,.\, \mathsf{path}(x, X) \wedge \\
& \forall y \,.\, X(y) \rightarrow \exists Y \,.\, \mathsf{path}(y, Y) \wedge \exists z \,.\, U(z) \wedge X(z) \wedge Y(z).
\end{aligned}$$
□

3.1.4 MSO on free monoids

Statement of Problem 3.1.17. Consider the free monoid of words over $\{a, b\}$

$$\mathfrak{A} = (\{a, b\}^*, \cdot, a, b, \varepsilon)$$

with additional constants a, b for one-letter words.

1. Prove that for every regular language $L \subseteq \{a, b\}^*$ there is a MSO formula $\varphi(x)$ with one free first-order variable *defining* L in the sense that

$$L = \{w \in \{a, b\}^* \mid \mathfrak{A}, x : w \models \varphi\}.$$

2. Find a formula of first-order logic with one free variable defining a non-regular language over $\Sigma = \{a, b\}$. □

Solution of Problem 3.1.17. For the first point, we translate a given regular expression r into an MSO formula $\varphi_r(x)$ of one free first-order variable x by structural induction on r:

$$\begin{aligned}
\varphi_\varepsilon(x) &\equiv x = \varepsilon, \\
\varphi_a(x) &\equiv x = a, \\
\varphi_b(x) &\equiv x = b, \\
\varphi_{s \cup t}(x) &\equiv \varphi_s(x) \vee \varphi_t(x), \\
\varphi_{s^*}(x) &\equiv \forall X \,.\, (X(\varepsilon) \wedge \forall x, y \,.\, X(x) \wedge \varphi_s(y) \rightarrow X(x \cdot y)) \rightarrow X(x).
\end{aligned}$$

In the last case, we encode Kleene star with a least fixpoint construction. For the second point, the language of squares $L = \{w \cdot w \mid w \in \Sigma^*\}$ is not regular and it is definable by $\varphi(x) \equiv \exists y \,.\, x = y \cdot y$. $\square$

Statement of Problem 3.1.18. Show that every context-free language is MSO definable over the free monoid (in the sense of Problem 3.1.17). $\square$

Solution of Problem 3.1.18. Let G be a context-free grammar with nonterminals $X_1, \ldots, X_n$, where X_1 is the initial nonterminal. We assume w.l.o.g. that G is in Chomsky normal form, i.e., all productions are of the form either $X_i \leftarrow X_j \cdot X_k$, or $X_i \leftarrow \varepsilon$ or $X_i \leftarrow a$, where $a \in \Sigma$ is a terminal symbol. The required formula $\varphi(x)$ is

$$\begin{aligned}\forall X_1, \ldots, X_n \,.\, ((&\bigwedge_{X_i \leftarrow X_j \cdot X_k} \forall y, z \,.\, X_j(y) \wedge X_k(z) \rightarrow X_i(y \cdot z)) \wedge \\ &(\bigwedge_{X_i \leftarrow a} X_i(a)) \wedge \\ &\bigwedge_{X_i \leftarrow \varepsilon} X_i(\varepsilon)) \rightarrow X_1(x).\end{aligned}$$ $\square$

3.2 Failures

Statement of Problem 3.2.1 "Compactness fails for ∀SO". Show that the compactness theorem fails for the universal fragment of second-order logic. What about its existential fragment? $\square$

Solution of Problem 3.2.1 "Compactness fails for ∀SO". Consider the set of sentences

$$\Gamma = \{\varphi_{\geq 1}, \varphi_{\geq 2}, \cdots\} \cup \{\varphi_{\mathrm{fin}}\}$$

obtained by adding the finiteness axiom φ_{fin} from Problem 3.1.1 "Finiteness" (which is a ∀SO sentence, but not an ∀MSO one) to the cardinality lower-bound constraints $\varphi_{\geq n}$ from Problem 2.1.6 "Cardinality constraints I". Every finite subset of Γ has a finite model, however Γ has no model.

The existential fragment of second-order logic satisfies the compactness theorem. An existential sentence $\exists R_1, \ldots, R_n \,.\, \varphi$, with φ first-order, has the same models as φ, and the same holds for a set Γ of such sentences after all the R_i's have been made globally fresh (one can think of R_i to be a name local to φ, and renaming is necessary if the same R_i appears in another sentence) Consider the set of first-order sentences $\widehat{\Gamma}$ obtained by removing the second-order quantifier prefix from sentences in Γ:

$$\widehat{\Gamma} = \{\varphi \mid \exists R_1, \ldots, R_n \, . \, \varphi \in \Gamma, \varphi \text{ first-order}\}. \tag{3.9}$$

It suffices to apply the compactness theorem for first-order logic to $\widehat{\Gamma}$. □

Statement of Problem 3.2.2 "Skolem-Löwenheim and SO*".* Consider the following problems relating the Skolem-Löwenheim theorem and second-order logic.

1. Prove that the Skolem-Löwenheim theorem does not hold for second-order logic.

2. Show that the Skolem-Löwenheim theorem does not hold for existential second-order logic.

3. Show that the Skolem-Löwenheim theorem does hold for universal second-order logic over the empty signature.

4. What happens in the case of universal second-order logic when the signature is not empty? *Hint: A non-empty signature provides additional prenex existential second-order quantifiers.* □

Solution of Problem 3.2.2 "Skolem-Löwenheim and SO*".* The Skolem-Löwenheim theorem does not hold in second-order logic (neither the upper nor the lower variant), since one can axiomatise countability of the model in SO (c.f. Problem 3.1.2 "Countability").

A Skolem-Löwenheim theorem for existential second-order logic follows from its first-order counterpart. Suppose that Γ is a set of existential second-order sentences over an at most countable signature Σ with an infinite model $\mathfrak{A}$, and let $\mathfrak{m}$ be any infinite cardinality. We can assume w.l.o.g. that Γ contains no two sentences differing only by the names of their quantified second-order variables (by removing the redundant ones). Consequently, the cardinality of the set of quantified variables does not exceed the cardinality of the set of all sentences. As in Problem 3.2.1 "Compactness fails for $\forall$SO", make the second-order variables globally fresh, and let $\widehat{\Gamma}$ be obtained from Γ according to (3.9). The set $\widehat{\Gamma}$ is an at most countable set of first-order sentences over a possibly larger but still countable signature. Moreover, $\widehat{\Gamma}$ is satisfiable, as witnessed by a suitable expansion $\widehat{\mathfrak{A}}$ of $\mathfrak{A}$ with additional interpretations $R_i^{\widehat{\mathfrak{A}}}$ for the existential second-order variables R_i's from Γ. By the Skolem-Löwenheim theorem for first-order logic, $\widehat{\Gamma}$ has a model $\mathfrak{B}$ of cardinality $\mathfrak{m}$. It is also a model of Γ, where each existential second-order quantifier $\exists R_i$ is witnessed by its interpretation $R_i^{\mathfrak{B}}$ in $\mathfrak{B}$.

A Skolem-Löwenheim theorem for universal second-order logic over the empty signature follows immediately from the previous point since, 1) if $\varphi \equiv \forall X_1, \dots, X_n \,.\, \psi$ with ψ first-order is universal, then $\neg\varphi$ is existential, and 2) when the signature is empty there is precisely one model of each cardinality (up to isomorphism), so φ has a model of cardinality $\mathfrak{m}$ if, and only if, $\neg\varphi$ has no model of cardinality $\mathfrak{m}$.

Finally, the theorem fails for universal second-order logic over the nonempty signature. For example, if we have the constant 0 and a unary function s, then the following sentence has only countable models:

$$
\begin{aligned}
&\forall X \,.\, (X(0) \wedge \forall y \,.\, X(y) \rightarrow X(s(y))) \rightarrow \forall y \,.\, X(y) \wedge && \text{(induction principle)}\\
&\forall x \,.\, s(x) \neq 0 \wedge && \text{(initial element)}\\
&\forall x, y \,.\, s(x) = s(y) \rightarrow x = y. && \text{(injectivity)}
\end{aligned}
$$

Thus the upward variant of the theorem fails.

Also the downward variant fails, since with a binary relation "<" one can write a second-order sentence φ has only uncountable models. Let $\varphi_{\mathrm{dlo}} = \bigwedge \Delta_{\mathrm{dlo}}$ be the (first-order) axioms for dense linear orders without endpoints (c.f. Problem 4.2.7 "Langford (1926) [20]"). For a monadic second-order variable X and a first-order variable x, we write $X \leq x$ for $\forall y \,.\, X(y) \rightarrow y \leq x$. Consider the universal sentence

$$
\varphi_{\mathrm{dlo}} \wedge \forall X \,.\, (\exists x \,.\, X \leq x) \rightarrow \exists x \,.\, X \leq x \wedge \forall y \,.\, X \leq y \rightarrow x \leq y. \quad \text{(completeness)}
$$

(The last condition says that every set with an upper bound has a least upper bound.) The sentence above has only uncountable models. Indeed, suppose to the contrary that there is a countable model. However, any countable dense linear order without endpoints is isomorphic to $(\mathbb{Q}, \leq)$, which does not satisfy the completeness statement—a contradiction. On the other hand $(\mathbb{R}, \leq)$ is a model of this sentence. Thus, the downward variant of the Skolem-Löwenheim theorem fails for second-order logic over the nonempty signature. □

3.3 Word models

Statement of Problem 3.3.3. Show that, for every NFA A one can effectively find an MSO sentence φ s.t. $L(A) = [\![\varphi]\!]$. □

Solution of Problem 3.3.3. We express the existence of an accepting run. Let the automaton A be over the alphabet $\Sigma = \{1, \dots, n\}$ and have m states $Q = \{1, \dots, m\}$. We introduce m MSO variables $X_1, \dots, X_m$ s.t. $x \in X_i$ iff when reading the input at position x the automaton is in state i. With this interpretation, we can write the following sentence:

$$
\begin{aligned}
\varphi \equiv \exists X_1, \dots, X_m \,.\, \forall x \,.\, \bigvee_i X_i(x) \;\wedge\; \bigwedge_{i \neq j} X_i \cap X_j = \varnothing \;\wedge& \qquad \text{(partition)}\\
\bigvee_{i \in I} X_i(0) \;\wedge& \qquad \text{(initial state)}\\
\forall x \,.\, \bigwedge_{i \in Q, a \in \Sigma} X_i(x) \wedge P_a(x) \to \bigvee_{i \xrightarrow{a} j} X_j(x+1) \;\wedge& \qquad \text{(transitions)}\\
\forall x \,.\, \bigwedge_{i \in Q, a \in \Sigma} X_i(x) \wedge P_a(x) \wedge \mathsf{last}(x) \to \bigvee_{i \xrightarrow{a} j \in F} \top .& \qquad \text{(final state)}
\end{aligned}
$$

We use $\mathsf{last}(x)$ to denote that x is the last position in the model. This can be expressed by, e.g., $\forall y \,.\, x \leq y \to x = y$. We use $X_j(x+1)$ as an abbreviation for $\forall y \,.\, x < y \wedge \neg(\exists z \,.\, x < z < y) \to X_j(y)$. □

Statement of Problem 3.3.4. Show that one can improve Problem 3.3.3 and produce an $\exists$MSO sentence with a *single* second-order quantifier. □

Solution of Problem 3.3.4. Let A be an NFA with k states $Q = \{0, \dots, k-1\}$ over alphabet Σ. For simplicity, we show the idea when the input is a multiple of $p = 2 \cdot k + 2$, i.e., we show that there exists an $\exists$MSO sentence of the form $\exists X \,.\, \psi$ with ψ first-order s.t. $L(A) \cap \Sigma^p = [\![\varphi]\!]$. The idea is to read the input p letters at a time. We represent the content of the second-order variable X as a sequence $z_0 z_1 \cdots \in \{0,1\}^\omega$ s.t. $n \in X$ iff $z_n = 1$. If after reading the $p \cdot i$-th letter $a_{p \cdot i}$ the automaton is in state $j \in Q$, then the bits $z_{p \cdot i} \cdots z_{p \cdot (i+1)-1}$ are precisely of the form

$$11\ 00 \cdots 00\ 01\ 00 \cdots 00,$$

The first two bits "11" are a marker delimiting the beginning of the block, and each pair of subsequent bits encodes a state. One can write the required sentence $\varphi \equiv \exists X . \psi$ checking that 1) each block has length p and starts with the control bits 11; 2) after the control bits, all the bit pairs are either of the form 00 or 01; 3) exactly one of them is of the form 01 (encoding that the automaton is in state j); 4) if the current block encodes that the automaton is in state j; and positions $p \cdot i, \ldots, (p \cdot (i+1) - 1)$ are labelled by letters $a_1, \ldots, a_p$, then the next block encodes that the automaton is in some state j' s.t. $j \xrightarrow{a_1 \cdots a_p} j'$; 5) the first block encodes that the automaton is in an initial state; 6) the last block encodes that the automaton is in a final state. We omit giving the sentence φ explicitly. □

Statement of Problem 3.3.5 "Star-free regular languages in first-order logic". Let Σ be a finite alphabet. A *star-free regular expression* over Σ is generated by the following grammar:

$$e, f ::= a \mid \Sigma^* \mid e \cup f \mid e \cdot f \mid \Sigma \setminus e,$$

where $a \in \Sigma$ and $\Sigma \setminus (\_)$ denotes the complementation operation. Show that star-free regular languages are definable in first-order logic over word models. *Hint: Construct the formula inductively over the structure of the expression. For this to go through, use formulas $\varphi_e(x, y)$ of two free variables x, y defining the language of words:*

$$[\![\varphi(x, y)]\!] = \{a_i \cdots a_{j-1} \in \Sigma^* \mid \mathcal{A}_{a_1 \ldots a_n}, x : i, y : j \models \varphi(x, y)\}. \qquad \square$$

Solution of Problem 3.3.5 "Star-free regular languages in first-order logic".

We proceed by structural induction on start-free expressions:

$$
\begin{aligned}
\varphi_a(x,y) &\equiv x < y \wedge P_a(x),\\
\varphi_{\Sigma^*}(x,y) &\equiv x \le y,\\
\varphi_{e \cup f}(x,y) &\equiv \varphi_e(x,y) \vee \varphi_f(x,y),\\
\varphi_{e \cdot f}(x,y) &\equiv \exists (x \le z \le y) \,.\, \varphi_e(x,z) \wedge \varphi_f(z,y),\\
\varphi_{\Sigma \setminus e}(x,y) &\equiv \neg \varphi_e(x,y).
\end{aligned}
$$

□

Statement of Problem 3.3.6. Show how to simulate first-order variables with MSO variables over word-models modulo the introduction of few new atomic formulas. *Hint: Interpret a first-order variable x as a second-order one representing the singleton $\{x\}$.* □

Solution of Problem 3.3.6. We introduce new atomic formulas:

$$
\begin{aligned}
X \subseteq Y &\equiv \forall x \,.\, X(x) \to Y(x), &(3.10)\\
X \subseteq P_a &\equiv \forall x \,.\, X(x) \to P_a(x), &(3.11)\\
X \le Y &\equiv \forall x, y \,.\, X(x) \wedge Y(y) \to x \le y, \text{ and} &(3.12)\\
\mathsf{singleton}(X) &\equiv \exists x \,.\, X(x) \wedge \forall y \,.\, X(y) \to y = x. &(3.13)
\end{aligned}
$$

We associate to a first-order variable a fresh second-order variable V_x. We define an inductive translation $[\_]$ from MSO formulas φ to formulas $[\varphi]$ without first-order variables (modulo the new atomic formulas above):

$$
\begin{aligned}
[x \le y] &\equiv V_x \le V_y,\\
[P_a(x)] &\equiv V_x \subseteq P_a,\\
[X(x)] &\equiv V_x \subseteq X,\\
[\exists x \,.\, \varphi] &\equiv \exists V_x \,.\, \mathsf{singleton}(V_x) \wedge [\varphi].
\end{aligned}
$$

The other connectives $\forall x, \exists X, \forall X, \wedge, \vee, \neg$ follow a similar pattern. □

Statement of Problem 3.3.8. Show that every MSO formula $\varphi(X_1, \ldots, X_k)$ with k free MSO variables $X_1, \ldots, X_k$ can be converted to an NFA A over Σ_k s.t. $[\![\varphi(X_1, \ldots, X_k)]\!] = [\![A]\!]$. *Hint: Proceed by structural induction on φ.* □

Solution of Problem 3.3.8. For each atomic formula φ from (3.10)–(3.13) one can build an equivalent NFA A_φ. Connectives $\vee, \wedge, \neg$ can be handled using the fact that NFA-recognisable languages are closed under Boolean operations. Finally, $\exists X_k \,.\, \varphi$ is handled by 1) inductively constructing an NFA A_φ over Σ_k equivalent to φ, and 2) projecting away the k-bit by replacing every transition in A_φ of the form $q \xrightarrow{(a,b_1,\dots,b_k)} q'$ by $q \xrightarrow{(a,b_1,\dots,b_{k-1})} q'$ (this operation possibly introduces nondeterminism). □

Statement of Problem 3.3.9 "c.f. [22, 29]". Fix an alphabet Σ. Construct an infinite sequence of satisfiable MSO formulas $\varphi_1, \varphi_2, \dots$ s.t., for every n, φ_n has size linear in n and the smallest word-model of φ_n has size

$$\geq 2^{2^{2^{\cdot^{\cdot^{2^n}}}}}\Big\}\, n \, .$$

□

Solution of Problem 3.3.9 "c.f. [22, 29]". We will work with regular expressions *with complementation* as a convenient tool, which can of course be converted succinctly into equivalent MSO formulas along the lines of Problem 3.3.3. Let $f(0) = 1$ and $f(n+1) = 2^{f(n)} \cdot (f(n)+1) + 1$, and assume the alphabet is of the form $\Sigma = \{0, 1, \$\}$. We will construct a family of regular expressions with complementation $e_0, e_1, \dots$ s.t. e_n generates exactly the singleton language

$$L(e_n) = \{0^{f(n)}\}.$$

The base case is simple enough: $e_0 = 0$. For the inductive case, assume e_n has already been constructed, and we proceed to construct e_{n+1}. First, we construct an expression f_n that generates a single word of length $f(n+1)$ by implementing a binary counter of $f(n)$ bits:

$$L(f_n) = \{\$w_0\$w_1\$\cdots\$w_{2^{f(n)}}\$\}$$

where each $w_i \in \{0,1\}^{f(n)}$ is a sequence of $f(n)$ bits and the number encoded by w_{i+1} is the successor of that encoded by w_i (thus $w_0 = 00\cdots0$, $w_{2^{f(n)}} = 11\cdots1$, and so on). If we are able to construct f_n, then we can obtain e_{n+1} from f_n by applying the morphism mapping all letters to 0. In turn, $f_n = \Sigma^* \setminus g_n$ is constructed as the complement of another expression g_n. The task for g_n is easier, because it suffices to find mistakes in the counter above. One kind of mistake is that a 0 in w_i is followed by a 0 in the corresponding position in w_{i+1}. In order to verify such a mistake, we can use the inductively constructed e_n in order to reliably skip the $f(n)+1$ symbols necessary to go from one position in w_i to the corresponding position in w_{i+1}. □

Statement of Problem 3.3.10. Is the language of palindromes over $\Sigma = \{0,1\}$ definable in MSO over word-models in the signature $\{\leq, P_0, P_1\}$, where P_0, P_1 are unary predicates encoding the labelling? □

Solution of Problem 3.3.10. No, the language of palindromes is not MSO definable. If it were so, then by Problem 3.3.8 it would be recognisable by a finite automaton, which can be shown not to be the case by a pumping argument. □

Statement of Problem 3.3.11. Consider the alphabet $\Sigma = \{a,b\}$. Is the language defined by the following SO sentence definable in MSO?

$$\begin{aligned}\varphi \equiv \exists R\,.\,\forall x,y\,.\,(R(x,y) \to (R(y,x) \wedge (P_a(x) \leftrightarrow P_b(y)))) \wedge \\ \forall x\,.\,\exists! y\,.\,R(x,y)\end{aligned}$$ □

Solution of Problem 3.3.11. No, the language $L = [\![\varphi]\!]$ is not regular. In order to see this, consider the language $M = L \cap a^*b^*$, which contains precisely all words of the form $a^n b^n$ with $n \geq 1$. A standard pumping argument shows that M is not regular, and since regular languages are closed under intersection, L is not regular either. □

Statement of Problem 3.3.12. Let $\Sigma = \{a,b\}$ be a binary alphabet. Prove that there is no MSO formula $\varphi(x,y,z)$ s.t. for every finite word $w \in \Sigma^*$ and positions $a,b,c \in \{0,\ldots,|w|-1\}$,

$$\mathfrak{A}_w, x:a, y:b, z:c \vDash \varphi \quad \text{if, and only if,} \quad a+b \equiv c \pmod{|w|}.$$

Hint: Show how to use φ to construct a nonregular language. □

Solution of Problem 3.3.12. Suppose that such a φ exists. We are going to demonstrate that it can be used to define a nonregular language of word-models, contradicting Problem 3.3.8. First, we express that z is the middle position in the word:

$$\mathsf{mid}(z) \equiv \exists x\,.\,\forall y\,.\,y \leq x \land z \neq x \land \varphi(z, z+1, x).$$

We can now define the nonregular language $\{a^n b^n \mid n \in \mathbb{N}\}$ with the sentence

$$\exists z\,.\,\mathsf{mid}(z) \land \forall y\,.\,(y \leq z \to P_a(y)) \land (y > z \to P_b(y)). \qquad \square$$

3.4 Miscellaneous problems

Statement of Problem 3.4.1 "Elementary separability of projective classes". A set of models is an *elementary class* if it is the set of models of a sentence of first-order logic, and it is a *projective class* if it is the set of models of an existential sentence of second-order logic. Show that any two disjoint projective classes can be separated by an elementary class. *Hint: Use interpolation.* $\square$

Solution of Problem 3.4.1 "Elementary separability of projective classes". Let C_1 be the projective class of models of $\exists\overline{R}\,.\,\varphi$ and C_2 that of $\exists\overline{T}\,.\,\psi$, where φ, ψ are sentences of first-order logic. Since C_1, C_2 are disjoint, $\vDash \neg(\exists\overline{R}\,.\,\varphi \land \exists\overline{T}\,.\,\psi)$, and thus $\vDash \varphi \to \neg\psi$. By Craig's interpolation theorem (c.f. Problem 2.13.6 "Interpolation for formulas without equality"), there exists an interpolant ξ defining an elementary class separating C_1 from C_2. $\square$

Statement of Problem 3.4.2. Consider the standard field of real numbers $(\mathbb{R}, +, \cdot, 0, 1)$. Write an MSO formula $\varphi(x)$ which holds precisely when x is a rational number: For every $a \in \mathbb{R}$,

$$\mathbb{R}, x : a \vDash \varphi \quad \text{if, and only if,} \quad a \in \mathbb{Q}.$$

Can the sentence be written in the universal fragment of SO? $\square$

Solution of Problem 3.4.2. Consider the formula $\mathsf{cl}(X)$ stating that X contains 0 and is closed under successor and predecessor:

$$\mathsf{cl}(X) \equiv X(0) \land \forall n\,.\,X(n) \to X(n+1) \land \exists m\,.\,n = m+1 \land X(m).$$

There are many sets satisfying $\mathsf{cl}(X)$, e.g., $\mathbb{Z}$ (the least such set), $\mathbb{Q}$, $\mathbb{R}$ among others. We now express that x is of the form p/q for some $p, q \in X$, and this holds for every closed X, and in particular for the least such set $\mathbb{Z}$, yielding the following $\forall\mathsf{MSO}$ formula:

$$\varphi(x) \equiv \forall X \,.\, \mathsf{cl}(X) \to \exists p, q \,.\, X(p) \land X(q) \land p \neq 0 \land x \cdot q = p. \qquad \square$$

Chapter 4

The decision problem

4.1 Finite model property

Statement of Problem 4.1.2 "Finite model property". Assume that Γ is a complete theory with the finite model property. Is it decidable whether $\varphi \in \Gamma$? $\square$

Solution of Problem 4.1.2 "Finite model property". Yes. By completeness, exactly one of $\varphi, \neg\varphi$ is in Γ, and thus it suffices to run two procedures in parallel, one looking for a finite counterexample to $\Gamma \cup \{\varphi\}$ and one for $\Gamma \cup \{\neg\varphi\}$. $\square$

Statement of Problem 4.1.3 "Small model property for the $\exists^*\forall^*$-fragment". Consider sentences of the form

$$\varphi \;\equiv\; \exists x_1, \ldots, x_m \,.\, \forall y_1, \ldots, y_n \,.\, \psi,$$

where ψ is quantifier-free possibly using equality, without function symbols. Can we bound the size of models of φ? What happens if ψ contains (at least) a single functional symbol? $\square$

Solution of Problem 4.1.3 "Small model property for the $\exists^*\forall^*$-fragment". If φ has a model, then it has a model of size $\leq m$: If the universal quantifiers are satisfied in a model of larger size, then they are trivially satisfied in any smaller structure containing witnesses for the x_i's (c.f. Problem 2.11.4 "Preservation for $\exists^*\forall^*$-sentences").

If ψ contains a single functional symbol f, then we can already express infiniteness of the model in the $\exists^*\forall^*$-fragment (c.f. Problem 2.3.5). ☐

Statement of Problem 4.1.4 "Small model property for monadic logic". Consider a signature consisting only of unary relation symbols without equality $\Sigma = \{P_1, \dots, P_k\}$ (i.e., monadic predicates) and no constants or function symbols. If a sentence φ over Σ is satisfiable, can we find a bound on the size of a finite model thereof? What happens if we allow equality? ☐

Solution of Problem 4.1.4 "Small model property for monadic logic". If φ is satisfiable and does not contain the equality relation, then it has a model of size $\leq 2^k$: Any set of elements satisfying the same set of predicates can be collapsed into a single element, and this operation is model-preserving. If we additionally allow equality and φ has quantifier rank r, then models of size $\leq r \cdot 2^k$ suffice. The latter fact can be shown by demonstrating that Duplicator wins a EF-game with r rounds played between the original model and the compressed model. ☐

4.2 Quantifier elimination

Statement of Problem 4.2.2. Show that a quantifier-elimination procedure needs only eliminate a single existential quantifier in formulas of the form

$$\exists x \,.\, \varphi_1 \wedge \cdots \wedge \varphi_n,$$

where $\varphi_1, \dots, \varphi_n$ are atomic formulas containing x. (In the context of database theory, such formulas are known as *conjunctive queries*.) ☐

Solution of Problem 4.2.2. It suffices to transform the input formula in PNF +NNF, and then eliminate the quantifiers starting from the innermost one. A universal quantifier is transformed into an existential one by double negation, and existential quantifiers are distributed over arbitrary disjunctions, and over conjunctions with formulas not containing x. ☐

Statement of Problem 4.2.3 "Quantifier elimination and completeness". Let Σ be a vocabulary without constant symbols. Show that if a theory Γ over Σ admits elimination of quantifiers, then Γ is complete. $\square$

Solution of Problem 4.2.3 "Quantifier elimination and completeness". Let φ be any sentence over Σ. By performing quantifier elimination we obtain an equivalent variable-free formula, which in a language without constants is either $\top$ or $\bot$. In the first case, $\varphi \in \Gamma$ and in the second case $\varphi \notin \Gamma$, thus showing that Γ is complete. $\square$

4.2.1 Equality

Statement of Problem 4.2.4 "Löwenheim (1915)". Consider the signature consisting of equality only $\Sigma = \{=\}$. Show that the theory of equality $\mathsf{Th}(A, =)$ admits effective elimination of quantifiers. *Hint: Consider separately the cases of A "big enough" vs. "small".* $\square$

Solution of Problem 4.2.4 "Löwenheim (1915)". Thanks to Problem 4.2.2 it suffices to remove an existential quantifier in front of a sequence of equalities and their negations

$$\exists x \,.\, x = y_1 \wedge \cdots \wedge x = y_m \wedge x \neq z_1 \wedge \cdots \wedge x \neq z_n.$$

Trivial equalities $x = x$ are replaced with $\top$, and trivial disequalities $x \neq x$ by $\bot$. We can thus assume no atomic formula is trivial, i.e., no variable y_i, z_j is x. If there exists at least one equality $m \geq 1$, then we replace $x = y_1$ with $\top$ and x by y_1 in all the other equalities and disequalities.

If there is no equality $m = 0$, then the quantifier free formula depends on the cardinality of the model A. If A is infinite or finite and of size $|A| \geq n+1$, then the formula is equivalent to $\top$ since there is always a choice for x satisfying all the disequalities. If A is of finite cardinality $|A| \leq n$, then there is a choice for x provided there are at most $|A| - 1$ distinct z_j's. In other words, the equivalent quantifier free formula is

$$\neg \bigvee \{ \bigwedge_{1 \leq h < k \leq |A|} z_{i_h} \neq z_{i_k} \mid 1 \leq j_1 < \cdots < j_{|A|} \leq n \}. \qquad \square$$

Statement of Problem 4.2.5. Consider the empty signature and sentences using only equality. Let Γ be the set of sentences

$$\{\forall x_1, \dots, x_n \,.\, \exists x_{n+1} \,.\, \bigwedge_{i=1}^{n} \neg x_{n+1} = x_i \mid n \in \mathbb{N}\}.$$

and consider the first-order theory of its logical consequences $\mathsf{Th}(\Gamma) = \{\varphi \mid \Gamma \vDash \varphi\}$.

1. Prove that $\mathsf{Th}(\Gamma)$ is decidable.

2. Prove that $\mathsf{Th}(\Gamma)$ is in PSPACE. □

4.2.2 One unary function

Statement of Problem 4.2.6 "2-cycles". Fix a signature $\Sigma = \{f : 1, = : 2\}$ containing the equality relation and a single unary function. Consider the following sentence:

$$\varphi \equiv \forall x \,.\, f(f(x)) = x \wedge f(x) \neq x.$$

Let $\Gamma = \{\varphi, \varphi_{\geq 1}, \varphi_{\geq 2}, \dots\}$ be the set of axioms including φ and infinitely many axioms ensuring that Γ has only infinite models (c.f. Problem 2.1.6 "Cardinality constraints I"). Is the theory $\mathsf{Th}(\Gamma)$ of the logical consequences of Γ (over the signature Σ) decidable? Is it complete? *Hint: Show that* $\mathsf{Th}(\Gamma)$ *admits effective elimination of quantifiers.* □

Solution of Problem 4.2.6 "2-cycles". The sentence φ says that the domain is a disjoint union of cycles of length 2. Terms in the language of one function symbol f are of the form $f^n(x)$ with x a variable, and thus atomic formulas are of the form $f^m(x) = f^n(y)$ or $f^m(x) \neq f^n(y)$, where in general x and y may be the same variable. By the definition of f, we can always normalise such atomic formulas to be of the form $x = y$ or $x = f(y)$, and similarly for "$\neq$". Thanks to Problem 4.2.2, it suffices to eliminate a single existential quantifier from a formula

$$\exists x \,.\, x = u_1 \wedge \dots \wedge x = u_m \;\wedge\; x \neq v_1 \wedge \dots \wedge x \neq v_n.$$

We can assume w.l.o.g. that the r.h.s. u_i, v_j's do not contain x: $x = x$ and $x \neq f(x)$ can be replaced by $\top$, and $x = f(x)$ and $x \neq x$ by $\bot$. We conclude by the same solution of Problem 4.2.4 "Löwenheim (1915)" which is applicable since Γ has only infinite models by construction. (Alternatively, we can replace all occurrences of $f(y)$ with a fresh variable y' and add the definition $y' = f(y)$, to which we can apply Problem 4.2.4 "Löwenheim (1915)".) Since quantifiers can be eliminated effectively and a quantifier-free formula over the signature Σ is logically equivalent to either $\top$ or $\bot$, the theory is decidable. The theory is complete thanks to Problem 4.2.3 "Quantifier elimination and completeness". □

4.2.3 Dense total order

Statement of Problem 4.2.7 "Langford (1926) [20]". Show that the axiomatic theory of dense total orders without endpoints $\mathsf{Th}(\Delta_{\text{dlo}})$ admits effective elimination of quantifiers, where

$$\begin{aligned} \Delta_{\text{dlo}} = \Delta_{\text{lin}} \cup \{ & \forall x \forall y \,.\, x < y \to \exists z \,.\, x < z \land z < y, && \text{(density)} \\ & \forall x \exists y \,.\, y < x, && \text{(no minimal element)} \\ & \forall x \exists y \,.\, x < y \}. && \text{(no maximal element)} \end{aligned}$$

□

Solution of Problem 4.2.7 "Langford (1926) [20]". By Problem 4.2.2, it suffices to eliminate an existential quantifier of the form

$$\exists x \,.\, x \sim_1 y_1 \land \cdots \land x \sim_1 y_n,$$

where w.l.o.g. $\sim_i \in \{=, <\}$. All trivial equalities of the form $x = x$ are removed. If there is any inequality of the form $x < x$, then the entire formula reduces to $\bot$. Thus, we can assume that no y_i is x. If there exists any equality $x = y_i$, then we can just replace it with $\top$ and replace x with y_i in the remaining atomic formulas (if any). Otherwise, there are only inequalities, which can be split into lower and upper bounds:

$$\exists x \,.\, \underbrace{y_1 < x \land \cdots \land y_m < x}_{\text{lower bounds}} \land \underbrace{x < z_1 \land \cdots \land x < z_n}_{\text{upper bounds}}.$$

The equivalent quantifier-free formula is then

$$\bigwedge_{i=1}^{m} \bigwedge_{j=1}^{n} y_i < z_j.$$

The formula above is $\top$ if either m or n is 0, which is correct since the are no endpoints. □

4.2.4 Discrete total order

Statement of Problem 4.2.8. Consider the theory of the integer numbers with order $\mathsf{Th}(\mathbb{Z}, \leq)$.

1. Does it admit elimination of quantifiers?
2. Consider the extended vocabulary $\mathfrak{A} = (\mathbb{Z}, s, \leq)$, where s is the successor function $s(z) = z+1$. Does $\mathsf{Th}(\mathfrak{A})$ admit elimination of quantifiers?
3. Is $\mathsf{Th}(\mathfrak{A})$ complete? □

Solution of Problem 4.2.8. If the only relation is "$\leq$", then there is no quantifier-free formula equivalent to

$$\varphi_s(x, y) \equiv x < y \wedge \forall z \,.\, x < z \to y \leq z.$$

This is the only obstacle to quantifier elimination: Adding the function symbol s (whose interpretation is provided by φ_s) yields a structure $\mathfrak{A} = (\mathbb{Z}, s, \leq)$ whose theory $\mathsf{Th}(\mathfrak{A})$ admits quantifier elimination. Notice that since the new symbol s can be interpreted in the original theory (by φ_s), $\mathsf{Th}(\mathbb{Z}, \leq) = \mathsf{Th}(\mathbb{Z}, s, \leq)$.

Terms in the language of $\mathfrak{A}$ are of the form $s^i(x)$ where x a variable, and thus atomic formulas can always be written as $s^m(x) \leq s^n(y)$. By abusing notation, we allow terms $s^z(x)$ with $z \in \mathbb{Z}$. Thanks to Problem 4.2.2, it suffices to eliminate a single existential quantifier "$\exists x$" in front of a conjunctive quantifier-free formula. Conjuncts where x appears on both sides of the inequality $s^m(x) \leq s^n(x)$ are replaced by $\top$ if $m \leq n$, and by $\bot$ otherwise. It remains to address conjuncts where x appears only on one side of the inequality. We conclude by splitting the set of inequalities into lower and upper bounds and reasoning as in the solution to Problem 4.2.7 "Langford (1926) [20]". The theory is complete by Problem 4.2.3 "Quantifier elimination and completeness". □

Statement of Problem 4.2.9. Consider the theory of natural numbers with order and successor $\mathsf{Th}(\mathbb{N}, s, \leq)$. Does it admit elimination of quantifiers?

If not, how can one extend the vocabulary in order to ensure that in the extended vocabulary elimination of quantifiers holds? □

Solution of Problem 4.2.9. The least element is definable by the following universal formula, but it cannot be defined by a quantifier-free one:

$$\varphi_0(x) \equiv \forall y \,.\, y \leq x \to y = x.$$

After adding the constant symbol 0 for the least element to the signature we obtain a structure $\mathfrak{A} = (\mathbb{N}, 0, s, \leq)$ whose theory enjoys elimination of quantifiers. □

4.2.5 Rational linear arithmetic

Statement of Problem 4.2.10 "Fourier-Motzkin elimination". Rational arithmetic is the structure $(\mathbb{Q}, \leq, +, (c\,\cdot)_{c\in\mathbb{Q}}, 1)$. Show that the theory of rational arithmetic admits effective elimination of quantifiers, where "+" is the binary sum operator and there is a unary function $\lambda x \,.\, c \cdot x$ for every rational number $c \in \mathbb{Q}$. Is the introduction of all the functions "$(c\,\cdot)$" necessary? □

Solution of Problem 4.2.10 "Fourier-Motzkin elimination". Every atomic formula in the language of rational arithmetic can be written in the form $u \sim v$ with $\sim \in \{=, \leq, <\}$, where u, v are terms obtained as linear combinations of the form

$$c_0 \cdot 1 + c_1 \cdot x_1 + \cdots + c_m \cdot x_n.$$

Enriching the language with unary functions "$(c\,\cdot)$" is necessary to perform quantifier elimination: For instance, if $c = \frac{p}{q}$ would be omitted, then the following formula would not have a quantifier-free equivalent:

$$\exists x \,.\, y = x \wedge p \cdot x = q \cdot 1.$$

In order to perform quantifier elimination, we first transform each atomic formula $u \sim v$ into either one not containing x, or into the "solved form" $x \sim t$. After each atomic formula is solved, we can just replace each maximal term t by a fresh variable y_t, add a new defining equality $y_t = t$, and apply Problem 4.2.7 "Langford (1926) [20]". □

4.2.6 Integral linear arithmetic

Statement of Problem 4.2.11 "Presburger's logic". Consider the theory of natural numbers with addition $\mathsf{Th}(\mathbb{N}, +, =)$. Show that it is decidable via effective elimination of quantifiers. *Hint: Extend the signature with suitable constants and relations.* □

Solution of Problem 4.2.11 "Presburger's logic". The following definable constants and relations need to be introduced because they have no quantifier-free equivalent in the language of "+":

$$\begin{aligned} \varphi_0(x) &\equiv \forall y\,.\, x + y = y, && \text{(zero)} \\ \varphi_\le(x, y) &\equiv \exists z\,.\, y = x + z, && \text{(order)} \\ \varphi_1(x) &\equiv \forall y\,.\, y < x + y \wedge \neg\exists z\,.\, y < z < x + y, && \text{(one)} \\ \varphi_{\mathrm{mod}\,k}(x, y) &\equiv \exists z\,.\, x = y + k \cdot z \vee y = x + k \cdot z, && \text{(modulo)} \end{aligned}$$

where $k \cdot z$ with $k \in \mathbb{N}$ is an abbreviation for $z + \cdots + z$ (k times). We now show quantifier elimination for the theory of the structure in the extended language

$$(\mathbb{N}, +, 0, 1, \le, (\equiv_k)_{k \in \mathbb{N}_{\ge 0}}).$$

Terms in this language can be normalised as affine terms of the form

$$a_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n, \qquad a_0, a_1, \cdots \in \mathbb{N}.$$

By Problem 4.2.2 it suffices to consider formulas of the form $\exists x\,.\, u_1 \sim_1 v_1 \wedge \cdots \wedge u_m \sim_m v_m$, where $\sim_i$ is one of $=, \le, <, \equiv_1, \equiv_2, \ldots$ or a negation thereof. Since $u \neq v$ is equivalent to $u < v \vee v < u$ and $u \not\equiv_k v$ to $u + 1 \equiv_k v \vee \cdots \vee u + k - 1 \equiv_k v$, we can further assume that atomic formulas do not contain negations.

We can assume that all modulo constraints $\equiv_{m_1}, \ldots \equiv_{m_k}$ are over the same modulo: Let $M = \mathrm{lcm}\{m_1, \ldots, m_k\}$ and replace $u \equiv_{m_i} v$ by the equivalent

$$u \equiv_M v + 0 \cdot m_i \;\vee\; u \equiv_M v + 1 \cdot m_i \;\vee\; \cdots \;\vee\; u \equiv_M v + \left(\frac{m}{m_i} - 1\right) \cdot m_i.$$

We can normalise the set of (in)equalities to the partially solved forms

$$a_i \cdot x = u_i, \quad a_i \cdot x \le u_i, \quad u_i \le a_i \cdot x, \quad a_i \cdot x \equiv_M u_i,$$

where each occurrence of x is multiplied by a possibly different coefficient $a_i \in \mathbb{N}$ and the u_i's do not contain x.

Let $a = \mathrm{lcm}\{a_1, \ldots, a_n\}$ be the least common multiplier of the coefficients a_i's of all the occurrences of x. We transform the partially solved forms into the solved forms

$$a \cdot x = u_i, \quad a \cdot x \leq u_i, \quad u_i \leq a \cdot x, \quad a \cdot x \equiv_M u_i,$$

by multiplying each side of $a_i \cdot x \sim_i u_i$ by $\frac{a}{a_i} \in \mathbb{N}$. Now all occurrences of x share the same coefficient $a \cdot x$.

We can ensure that x's coefficient is $a = 1$ by adding an extra modulo constraint $x \equiv_a 0$ and replacing $a \cdot x$ with x in all atomic formulas.

We can ensure that x appears in at most one modulo constraint: If there is more than one modulo constraint $x \equiv_M u_1 \wedge x \equiv_M u_2 \wedge \cdots \wedge x \equiv_M u_m$, then we can replace it with

$$x \equiv_M u_1 \wedge u_1 \equiv_M u_2 \wedge \cdots \wedge u_1 \equiv_M u_m.$$

If there is any equality $x = u_i$, then x can be eliminated by removing this equality and replacing x with u_i throughout in the other atomic formulas. If there is no equality, then we have a system of inequalities and a single modulo constraint of the form

$$\begin{array}{lll} \exists x \,. & u_1 \leq x \wedge \cdots \wedge u_m \leq x \ \wedge & \text{(lower bounds)} \\ & x \leq v_1 \wedge \cdots \wedge x \leq v_n \ \wedge & \text{(upper bounds)} \\ & x \equiv_M t. & \text{(modulo constraint)} \end{array}$$

We can assume w.l.o.g. that there exists at least one lower bound constraint $m \geq 1$ because over the naturals we can always add the constraint $0 \leq x$. The equivalent quantifier-free formula guesses the strongest (largest) lower bound u_i and checks that there exists a witness for x of the form $u_i + 0, \ldots, u_i + M - 1$:

$$\begin{array}{l} \displaystyle\bigvee_{i=1}^{m} \bigvee_{k=0}^{M-1} \quad u_1 \leq u_i + k \wedge \cdots \wedge u_m \leq u_i + k \ \wedge \\ \qquad u_i + k \leq v_1 \wedge \cdots \wedge u_i + k \leq v_n \ \wedge \\ \qquad u_i + k \equiv_M t. \end{array}$$

□

4.3 Interpretations

4.3.1 Real numbers

Statement of Problem 4.3.1. Consider the language of $(\mathbb{R}, +, \cdot, 0, 1, \leq)$, and let

$$p(x) = a + b \cdot x + c \cdot x^2$$

be a second-degree polynomial, where x, a, b, c are its free variables. Find quantifier-free equivalents for the following formulas

$$\begin{aligned}
\varphi_1 &\equiv \exists x \,.\, p(x) = 0, \\
\varphi_2 &\equiv \forall x \,.\, p(x) = 0, \\
\varphi_3 &\equiv \exists x_1, x_2 \,.\, x_1 \neq x_2 \wedge p(x_1) = 0 \wedge p(x_2) = 0, \\
\varphi_4 &\equiv \forall (x \leq y \leq z) \,.\, p(y) > 0.
\end{aligned}$$

□

Statement of Problem 4.3.3 "First-order theory of the complex numbers". Is the first-order theory of the complex numbers $\mathsf{Th}(\mathbb{C}, +, \cdot, 0, 1)$ decidable? *Hint: Interpret the complex numbers in the real numbers.* □

Solution of Problem 4.3.3 "First-order theory of the complex numbers". The first-order theory of the complex numbers is decidable, and this can be proved by a two-dimensional interpretation in the real numbers. A complex number $a + ib \in \mathbb{C}$ is interpreted as the pair $(a, b) \in \mathbb{R} \times \mathbb{R}$. A formula φ in the language of $\mathbb{C}$ is converted into a formula $[\varphi]$ in the language of $(\mathbb{R}, +, \cdot, 0, 1)$ by replacing every variable x into two copies x^0, x^1 thereof corresponding to its real, resp., imaginary part. Formally, we define two translation functions $[\_]^0, [\_]^1$ on terms

$$\begin{aligned}
[x]^i &= x^i, & i \in \{0, 1\}, \\
[u + v]^i &= [u]^i + [v]^i, & i \in \{0, 1\}, \\
[u \cdot v]^0 &= [u]^0 \cdot [v]^0 - [u]^1 \cdot [v]^1, \\
[u \cdot v]^1 &= [u]^0 \cdot [v]^1 + [u]^1 \cdot [v]^0,
\end{aligned}$$

and a translation function [_] on formulas

$$
\begin{aligned}
[u = v] &\equiv [u]^0 = [v]^0 \wedge [u]^1 = [v]^1, \\
[\varphi \wedge \psi] &\equiv [\varphi] \wedge [\psi], \\
[\neg\varphi] &\equiv \neg[\varphi], \\
[\exists x \,.\, \varphi] &\equiv \exists x^0, x^1 \,.\, [\varphi].
\end{aligned}
$$

Given a sentence φ over $\mathbb{C}$, we convert it into $[\varphi]$ over $\mathbb{R}$, apply quantifier elimination by Theorem 4.3.2 "Tarski–Seidenberg", and and check by direct inspection whether the resulting variable-free formula is a tautology or not. □

Statement of Problem 4.3.4 "First-order theory of planar Euclidean geometry". Consider planar Euclidean geometry (P, B, C) where P is the set of points of the plane, the *betweenness* relation $B \subseteq P^3$ contains triples of points (a, b, c) on the same line s.t. b is between a and c, and the *congruence* relation $C \subseteq P^4$ contains four-tuples of points (a, b, c, d) s.t. the line segment ab has the same length as cd. Show that (P, B, C) is complete and decidable. *Hint: Interpret euclidean geometry in the real numbers.* □

Solution of Problem 4.3.4 "First-order theory of planar Euclidean geometry". We interpret P as $\mathbb{R} \times \mathbb{R}$ by encoding a point p with its Cartesian coordinates (p_x, p_y). Then, B, C can be encoded as suitable first-order formulas over the reals:

$$
\begin{aligned}
\varphi_B(p, q, r) &\equiv p_x = q_x = r_x \wedge p_y \le q_y \le r_y \;\vee \\
&\quad\; \exists a, b \,.\, p_y = a \cdot p_x + b \;\wedge \\
&\quad\; q_y = a \cdot q_x + b \;\wedge \\
&\quad\; r_y = a \cdot r_x + b \;\wedge \\
&\quad\; p_x \le q_x \le r_x, \\
\varphi_C(p, q, r, s) &\equiv (p_x - q_x)^2 + (p_y - q_y)^2 = (r_x - s_x)^2 + (r_y - s_y)^2.
\end{aligned}
$$

□

4.4 Model-checking on finite structures

Statement of Problem 4.4.1 "First-order logic model-checking". Consider the following decision problem.

First-order logic model-checking problem.
Input: A first-order logic sentence φ and a finite structure $\mathfrak{A}$.
Output: YES if, and only if, $\mathfrak{A} \models \varphi$.

What is its computational complexity? What happens if we bound the width of the input formulas (maximal number of free variables in every subformula)? □

Solution of Problem 4.4.1 "First-order logic model-checking". The first-order logic model-checking problem is PSPACE-complete. The upper bound can be shown by designing two player game of polynomial length, which can be solved in APTIME = PSPACE [6]. Let $\varphi, \mathfrak{A}$ be the input formula and structure; thanks to Problem 2.2.1 "Negation normal form" we assume that φ is in NNF, and thus negations only appear in front of atomic formulas. Positions in the game are of the form (ψ, ϱ), where ψ is a subformula of φ and ϱ is a variable valuation. The game proceeds as to mimic the semantics of the formula:

1. If $\psi \equiv \top$, then Player I wins immediately.
2. If $\psi \equiv \bot$, then Player II wins immediately.
3. If $\psi \equiv R_j(t_1, \dots, t_n)$, then Player I wins if
$$([\![t_1]\!]^{\mathfrak{A}}_{\varrho}, \dots, [\![t_{k_j}]\!]^{\mathfrak{A}}_{\varrho}) \in R^{\mathfrak{A}}_j,$$
and Player II wins otherwise.
4. The condition for $\psi \equiv \neg R_j(t_1, \dots, t_n)$ is similar.
5. If $\psi \equiv \psi_1 \wedge \psi_2$, then Player II chooses a conjunct ψ_i and the game goes to position (ψ_i, ϱ).
6. If $\psi \equiv \psi_1 \vee \psi_2$, then Player I chooses a conjunct ψ_i and the game goes to position (ψ_i, ϱ).
7. If $\psi \equiv \forall x \, . \, \psi'$, then Player II chooses an element of the domain $a \in A$ and the game goes to position $(\psi', \varrho[x \mapsto a])$.
8. If $\psi \equiv \exists x \, . \, \psi'$, then Player I chooses an element of the domain $a \in A$ and the game goes to position $(\psi', \varrho[x \mapsto a])$.

Hardness for PSPACE can be shown by reducing from QBF, which is PSPACE-hard [24]. In order to solve the satisfiability problem for a QBF formula

$$\varphi \equiv \exists X_1 \forall Y_1 \cdots \exists X_n \forall Y_n \psi$$

with φ propositional, we consider evaluation in the the fixed model $\mathfrak{B} = (\mathbb{B}, \wedge^{\mathfrak{B}}, \vee^{\mathfrak{B}}, \neg^{\mathfrak{B}})$, where $\mathbb{B} = \{\top, \bot\}$ and the semantics of the Boolean connectives $\wedge^{\mathfrak{B}}, \vee^{\mathfrak{B}}, \neg^{\mathfrak{B}}$ is given by the respective truth tables.

If the width is bounded, then the problem becomes PTIME-complete. □

Statement of Problem 4.4.2 "SO model-checking". What is the computational complexity of the following decision problem?

SO MODEL-CHECKING PROBLEM.
Input: A SO sentence φ and a finite structure $\mathfrak{A}$.
Output: YES if, and only if, $\mathfrak{A} \models \varphi$. □

Solution of Problem 4.4.2 "SO model-checking". For every fixed arity k, the problem is PSPACE-complete, like in the first-order case. The upper bound follows from the fact that, once we have fixed a structure $\mathfrak{A}$ with n elements, we can simulate second-order quantification $\exists R$, where R is a k-ary relation, by $n^k \cdot k$ first-order quantifications

$$\exists x^R_{1,1}, \cdots, x^R_{1,k}, \cdots, x^R_{n^k,k}.$$

Atomic formulas of the form $R(t_1, \ldots, t_k)$ are then replaced by a finite disjunction

$$\bigvee_{i=1}^{n^k} t_1 = x^R_{i,1} \wedge \cdots \wedge t_k = x^R_{i,k}.$$

When k is fixed, we get a polynomially larger formula which is equivalent to the original one w.r.t. the model-checking problem, and we can thus apply Problem 4.4.1 "First-order logic model-checking" in order to obtain a PSPACE upper bound.

When k is part of the input, the argument above gives an EXPSPACE bound. We leave it open whether there exists a corresponding lower-bound. □

Chapter 5

Arithmetic

5.1 Numbers

Statement of Problem 5.1.1. Show that there exists a predicate $\beta \subseteq \mathbb{N}^4$ definable in arithmetic s.t. for every sequence of natural numbers $a_1, \dots, a_k \in \mathbb{N}$ there are numbers $a, b \in \mathbb{N}$ s.t. for every index $1 \le i \le k$ and any $x \in \mathbb{N}$,

$$\beta(a, b, i, x) \qquad \text{if, and only if,} \qquad a_i = x. \tag{β}$$

□

Solution of Problem 5.1.1. Consider the following definition for β:

$$\beta = \{(a, b, i, x) \mid x = a \bmod (1 + (1 + i) \cdot b)\}.$$

The modulo operation above is definable in arithmetic (and thus β) by the following existential formula:

$$\varphi_{\text{mod}}(x, y, z) \;\equiv\; x \le z \wedge \exists k \,.\, x = y - k \cdot z.$$

Then, $a = b \bmod c$ iff $\mathbb{N}, x : a, y : b, z : c \vDash \varphi_{\text{mod}}$. Establishing that β encodes sequences of numbers in the sense (β) follows from elementary arithmetical facts. □

Statement of Problem 5.1.2 "Simplified function χ". From the definition of β it is clear that a sequence of natural numbers is encoded as a *pair* of numbers $a, b \in \mathbb{N}$. Is it possible to encode it as a *single* natural number $p \in \mathbb{N}$? □

Solution of Problem 5.1.2 “Simplified function χ”. Let $\varphi(p,a,b)$ be any predicate encoding a objective pairing function $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Then, let

$$\chi(p,i,x) \;\equiv\; \forall a,b\,.\,\varphi(p,a,b) \to \beta(a,b,i,x). \qquad \square$$

Statement of Problem 5.1.3. Express the following functions and predicates in arithmetic:

1. The divisibility predicate $m\,|\,n$.
2. The predicate $\mathrm{prime}(n)$ which is true iff n is a prime number.
3. The binary predicate saying that m, n are relatively prime.
4. The least common multiplier function $\mathrm{lcm}(m,n)$.
5. The binary predicate saying that m is the largest power of a prime that divides n. $\square$

Solution of Problem 5.1.3. The divisibility predicate $m\,|\,n$ is expressed directly as $\exists x\,.\,n = x\cdot m$, which allows us to express $\mathrm{prime}(n)$ as

$$\forall x\,.\,x\,|\,n \to x = 1 \lor x = n,$$

and the fact that m, n are relatively prime as

$$\forall x\,.\,x\,|\,m \land x\,|\,n \to x = 1.$$

The function $\mathrm{lcm}(m,n)$ is expressed by the following ternary predicate (and similarly for the last point)

$$\varphi(m,n,x) \;\equiv\; \underbrace{m\,|\,x \land n\,|\,x}_{\text{common multiplier}} \;\land\; \underbrace{\forall y\,.\,m\,|\,y \land n\,|\,y \to x \le y}_{\text{minimality}}. \qquad \square$$

Statement of Problem 5.1.4. Express the following functions and predicates in arithmetic:

1. The exponential function 2^n.
2. The factorial function $n!$.

3. The Fibonacci function:

$$f(0) = 0, \quad f(1) = 1, \quad f(n+2) = f(n+1) + f(n), n \geq 0.$$

4. The inverse of the exponential function $\lfloor \log n \rfloor$.

5. The unary predicate saying that n is a *perfect number*, i.e., it is the sum of its divisors, except itself. □

Solution of Problem 5.1.4. The idea is the same in every case. We demonstrate it with 2^n, which is encoded as the existence of a sequence of $n+1$ numbers $2^0, 2^1, \ldots, 2^n$ starting at 1 and where the next number is obtained by doubling the previous one:

$$\varphi(n,x) \equiv \underbrace{\exists p\,.}_{\text{there is a sequence encoded by } p} \underbrace{\chi(p,0,2^0)}_{\text{the first element is } 2^0} \wedge \underbrace{\chi(p,n,x)}_{\text{the } n\text{-th element is } x} \wedge \underbrace{\forall i,y\,.\,\xi(p,i,y) \to \chi(p,i+1,2\cdot y)}_{\text{every element is twice its predecessor}}\,.$$

If $\varphi(n,x)$ encodes $x = 2^n$, then its inverse function $y = \lfloor \log n \rfloor$ is easily expressed as

$$\varphi^{-1}(n,y) \equiv \exists x\,.\,n-1 < x \leq n \wedge \varphi(y,x).$$

We can express that n is a perfect number by listing its divisors and computing their sum:

$$\underbrace{\exists p,k\,.\,\forall(i\le k),x\,.\,\chi(p,i,x)\to x\,|\,n}_{p\text{ encodes a list of divisors of }n}\ \wedge$$
$$\underbrace{\chi(p,0,1)}_{\text{the first divisor is 1}}\quad\wedge\quad\underbrace{\chi(p,k,n)}_{\text{the last divisor is }n}\quad\wedge$$
$$\underbrace{\forall(i<j\le k)\,.\,\forall x,y\,.\,\chi(p,i,x)\wedge\chi(p,j,y)\to x<y}_{\text{divisors are totally ordered}}\ \wedge$$
$$\underbrace{\exists q\,.}_{q\text{ encodes partial sums of divisors}}\quad\underbrace{\chi(q,0,0)}_{\text{start at 0}}\ \wedge\ \underbrace{\chi(q,k,n)}_{\text{end at }n}\ \wedge$$
$$\underbrace{\forall(i<k)\,.\,\forall x,y\,.\,\chi(q,i,x)\wedge\chi(p,i,y)\to\chi(q,i+1,x+y)}_{\text{each next element is the sum of the previous one and the corresponding divisor}}.$$
□

Statement of Problem 5.1.5 "Collatz problem". Write a sentence $\varphi_{\mathrm{Collatz}}$ expressing that the following sequence always reaches value 1, for every starting value a_0:

$$a_{n+1}=\begin{cases}\frac{a_n}{2} & \text{if } n \text{ is even,}\\ 3\cdot n+1 & \text{otherwise.}\end{cases}$$

Whether $\varphi_{\mathrm{Collatz}}$ is true in arithmetic is a long-standing open problem in number theory. □

Solution of Problem 5.1.5 "Collatz problem". The Collatz sequence can be expressed by the same technique as in Problem 5.1.4 as the arithmetical predicate $\psi_{\mathrm{Collatz}}(a_0,n,x)$ s.t. when starting at a_0 the n-th element a_n is x. The Collatz conjecture is expressed by the sentence

$$\varphi_{\mathrm{Collatz}}\ \equiv\ \forall a_0\exists n\,.\,\psi_{\mathrm{Collatz}}(a_0,n,1).$$
□

Statement of Problem 5.1.6. Consider arithmetic $\mathfrak{A}=(\mathbb{N},+,\cdot,f)$ extended with an uninterpreted function symbol f. Write a sentence φ expressing the fact that f is a univariate polynomial with coefficients from $\mathbb{N}$. □

Solution of Problem 5.1.6. A univariate polynomial with natural coefficients of degree n is of the form

$$a_0 \cdot x^0 + a_1 \cdot x^1 + \cdots + a_n \cdot x^n.$$

The formula φ guesses the sequence of coefficients and checks that $f(x)$ equals the polynomial above. Evaluating the polynomial on input x can be done by guessing another sequence computing partial sums. □

Statement of Problem 5.1.7 "Counting solutions". For a given formula $\varphi(x)$ in the language of first-order arithmetic of one free variable x construct a formula $\#\varphi(y)$ s.t., for every $n \in \mathbb{N}$,

$$\mathbb{N}, y : n \models \#\varphi(y) \quad \text{if, and only if,} \quad |\{m \in \mathbb{N} \mid \mathbb{N}, x : m \models \varphi(x)\}| = n. \qquad \square$$

Solution of Problem 5.1.7 "Counting solutions". The formula $\#\varphi(y)$ guesses a sequence $n_0, \ldots, n_{y-1} \in \mathbb{N}$ of y distinct natural numbers s.t. each n_i is a solution of φ and there is no other solution:

$$\begin{aligned}\#\varphi(y) \;\equiv\; \exists p \,.\, & \forall (i < j < y) \,.\, \forall x, z \,.\, \chi(p, i, x) \wedge \chi(p, j, z) \to x \neq z \;\wedge \\ & \forall (i < y) \,.\, \forall x \,.\, \chi(p, i, x) \to \varphi(x) \;\wedge \\ & \forall x \,.\, \varphi(x) \to \exists (i < y) \,.\, \chi(p, i, x).\end{aligned} \qquad \square$$

5.2 Automata and formal languages

Statement of Problem 5.2.1. Show that every regular language $L \subseteq \Sigma^*$ can be recognised by a formula of arithmetic φ_L. □

Solution of Problem 5.2.1. Let $A = (Q, \Sigma, I, F, \Delta)$ be a nondeterministic finite automaton recognising $L(A) = L$, where $Q = \{0, \ldots, n\}$ if a finite set of states, of which $I, F \subseteq Q$ are the initial, resp., finite ones, and Δ is a finite set of transitions of the from $p \xrightarrow{a} q$ with $p, q \in Q$ and $a \in \Sigma$.

First of all, we write two formulas $\varphi_i(x, y)$, $i \in \{0, 1\}$, with two free variables x, y expressing that the y-th least significant digit in the binary encoding of x is i. Then we can write a formula $\varphi_{\text{enc}}(a, n, x)$ expressing that a is the encoding of the sequence $w \in \Sigma^n$ s.t. $x = [w]_2$.

We construct a formula $\varphi_L(x)$ which guesses an accepting computation over the word w encoding $x = [w]_2$:

$$\exists a, n, p \,.\, \underbrace{\varphi_{\mathrm{enc}}(a, n, x)}_{\text{input}} \wedge \underbrace{\bigvee_{p_0 \in I} \chi(p, 0, p_0)}_{\text{initial state}} \wedge \underbrace{\bigvee_{p_n \in F} \chi(p, n, p_n)}_{\text{final state}} \wedge$$

$$\forall (i < n) \,.\, \bigvee_{p_i \xrightarrow{a_i} p_{i+1}} \underbrace{\chi(a, i, a_i) \wedge \chi(p, i, p_i) \wedge \chi(p, i+1, p_{i+1})}_{i\text{-th transition}} \,. \qquad \square$$

Statement of Problem 5.2.2. Show that a context-free language $L \subseteq \Sigma^*$ can be recognised by a formula of arithmetic φ_L $\square$

Solution of Problem 5.2.2. Let $A = (P, \Sigma, \Gamma, I, F, \Delta)$ be a nondeterministic pushdown automaton (PDA) recognising the context-free language $L(P) = L$, where $P = \{0, \ldots, n\}$ is a finite set of control locations, Γ is a finite stack alphabet, $I, F \subseteq P$ are the initial, resp., final control locations, and Δ is a set of transitions of the form $p \xrightarrow{a, \mathsf{op}} q$ where $p, q \in Q$, $a \in \Sigma$, and op is a stack operation in

$$\{\mathsf{nop}\} \cup \{\mathsf{push}(\gamma), \mathsf{pop}(\gamma) \mid \gamma \in \Gamma\}.$$

A *configuration* of a PDA is a pair (p, γ), where $p \in Q$ is a control location and $\gamma = b_0 \cdots b_m \in \Gamma^*$ is the content of the stack. We can assume w.l.o.g. that $\Gamma = \{0, 1\}$ and consequently the stack contents γ can be encoded as the integer $[\gamma]_2$. In order to guarantee a unique encoding, we assume that the stack contains always a bottom symbol 1 which cannot be popped. Under this encoding, pushing 0 on the stack corresponds to multiplying by 2, pushing 1 corresponds to multiplying by 2 and adding 1, popping 0 corresponds to check that $[\gamma]_2$ is even followed by integral division by 2, and similarly popping 1 corresponds to check that $[\gamma]_2$ is odd followed by integral division by 2. All those operations can be represented by simple arithmetic formulas, and thus we assume that we have a formula $\varphi_{\mathsf{op}}(\gamma, \gamma')$ checking that the stack encoded by γ' can be obtained by applying op to the stack encoded by γ.

The required formula φ_L can now be constructed as in Problem 5.2.1 with the additional introduction of the stack contents:

$$\exists a, n, p, \gamma \,.\, \underbrace{\varphi_{\text{enc}}(a, n, x)}_{\text{input}} \wedge \underbrace{\bigvee_{p_0 \in I} \chi(p, 0, p_0)}_{\text{initial location}} \wedge \underbrace{\chi(\gamma, 0, 1)}_{\text{initial stack}} \wedge \underbrace{\bigvee_{p_n \in F} \chi(p, n, p_n)}_{\text{final location}} \wedge$$
$$\forall (i < n) \,.\, \bigvee_{p_i \xrightarrow{a_i, \mathsf{op}_i} p_{i+1}} \underbrace{\chi(a, i, a_i) \wedge \chi(p, i, p_i) \wedge \chi(p, i+1, p_{i+1})}_{i\text{-th transition}} \wedge$$
$$\underbrace{\forall \gamma_i, \gamma_{i+1} \,.\, \chi(\gamma, i, \gamma_i) \wedge \chi(\gamma, i+1, \gamma_{i+1}) \to \varphi_{\mathsf{op}_i}(\gamma_i, \gamma_{i+1})}_{\text{stack}} \,. \qquad \square$$

Statement of Problem 5.2.3. Show that for any recursively-enumerable language $L \subseteq \Sigma^*$ there is a formula of arithmetic φ_L recognising it. □

Solution of Problem 5.2.3. We can model the tape of a Turing machine with two stacks. It then suffices to encode them separately and apply a construction similar to the one in Problem 5.2.2. □

Statement of Problem 5.2.3. □

Statement of Problem 5.2.4. Prove that the decision problem for arithmetic is undecidable. □

Solution of Problem 5.2.4. We reduce from the halting problem of Turing machines. From Problem 5.2.3, for any recursively enumerable language L, we can construct a formula $\varphi_L(x)$ with one free variable x recognising it, and thus the following sentence can express whether L is nonempty:

$$\exists x \,.\, \varphi_L(x).$$

An analysis of the formulas involved in the construction of φ_L shows that the sentence above is of the form $\exists^* \forall^*$. (The celebrated theorem of Davis-Matiyasevich-Putnam-Robinson shows that the $\exists^*$ fragment of arithmetic, corresponding to solvability of *Diophantine equations*, i.e., polynomial equations over the integers, is already undecidable.) □

Statement of Problem 5.2.5 "Modular arithmetic". Let $\Sigma = \{R, =\}$ be a signature containing a binary relation R and equality. Provide an axiomatisation of addition and multiplication over the signature Σ admitting finite models. □

Solution of Problem 5.2.5 "Modular arithmetic". First of all, we axiomatise that R is a strict discrete total order with least and greatest elements, denoted $<$ in the following, with a sentence $\varphi_<$. Zero is axiomatised as the least element in the order, and -1 as the greatest one:

$$\begin{aligned}\varphi_0(x) &\equiv \forall y \,.\, x \leq y,\\ \varphi_{-1}(x) &\equiv \forall y \,.\, x \geq y.\end{aligned}$$

The successor function maps -1 back to 0:

$$\varphi_s(x,y) \equiv (\neg\varphi_{-1}(x) \wedge x < y \wedge \forall z \,.\, x < z \rightarrow y \leq z) \vee \varphi_{-1}(x) \wedge \varphi_0(y).$$

Every element in the order is reachable by taking successors and predecessors:

$$\forall x, y \,.\, x < y \leftrightarrow s(x) \leq y \wedge x \leq s^{-1}(y).$$

Finally, we can axiomatise addition (and similarly multiplication):

$$\begin{aligned}\varphi_+(x,y,z) \equiv\ & y = 0 \rightarrow z = x \ \wedge\\ & \forall y' \,.\, y = s(y') \rightarrow \varphi_+(x,y',z') \wedge z = s(z').\end{aligned}$$

(Note that there is no induction axiom schema, and thus some usual property of "+" such as associativity cannot be proved in this axiomatisation.) Modular arithmetic $(\{0, \dots, n-1\}, +_n, \cdot_n)$ is a finite model of these axioms, where $x +_n y$ is interpreted as $(x + y) \bmod n$, and similarly for $\cdot_n$. □

Statement of Problem 5.2.6 "Trakhtrenbrot's theorem". Show that the finite validity problem of first-order logic over a signature containing at least one non-unary relation (i.e., not monadic) is undecidable. What about the finite satisfiability problem? □

Solution of Problem 5.2.6 "Trakhtrenbrot's theorem". We have seen in Problem 5.2.5 "Modular arithmetic" that one binary relation is enough to axiomatise modular arithmetic. The sentence φ_M encoding acceptance of a

Turing machine M (cf. Problem 5.2.3) is in the $\exists^*\forall^*$-fragment, and thus by Problem 4.1.3 "Small model property for the $\exists^*\forall^*$-fragment" it has the finite model property: M halts iff φ_M has a finite model, thus showing that finite satisfiability is undecidable. Since finite satisfiability is recursively enumerable (we can just guess a finite model and check its validity), it follows that finite validity is undecidable too. □

Statement of Problem 5.2.7. Is the first-order theory of the structure $\mathsf{Th}(\mathbb{Z}, +, \cdot)$ decidable? *Hint: Show that ≤ is definable by appealing to Lagrange's four square theorem.* □

Solution of Problem 5.2.7. Arithmetic over the integers is undecidable, since we can express ≤, which allows to encode $\mathbb{N}$ in $\mathbb{Z}$:

$$\varphi_{\leq}(x, y) \equiv \exists a, b, c, d \,.\, y = x + a^2 + b^2 + c^2 + d^2. \qquad \square$$

5.3 Miscellanea

Statement of Problem 5.3.1. Recall the definition of finitely generated monoids $\mathfrak{M} = (M, \circ, e)$ from Problem 2.9.11 "Finitely generated monoids are not axiomatisable". We can encode a monoid $\mathfrak{M}$ by arithmetic formulas $\mu(x), \nu(x, y, z), \epsilon(x)$ whenever

$$\begin{aligned} M &= \{a \in \mathbb{N} \mid \mathbb{N}, x : a \models \mu\}, \\ \circ &= \{(a, b, c) \in \mathbb{N}^3 \mid \mathbb{N}, x : a, y : b, z : c \models \nu\}, \text{and} \\ \{e\} &= \{a \in \mathbb{N} \mid \mathbb{N}, x : a \models \epsilon\}. \end{aligned}$$

Write an arithmetic sentence $\gamma_{\mathfrak{M}}$ which may use μ, ν, ϵ encoding that $\mathfrak{M}$ is finitely generated. □

Solution of Problem 5.3.1. The idea is as in Problem 5.1.4: We write a formula that guesses a set of generators and checks that every element of the monoid is a product of generators. □

Statement of Problem 5.3.2 "Second-order quantifier elimination". Weak monadic second-order logic (WMSO) has the same syntax as MSO. Semantically, the second-order quantifier $\exists X$ means that *there exists a finite subset of the universe* X, and dually for $\forall X$. Prove that for any WMSO formula

φ over the signature of arithmetic without free variables of second-order there is a equivalent formula ψ of first-order logic. $\square$

Solution of Problem 5.3.2 "Second-order quantifier elimination". We encode sets of elements by sequences: A second-order quantifier $\exists X$ is replaced by $\exists p_X \exists m_X$, where p_X encodes the sequence of the elements of X and m_X its length. An atomic formula $x \in X$ within the range of this quantifier is replaced by $\exists i \,.\, i < m_X \wedge \chi(p_X, i, x)$. $\square$

Bibliography

[1] Miklos Ajtai and Ronald Fagin. Reachability is harder for directed than for undirected finite graphs. *The Journal of Symbolic Logic*, 55(1):113–150, 1990. URL: http://www.jstor.org/stable/2274958.

[2] Sanjeev Arora and Boaz Barak. *Computational Complexity - A Modern Approach*. Cambridge University Press, 2009.

[3] Günter Asser. Das Repräsentenproblem in Prädikatenkalkül der ersten Stufe mit Identität. In *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, volume 1, pages 252—263, 1955.

[4] E. W. Beth. On Padoa's Method in the Theory of Definition. *Journal of Symbolic Logic*, 21(2):194–195, 1956. doi:10.2307/2268764.

[5] Richard Büchi. Weak second-order arithmetic and finite automata. *Z. Math. Logik und grundl. Math.*, 6:66–92, 1960.

[6] Ashok K. Chandra, Dexter C. Kozen, and Larry J. Stockmeyer. Alternation. *J. ACM*, 28(1):114–133, January 1981. URL: http://doi.acm.org/10.1145/322234.322243, doi:10.1145/322234.322243.

[7] E. F. Codd. A relational model of data for large shared data banks. *Commun. ACM*, 13(6):377–387, June 1970. URL: http://doi.acm.org/10.1145/362384.362685, doi:10.1145/362384.362685.

[8] Stephen A. Cook. A taxonomy of problems with fast parallel algorithms. *Inf. Control*, 64(1-3):2–22, March 1985. URL: http://dx.doi.org/10.1016/S0019-9958(85)80041-3, doi:10.1016/S0019-9958(85)80041-3.

[9] Arnaud Durand, Ronald Fagin, and Bernd Loescher. Spectra with only unary function symbols. In Mogens Nielsen and Wolfgang Thomas, editors, *Computer Science Logic*, pages 189–202, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[10] Arnaud Durand, Neil D. Jones, Johann A. Makowsky, and Malika More. Fifty years of the spectrum problem: survey and new results. *The Bulletin of Symbolic Logic*, 18(4):505—553, 2012. doi:10.2178/bsl.1804020.

[11] Calvin C. Elgot. Decision problems of finite automata design and related arithmetics. *Transactions of the American Mathematical Society*, 98(1):21–51, 1961. URL: http://www.jstor.org/stable/1993511.

[12] Ronald Fagin. *Contributions to the model theory of finite structures*. PhD thesis, University of California, Berkeley, 1973.

[13] Ronald Fagin. Generalized first-order spectra and polynomial-time recognizable sets. *Complexity of Computation*, 7:43–73, 1974.

[14] Ronald Fagin. Monadic generalized spectra. *Mathematical Logic Quarterly*, 21(1):89–96, 1975. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/malq.19750210112, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/malq.19750210112, doi:10.1002/malq.19750210112.

[15] Armin Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985. Third Conference on Foundations of Software Technology and Theoretical Computer Science. URL: http://www.sciencedirect.com/science/article/pii/0304397585901446, doi:https://doi.org/10.1016/0304-3975(85)90144-6.

[16] N. Immerman. Nondeterministic space is closed under complementation. *SIAM Journal on Computing*, 17(5):935–938, 1988. URL: http://epubs.siam.org/doi/abs/10.1137/0217058, arXiv:http://epubs.siam.org/doi/pdf/10.1137/0217058, doi:10.1137/0217058.

[17] Neil D. Jones and Alan L. Selman. Turing machines and the spectra of first-order formulas. *The Journal of Symbolic Logic*, 39(1):139–150, 1974. URL: http://www.jstor.org/stable/2272354.

[18] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997. URL: http://www.jstor.org/stable/2275541.

[19] Saul A. Kripke. Semantical analysis of intuitionistic logic i. In J.N. Crossley and M.A.E. Dummett, editors, *Formal Systems and Recursive Functions*, volume 40 of *Studies in Logic and the Foundations of Mathematics*, pages 92 – 130. Elsevier, 1965. URL: http://www.sciencedirect.com/science/article/pii/S0049237X08716859, doi:https://doi.org/10.1016/S0049-237X(08)71685-9.

[20] C. H. Langford. Some theorems on deducibility. *Annals of Mathematics*, 28(1/4):16–40, 1926. URL: http://www.jstor.org/stable/1968352.

[21] K. L. McMillan. Interpolation and sat-based model checking. In Warren A. Hunt and Fabio Somenzi, editors, *Computer Aided Verification*, pages 1–13, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[22] Albert Meyer. Weak monadic second order theory of succesor is not elementary-recursive. Technical report, MIT - Project MAC Technical Memorandum 38, 1973.

[23] Daniele Mundici. A lower bound for the complexity of Craig's interpolants in sentential logic. *Archiv für mathematische Logik und Grundlagenforschung*, 23(1):27–36, Dec 1983. doi:10.1007/BF02023010.

[24] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[25] Elena Pezzoli. Computational complexity of Ehrenfeucht-Fraïssé games on finite structures. In Georg Gottlob, Etienne Grandjean, and Katrin Seyr, editors, *Proc. of CSL'99*, pages 159–170, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[26] Pavel Pudlak. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symbolic Logic*, 62(3):981–998, 09 1997. URL: https://projecteuclid.org:443/euclid.jsl/1183745308.

[27] Dana Scott and Patrick Suppes. Foundational aspects of theories of measurement. *The Journal of Symbolic Logic*, 23(2):113–128, 1958. URL: http://www.jstor.org/stable/2964389.

[28] Michael Sipser. *Introduction to the Theory of Computation*. Thomson South-Western, 3 edition, 2012. URL: http://gen.lib.rus.ec/book/index.php?md5=83b32c22675567f3e22c93bd6bd372be.

[29] Larry J. Stockmeyer. *The complexity of decision problems in automata theory and logic*. PhD thesis, 1974.

[30] Róbert Szelepcsényi. The method of forced enumeration for nondeterministic automata. *Acta Informatica*, 26(3):279–284, Nov 1988. doi:10.1007/BF00299636.

[31] W. W. Tait. A counterexample to a conjecture of scott and suppes. *Journal of Symbolic Logic*, 24(1):15–16, 1959. doi:10.2307/2964569.

[32] B. A. Trakhtenbrot. Finite automata and the logic of one-place predicates. *Siberian Math. J.*, 1962.

[33] G. S. Tseitin. *On the Complexity of Derivation in Propositional Calculus*, pages 466–483. Springer Berlin Heidelberg, Berlin, Heidelberg, 1983. doi:10.1007/978-3-642-81955-1_28.