Computing and Software 701

Logic and Discrete Mathematics In Software Engineering

Fall 2002

Exercises

Revised: 03 December 2002

1. What did A. Fraenkel contribute to ZF set theory?

2. Describe one of the set-theoretic paradoxes other than Russell's Paradox.

3. What is the cardinality of the function space $\mathbf{N} \to \mathbf{N}$, where $\mathbf{N}$ denotes the set of natural numbers?

4. (a) Let T_n be a full binary tree of height $n \geq 1$. What is the cardinality of the set of nodes in T_n? What is the cardinality of the set of paths in T_n?

   (b) Let T_∞ be a full binary tree of infinite height. What is the cardinality of the set of nodes in T_∞? What is the cardinality of the set of paths in T_∞?

5. State and prove the de Morgan Laws for sets.

6. Prove the Schröder-Bernstein Theorem that says, if $f : A \to B$ and $g : B \to A$ are total injective functions, then there exists a total bijective function $h : A \to B$.

7. Let an *ordinal* be a set α such that $\bigcup \alpha \subseteq \alpha$ and α is strictly well-ordered by the $\in$ relation. Prove that every ordinal is a set of ordinals well-ordered by the $\subseteq$ relation.

8. The ordinals represent the well-order types. For a string s, let $|s|$ denote the length of s. For strings s and t over a well-ordered alphabet, let $s \prec t$ mean that either $|s| < |t|$ or $|s| = |t|$ and s comes before t in lexicographic order.

(a) Let $\mathcal{S}$ be the set of all strings of length m over a well-ordered alphabet of order type $n < \omega$. What ordinal has the same order type as $(\mathcal{S}, \prec)$?

(b) Let $\mathcal{S}$ be the set of all strings of length m over a well-ordered alphabet of order type ω. What ordinal has the same order type as $(\mathcal{S}, \prec)$?

(c) Let $\mathcal{S}$ be the set of all strings over a well-ordered alphabet of order type $n < \omega$. What ordinal has the same order type as $(\mathcal{S}, \prec)$?

(d) Let $\mathcal{S}$ be the set of all strings over a well-ordered alphabet of order type ω. What ordinal has the same order type as $(\mathcal{S}, \prec)$?

9. Let $f : A \to B$ and $g : B \to C$ be total, and let $h = g \circ f : A \to C$ be the composition of g and f.

   (a) Prove that, if f and g are injective, then h is injective, but the converse is false.

   (b) Prove that, if f and g are surjective, then h is surjective, but the converse is false.

10. Show how a relation $R \subseteq A \times B$ can be transformed into an "equivalent" total function $f_R : A \to \mathcal{P}(B)$, where $\mathcal{P}(B)$ is the power set of B. (A function like f_R is sometimes called a *many-valued function*.)

11. (a) Suppose $R \subseteq A^2$ is an equivalence relation. Let the *equivalence class* of $a \in A$ be the set $\{b \mid aRb\}$. Show that the set of equivalence classes is a *partition* of A.

    (b) Suppose P is a partition of A. Let $R \subseteq A^2$ be the relation such that aRb iff, for some $C \in P$, $a, b \in C$. Show that R is an equivalence relation.

12. Let $A = \{a, b, c\}$.

    (a) List all the equivalence relations on A.

    (b) List all the (nonstrict) preorders on A that are not nonstrict partial orders.

    (c) List all the nonstrict partial orders on A that are not nonstrict linear orders.

    (d) List all the nonstrict linear orders on A.

13. Give an example of a relation that is symmetric and transitive but not reflexive.

14. (a) What properties define a *nonstrict* linear order?
    (b) What properties define a *strict* linear order?

15. Suppose $P = (S, \leq)$ is a preorder. Define a nontrivial equivalence relation R on S such that the *quotient structure* P/R is a partial order.

16. Define the *transitive closure* of a binary relation. Prove that the transitive closure of a union of equivalence relations is an equivalence relation.

17. Define what a *Goodstein sequence* is. Using ordinals show that every Goodstein sequences converges to 0! (See Reuben L. Goodstein, "On the restricted ordinal theorem", J. Symbolic Logic 9:33-41, 1944. L. Kirby and J. Paris showed in 1982 the remarkable result that the Goodstein theorem cannot be proven in Peano arithmetic.)

18. Let $M = (D, 0, +)$ be an arbitrary monoid. For $m, n \in \mathbf{Z}$ and a total function $f : \mathbf{Z} \to D$, define

$$\sum_{i=m}^{n} f(i) = \begin{cases} f(m) + f(m+1) + \cdots + f(n) & \text{if } m \leq n \\ 0 & \text{if } m > n \end{cases}$$

    Is the following statement true in M? For all $m, n \in \mathbf{Z}$ and total functions $f, g : \mathbf{Z} \to D$,

$$\sum_{i=m}^{n} (f(i) + g(i)) = \sum_{i=m}^{n} f(i) + \sum_{i=m}^{n} g(i).$$

    If so, prove it. If not, find a condition that characterizes the set of monoids in which the statement is true, and then prove the statement assuming the condition.

19. Turing machines.

    (a) Construct a Turing machine that computes the function $f : \mathbf{N} \to \mathbf{N}$ such that $f(x) = 2 * x$.
    (b) Show how to construct a universal Turing machine.

20. Unlimited register machines (URMs).

    (a) Define what a URM is.

    (b) Construct a URM that computes the function $f : \mathbf{N} \to \mathbf{N}$ such that $f(x) = 2 * x$.

    (c) Show how to construct a universal URM.

21. Regular expressions.

    (a) Define the notion of a *regular expression*.

    (b) Find out how regular expressions are used by the Unix `grep` command.

    (c) Review the proof that a language can be represented by a regular expression iff it can be represented by a finite automaton.

    (d) Prove the algebraic laws of regular expressions given in Exercise 3.4.1 of J. Hopcraft, R. Motwani, and J. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Second Edition, Addison Wesley, 2001.

22. Show how the Sheffer stroke | (a.k.a. NAND) can be used to define the following propositional connectives: $\neg$, $\Rightarrow$, $\wedge$, $\vee$, and $\Leftrightarrow$.

23. Use truth tables to verify that the following propositional formulas are tautologies.:

    (a) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ (Modus Ponens)

    (b) $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ (Law of Contraposition).

    (c) $P \vee \neg P$ (Law of Excluded Middle)

    (d) $\neg\neg P \Rightarrow P$ (Law of Double Negation).

    (e) $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$ (De Morgan Law)

    (f) $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$ (De Morgan Law)

24. Prove each of the tautologies listed in Exercise 23 in a sound and complete Gentzen system for propositional logic.

25. Prove each of the tautologies listed in Exercise 23 in a sound and complete natural deduction system for propositional logic.

26. Prove each of the tautologies listed in Exercise 23 in a sound and complete semantic tableau system for propositional logic.

27. Define what it means for a formula of propositional logic to be in *disjunctive normal form* and in *conjunctive normal form*. Given a language L of propositional logic, prove that, for every formula φ of L, there is a formula ψ_1 of L in disjunctive normal form and a formula ψ_2 of L in conjunctive normal form such that $\varphi \Leftrightarrow \psi_1$ and $\varphi \Leftrightarrow \psi_2$ are tautologies.

28. Define what it means for a formula of first-order logic to be in *prenex normal form*. Given a language L of first-order logic, prove that, for every formula φ of L, there is a formula ψ of L in prenex normal form such that $\varphi \Leftrightarrow \psi$ is valid.

29. Find a set S of real numbers such that the order type of $(S, \leq)$ is $\omega+1$.

30. State and prove the compactness theorem for first-order logic assuming the completeness theorem for first-order logic. Use the compactness theorem to prove the following:

    (a) Every first-order theory that has arbitrarily large finite models, has an infinite model.

    (b) There exists a *nonstandard model* of first-order Peano arithmetic.

    (c) There exists an extension of the standard first-order model of real arithmetic that contains infinitesimals. (A *(positive) infinitesimal* is a number ϵ such that, for all $r \in \mathbf{R}$, if $0 < r$, then $0 < \epsilon < r$).

31. Formalize the following theories in first-order logic:

    (a) The theory of partial orders $(D, \leq)$ where $\leq \subseteq D \times D$.

    (b) The theory of linear orders $(D, \leq)$ where $\leq \subseteq D \times D$.

    (c) The theory of dense linear orders $(D, \leq)$ where $\leq \subseteq D \times D$.

    (d) The theory of lattices $(D, \leq, \cup, \cap)$ where $\leq \subseteq D \times D$, $\cup : D \times D \to D$, and $\cap : D \times D \to D$.

    (e) The theory of boolean algebras $(D, +, *, ^-, 0, 1)$ where $+ : D \times D \to D$, $* : D \times D \to D$, $^- : D \to D$, $0 \in D$, and $1 \in D$.

    (f) The theory of monoids $(D, +, 0)$ where $+ : D \times D \to D$ and $0 \in D$.

(g) The theory of groups $(D, +, ^-, 0)$ where $+ : D \times D \to D$, $^- : D \to D$, and $0 \in D$.

(h) The theory of rings $(D, +, ^-, 0, *)$ where $+ : D \times D \to D$, $^- : D \to D$, $0 \in D$, and $* : D \times D \to D$.

(i) The theory of fields $(D, +, ^-, 0, *, ^{-1}, 1)$ where $+ : D \times D \to D$, $^- : D \to D$, $0 \in D$, $* : D \times D \to D$, $^{-1} : D \to D$, and $1 \in D$.

(j) The theory of graphs (N, E) where $E \subseteq N \times N$.

(k) The theory of bipartite graphs (N, B, R, E) where $B \subseteq N$, $R \subseteq N$, and $E \subseteq N \times N$.

32. Formalize the following theories in simple type theory:

(a) The theory of well orders $(D, \leq)$ where $\leq \subseteq D \times D$.

(b) The theory of a complete ordered field $(D, +, ^-, 0, *, ^{-1}, 1)$ where $+ : D \times D \to D$, $^- : D \to D$, $0 \in D$, $* : D \times D \to D$, $^{-1} : D \to D$, and $1 \in D$. This is the theory of the real numbers. It is *categorical*, i.e., it has one model (up to isomorphism).

33. Let BESTT$^-$ be the BESTT logic without type variables.

(a) Write down the traditional semantics for BESTT$^-$.

(b) Write down the partial semantics for BESTT$^-$.

34. Define the following theories of stacks in BESTT.

(a) T_1 is a theory of abstract stacks of integers.

(b) T_2 is a theory of abstract stacks of abstract elements.

(c) T_3 is a theory of stacks of abstract elements represented as lists.

35. Let T be a formalization in BESTT with the partial semantics of the theory of a complete ordered field.

(a) Define a predicate constant in T that formalizes the notion of a continuous function.

(b) Define a function constant in T that formalizes the mapping from an infinite sequence of real numbers to its limit. (The mapping is undefined if the sequence has no limit.)

(c) Define the $\sum$ and $\prod$ operators in T.

36. Show that the exponential function on $\mathbf{N}$ is primitive recursive.

37. Give an example of a computable total function on $\mathbf{N}$ that is not primitive recursive.

38. Show how Hilbert's ϵ operator can be used to define the quantifiers $\forall$ and $\exists$.

39. Define the notion of an isomorphism from one model of STT to another.

40. Well-founded relations.

    (a) Show that a well-founded relation has no infinite descending sequences.

    (b) Give a natural example of a well-founded relation that is not a partial order.

41. Let $f : \mathbf{N} \to \mathbf{N}$ generate the Fibonacci sequence.

    (a) Show that f is a primitive recursive function.

    (b) Define f by well-founded recursion.

    (c) Define f by recursion via a monotone functional.

42. Construct a monotone functional $F : \alpha \to \alpha$ such that the least fixed point of F is $F^\gamma(\triangle_\alpha)$ where $\omega < \gamma$ and $\triangle_\alpha$ is the empty function of type α

43. Define the set of terms and the set of formulas of PFOL as two sets of strings by mutual recursion.

44. Let a *tree* be defined by:

    - Every real number is a tree.
    - If s and t are trees, then the pair (s, t) is a tree.

    (a) Formulate a theory of trees in BESTT similar to Peano arithmetic.

    (b) Define the "mirror" of a tree by well-founded recursion and prove by induction that the mirror operation is idempotent.