Exercises for Mathematical Logic (Fall 2024/25)

We have seen in the lecture that the De Morgan language $\{\wedge, \vee, \neg, \top, \bot\}$ is functionally complete, and specifically, that every Boolean function can be represented by a CNF or DNF of size $O(2^n n)$.

1. Prove that $\{\vee, \neg\}$, $\{\to, \bot\}$, and $\{\uparrow\}$ are functionally complete, where $x \uparrow y$ denotes the Sheffer stroke $\neg(x \wedge y)$.

2. Prove that $\{\to\}$, $\{\wedge, \vee, \top, \bot\}$, and $\{\leftrightarrow, \top, \bot\}$ are not functionally complete.
[Hint: Find a nontrivial property of Boolean functions which is preserved by composition, and holds for functions in the given basis.]

3. For any Boolean function $f\colon \{0,1\}^n \to \{0,1\}$, the following are equivalent:

(i) $\{f\}$ is functionally complete.

(ii) $f(0,\dots,0) = 1$, $f(1,\dots,1) = 0$, and there exists an assignment $\langle e_0,\dots,e_{n-1}\rangle \in \{0,1\}^n$ such that $f(e_0,\dots,e_{n-1}) = f(\neg e_0,\dots,\neg e_{n-1})$.

[Hint: For (ii) $\to$ (i), look at functions obtained from f by identifying some of the variables.]

4. For any $n \in \mathbb{N}$, the *parity* function $\bigoplus_{i<n} x_i \colon \{0,1\}^n \to \{0,1\}$ is defined as $\left(\sum_{i<n} x_i\right) \bmod 2$. Show that any DNF or CNF representing $\bigoplus_{i<n} x_i$ has size $\Omega(2^n n)$. [Hint: What terms of the form $\bigwedge_{i\in I} x_i^{e_i}$ can imply one of $\bigoplus_{i<n} x_i = 0$ or $\bigoplus_{i<n} x_i = 1$? Here, $I \subseteq [n]$, $e_i \in \{0,1\}$, $x^1 = x$, $x^0 = \neg x$.]

5. There are formulas representing $\bigoplus_{i<n} x_i$ of size $O(n^c)$ for some constant c.
[Hint: Consider a balanced tree of binary parities. You may get it down to $c = 2$.]

6. Any DNF equivalent to the CNF $\bigwedge_{i<n}(x_i \vee y_i)$ has size $\Omega(2^n n)$.

7. Every Boolean function $f\colon \{0,1\}^n \to \{0,1\}$ can be represented by a formula of size $O(2^n)$.
[Hint: Inductively express a formula in $n+1$ variables as a combination of formulas in n variables.]

8. Prove the propositional soundness theorem: for all $\Gamma \subseteq \mathrm{Prop}_A$ and $\varphi \in \mathrm{Prop}_A$, if $\Gamma \vdash \varphi$, then $\Gamma \vDash \varphi$.

9. Let $\Gamma, \Delta \subseteq \mathrm{Prop}_A$ and $\varphi, \psi \in \mathrm{Prop}_A$. Show that if $\Gamma \vdash \varphi$ and $\Delta, \varphi \vdash \psi$, then $\Gamma, \Delta \vdash \psi$.

10. For every $\varphi \in \mathrm{Prop}_A$, its *De Morgan dual* $\varphi^{\mathrm{d}} \in \mathrm{Prop}_A$ is obtained by exchanging $\wedge$ with $\vee$, and $\top$ with $\bot$ inside φ. Formally, we define φ^{d} by induction on the complexity of φ:

$$\begin{aligned} a^{\mathrm{d}} &= a, \quad a \in A, & (\neg\varphi)^{\mathrm{d}} &= \neg(\varphi^{\mathrm{d}}), \\ \top^{\mathrm{d}} &= \bot, & \bot^{\mathrm{d}} &= \top, \\ (\varphi \wedge \psi)^{\mathrm{d}} &= (\varphi^{\mathrm{d}} \vee \psi^{\mathrm{d}}), & (\varphi \vee \psi)^{\mathrm{d}} &= (\varphi^{\mathrm{d}} \wedge \psi^{\mathrm{d}}). \end{aligned}$$

Show that for all assignments $v\colon A \to \{0,1\}$, $v(\varphi^{\mathrm{d}}) = v_\neg(\neg\varphi)$, where $v_\neg\colon A \to \{0,1\}$ is the assignment defined by $v_\neg(a) = 1 - v(a)$ for each $a \in A$.

11. Let $\varphi, \psi \in \mathrm{Prop}_A$.

(i) $\varphi \equiv \psi$ if and only if $\varphi^{\mathrm{d}} \equiv \psi^{\mathrm{d}}$.

(ii) $\varphi \vDash \psi$ if and only if $\psi^{\mathrm{d}} \vDash \varphi^{\mathrm{d}}$.

In the lecture, we have proved completeness of a proof system using connectives $\{\to, \bot\}$. A complete system using the De Morgan language $\{\wedge, \vee, \neg, \bot, \top\}$ is given in the van den Dries lecture notes, but the next exercise shows how to construct one mechanically.

12. For any $\{\to, \bot\}$-formula φ, let φ^* denote the De Morgan formula such that $p^* = p$ for atoms p, $\bot^* = \bot$, and $(\varphi \to \psi)^* = (\neg\varphi^* \vee \psi^*)$. Similarly, given a De Morgan formula ψ, let $\psi^{\#}$ be its translation to a $\{\to,\bot\}$-formula using fixed $\{\to,\bot\}$-translations of all De Morgan connectives. Let $\vdash_0$ denote a sound and complete Hilbert-style proof system for $\{\to,\bot\}$-formulas such as the one given in the lecture, and let $\vdash_1$ be the Hilbert-style proof system in the De Morgan language that has inference rule schemata $\varphi_1^*,\dots,\varphi_k^* \ / \ \varphi_0^*$ for each rule schema $\varphi_1,\dots,\varphi_k \ / \ \varphi_0$ of $\vdash_0$ (where axioms are treated as rules with $k=0$), and axiom schemata $\neg c(\varphi_0,\dots,\varphi_{k-1})\vee c^{\#*}(\varphi_0,\dots,\varphi_{k-1})$, $\neg c^{\#*}(\varphi_0,\dots,\varphi_{k-1})\vee c(\varphi_0,\dots,\varphi_{k-1})$ for each k-ary De Morgan connective c. Then $\vdash_1$ is a sound and complete proof system in the De Morgan language. [Hint: You will need to show $\vdash_1 \neg\psi\vee\psi^{\#*}$, $\vdash_1 \neg\psi^{\#*}\vee\psi$ for all De Morgan formulas ψ.]

13. (If you are familiar with topology.) Give a direct proof of the propositional compactness theorem, not using the completeness theorem.
[Hint: Consider the product topology on the set $\{0,1\}^A$ of all assignments.]

14. A set of propositional or first-order sentences S is *independent* if S is not equivalent to S' for any proper subset $S'\subsetneq S$.

(i) S is independent iff $S\smallsetminus\{\varphi\}\nvDash\varphi$ for all $\varphi\in S$.

(ii) Show that every countable theory T has an independent axiomatization, i.e., an independent set of sentences S equivalent to T. [Hint: Try to generalize the fact that $\{\varphi,\psi\}\equiv\{\varphi,\psi\vee\neg\varphi\}$.]

(Uncountable theories have independent axiomatizations as well by a theorem of I. Reznikoff, but this is more difficult to prove.)

15. Prove that if a term $t(x_0,\dots,x_{n-1},y)$ is free for y in a formula $\varphi(x_0,\dots,x_{n-1},y)$, then for all terms $s_0,\dots,s_{n-1},r$, the formula $\bigl(\varphi(t/y)\bigr)(s_0/x_0,\dots,s_{n-1}/x_{n-1},r/y)$ is syntactically identical to the formula $\varphi\bigl(s_0/x_0,\dots,s_{n-1}/x_{n-1},t(s_0/x_0,\dots,s_{n-1}/x_{n-1},r/y)/y\bigr)$.

16. Let $\mathcal{A}$ be an L-structure, t a closed L-term such that $t^{\mathcal{A}}=a\in A$, and $\varphi(x)$ an L-formula. Show that $\mathcal{A}\vDash\phi(t)$ iff $\mathcal{A}\vDash\phi(\underline{a})$.

17. Consider a modification of the first-order proof system given in the lecture such that the axioms of equality are replaced with the axiom $x=x$ and the axiom schema $t=s\wedge\varphi(t/x)\to\varphi(s/x)$ for all formulas φ and terms t,s free for x in φ. Show that this is equivalent to the original proof system.

18. For any formula $\varphi(x)$ and variable y free for x in φ, show that the formula $\exists y\,(\exists x\,\varphi(x)\to\varphi(y))$ is provable.

19. Using Vaught's test, show the completeness of the theory of a successor: it has a language with one unary function symbol s, and axioms $s(x)=s(y)\to x=y$, $\forall x\,\exists y\,s(y)=x$, and $s^n(x)\neq x$ for each $n\in\mathbb{N}_{>0}$, where s^n denotes the n-fold iteration of s (i.e., $s^0(x)$ is x, and s^{n+1} is $s(s^n(x))$).

20. For each $n\in\mathbb{N}$, let P_n denote the path graph of length n, i.e., the structure $\langle[n],E_n\rangle$, where $[n]=\{0,\dots,n-1\}$ and $E_n=\{\langle i,j\rangle\in[n]^2 : |i-j|=1\}$. Show that there is no sentence φ such that for all $n\in\mathbb{N}$, $P_n\vDash\varphi$ iff n is odd. [Hint: Adapt the previous exercise.]

21. Fix a field F. The theory of vector spaces over F has a language consisting of the language $\{+,-,0\}$ of abelian groups and unary functions $a\cdot x$ for each $a\in F$; it has the usual algebraic axioms (axioms of abelian groups, $ab\cdot x=a\cdot(b\cdot x)$, $1\cdot x=x$, $(a+b)\cdot x=a\cdot x+b\cdot x$, $a\cdot(x+y)=a\cdot x+a\cdot y$). Show that the theory of infinite vector spaces over F (i.e., with additional axioms $\exists x_0\dots\exists x_n\bigwedge_{i<j}x_i\neq x_j$ for $n\in\mathbb{N}$) is complete and κ-categorical for all infinite $\kappa>|F|$. [Hint: Every vector space has a basis.]

22. An *atom* in a Boolean algebra $\mathbf{A}=\langle A,0,1,\wedge,\vee,-,\leq\rangle$ is an element $a\in A$ such that $a>0$, but $0<x<a$ for no $x\in A$; $\mathbf{A}$ is *atomless* if $0\neq1$ and $\mathbf{A}$ has no atoms. Show that the theory of atomless Boolean algebras is $\aleph_0$-categorical, hence complete.
[Hint: Construct an isomorphism between two countable atomless Boolean algebras $\mathbf{A}$ and $\mathbf{B}$ by a back-and-forth argument, as a union of a sequence of isomorphisms between finite subalgebras. It might help to observe that if $\mathbf{A}_0$ is a finite subalgebra of $\mathbf{A}$, and $\mathbf{A}_1$ is the algebra generated by $A_0\cup\{b\}$ for some $b\in A$, then each atom of $\mathbf{A}_0$ either remains an atom in $\mathbf{A}_1$, or splits into two atoms.]

23. Show that the functions $+\colon \mathbb{N}^2 \to \mathbb{N}$ and $\cdot\colon \mathbb{N}^2 \to \mathbb{N}$ are computable when the input and output are represented in unary.

24. The same when the input and output are represented in binary.

25. Show that there are computable functions converting natural numbers from one representation to another (unary, ordinary base-k, bijective base-k, considering also different k's).

26. Fix an alphabet Σ.

(i) The following functions are computable: the constant function ε; the functions $s_a\colon \Sigma^* \to \Sigma^*$ for $a \in \Sigma$, defined by $s_a(x) = x\smile a$; the projections $\pi^n_i : (\Sigma^*)^n \to \Sigma^*$, $\pi^n_i(x_0, \dots, x_{n-1}) = x_i$.

(ii) If $f\colon (\Sigma^*)^n \to \Sigma^*$ and $g_i\colon (\Sigma^*)^m \to \Sigma^*$, $i < n$, are computable functions, their composition $h\colon (\Sigma^*)^m \to \Sigma^*$, $h(\vec{x}) = f(g_0(\vec{x}), \dots, g_{n-1}(\vec{x}))$, is computable.

(iii) If $f_\varepsilon\colon (\Sigma^*)^n \to \Sigma^*$ and $f_a\colon (\Sigma^*)^{n+2} \to \Sigma^*$, $a \in \Sigma$, are computable, the function $h\colon (\Sigma^*)^{n+1} \to \Sigma^*$ defined from them by the recursion

$$h(\vec{x}, \varepsilon) = f_\varepsilon(\vec{x}),$$
$$h(\vec{x}, y\smile a) = f_a(\vec{x}, y, h(\vec{x}, y))$$

is computable.

Functions in the smallest class that contains the functions from (i) and that is closed under the operations (ii) and (iii) are called *primitive recursive.* (Usually, the definition of primitive recursive functions is stated for functions $\mathbb{N}^n \to \mathbb{N}$, corresponding to our definition with $|\Sigma| = 1$ and the integers represented in unary. Our more general definition is equivalent up to the bijective base-$|\Sigma|$ numeration.)

27. The set of well bracketed strings over the alphabet $\Sigma = \{(_i,)_i : i < k\}$ is the smallest set of strings such that the empty string ε is well bracketed, and if x and y are well bracketed and $i < k$, then xy and $(_i x)_i$ are well bracketed. E.g., $(_3(_1)_1(_2(_0)_0)_2(_1)_1)_3(_2)_2$ is well bracketed. Show that the set of well bracketed strings is decidable.

28. Let L be a finite first-order language. Show that the following sets and functions are computable:

(i) The set of L-terms.

(ii) The set of L-formulas.

(iii) The set of pairs $\langle \varphi, x\rangle$ where x is a free variable of an L-formula φ.

(iv) The substitution function: given an L-formula φ, a variable x, and an L-term t, compute $\varphi(t/x)$.

(v) The set of triples $\langle \Gamma, \varphi, \pi\rangle$ where π is a proof of an L-formula φ from a finite set of L-formulas Γ.

29. A language $X \subseteq \Sigma^*$ is semidecidable iff it can be represented as $\exists w \in \Sigma'^*\, P(x, w)$ for a finite alphabet Σ' (which we might take to be Σ itself if $|\Sigma| \geq 2$) and a decidable predicate P.
[Hint: Consider a description of an accepting run of a Turing machine, or—if you are already familiar with the section on arithmetic—a Σ_1-formula that defines X in $\mathbb{N}$.]

30. (Craig's trick.) Every semidecidable theory is recursively axiomatizable. [Hint: Express $\mathrm{Thm}(T)$ as $\exists w\, P(\varphi, w)$ with P decidable. Given φ and w, devise a sentence equivalent to φ that encodes w.]

31. Show that every decidable consistent theory T has a decidable complete extension.
[Hint: Consider a completion procedure that enumerates sentences φ one by one, and extends the current list of axioms with φ or $\neg\varphi$, whichever maintains consistency with T.]

32. Prove $\mathsf{Q} \vdash \forall x\,(x \le \overline{n} \vee \overline{n} \le x)$ for each $n \in \mathbb{N}$.

33. Q proves $x \cdot y = 0 \to x = 0 \vee y = 0$, and more generally, $x \cdot y = \overline{n} \to x = 0 \vee y \le \overline{n}$ for each $n \in \mathbb{N}$.

34. The standard model $\mathbb{N}$ extends to an L_{PA}-structure $\mathbb{N}^\infty$ with domain $\mathbb{N} \cup \{\infty\}$, $\infty \notin \mathbb{N}$, so that $\mathbb{N}^\infty \vDash \mathsf{Q}$. Moreover, we are free to choose $(0 \cdot \infty)^{\mathbb{N}^\infty}$ in an arbitrary way (while the rest of the model is uniquely determined by the axioms of Q). Conclude that Q does not prove any of the formulas $S(x) \nleq x$, $x \cdot y = y \cdot x$, or $0 \cdot x \ne 1$.

35. Q does not prove $x + y = y + x$ or $0 + (x + y) = (0 + x) + y$.
[Hint: Modify the previous exercise to a model with two "infinities".]

36. All Σ_1-definable sets are semidecidable.

In the lecture, we developed an encoding of sequences in the language of arithmetic using Gödel's β-function. In the next three exercises, you will devise an alternative sequence encoding scheme due to E. Nelson, as simplified by P. Pudlák.

37. The set $\{x : \exists n \in \mathbb{N}\, x = 2^n\}$ of powers of 2 is definable by a Δ_0 formula, not using the 2^n function.
[Hint: Consider the divisors of x.]

38. Consider an encoding of finite sets $X \subseteq \mathbb{N}$ by pairs $[r, w]$ where the binary expansion of w is a concatenation of binary expansions of elements of X, and the binary expansion of r acts as a "ruler" such that the positions of 1's mark where the individual elements of X start in w. Show that the predicate "x is in the set encoded by $[r, w]$" is Δ_0-definable.

39. Construct a Δ_0 encoding of finite sequences based on the previous exercise.

As yet another alternative, we will look at a representation of binary strings introduced by A. A. Markov Jr., who attributes it to J. Nielsen. The idea of using it for encoding strings in weak theories of arithmetic is due to J. Murwanashyaka; the extension to sequences of integers is due to A. Visser.

40. Let $\langle \mathrm{SL}_2(\mathbb{N}), I, \cdot \rangle$ denote the monoid of non-negative integer matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{N}^{2\times 2}$ of determinant 1, with $\cdot$ being matrix multiplication and $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Put $A_0 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $A_1 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

- (i) Given $i = 0, 1$, which $M \in \mathrm{SL}_2(\mathbb{N})$ are of the form NA_i for $N \in \mathrm{SL}_2(\mathbb{N})$? [Hint: Focus on comparisons between the entries of M.]
- (ii) Using (i), show that each $M \in \mathrm{SL}_2(\mathbb{N}) \smallsetminus \{I\}$ can be written in a unique way as NA_0 or NA_1 with $N \in \mathrm{SL}_2(\mathbb{N})$.
- (iii) Conclude that $\mathrm{SL}_2(\mathbb{N}) \simeq \langle \{0,1\}^*, \varepsilon, \smile \rangle$.

41. Develop a Δ_0 encoding of finite sequences based on the previous exercise. [Hint: You may represent $\{n_0, \dots, n_{k-1}\}$ by $A_0^{n_0} \cdots A_1 A_0^{n_{k-1}} A_1$, using $A_0^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$. Then encode sequences by sets.]

A formula $\varphi(x)$ *represents* a set $X \subseteq \mathbb{N}$ in a theory T if $T \vdash \varphi(\overline{n})$ for all $n \in X$, and $T \vdash \neg\varphi(x)$ for all $n \in \mathbb{N} \smallsetminus X$.

A formula $\varphi(x, y)$ represents in T a partial function $f \colon \mathbb{N} \rightharpoonup \mathbb{N}$ if $T \vdash \forall y\,(\varphi(\overline{n}, y) \leftrightarrow y = \overline{m})$ for all $n, m \in \mathbb{N}$ such that $f(n) = m$.

42. All decidable sets are Σ_1-representable in Q.
[Hint: Starting with Σ_1-definitions of X and $\mathbb{N} \smallsetminus X$, write a Σ_1 formula expressing "there is a witness for $x \in X$ smaller than any witness for $x \notin X$". Use Exer. 32 to show that it works.]

43. All partial computable functions are Σ_1-representable in Q.
[Hint: Using a Σ_1-definition of the graph of f, adapt the witness comparison argument from Exer. 42.]

44. Prove Gödel's diagonal lemma: for every formula $\varphi(x)$, there exists a sentence α such that $Q \vdash \alpha \leftrightarrow \varphi(\overline{\ulcorner \alpha \urcorner})$. [Hint: Using representability of a suitable computable function, construct a formula $\psi(x)$ such that $\mathsf{Q} \vdash \psi(\overline{\ulcorner \chi \urcorner}) \leftrightarrow \varphi(\overline{\ulcorner \chi(\overline{\ulcorner \chi \urcorner}) \urcorner})$ for all $\chi(x)$.]