CS30053 Foundations of Computing, Spring 2004

Practice exercises : Set 1

---

1. Prove the following equivalences of propositions:

(a) $(p \to q) \wedge (q \to r) \equiv (p \to r)$.

(b) $p \to (q \to r) \equiv (p \wedge q) \to r$.

(c) $\neg p \to (q \to r) \equiv q \to (p \vee r)$.

2. Which of the following statements is/are true?

(a) $\forall x \in \mathbb{Z}^+ \left[\text{isComposite}(x) \to \exists y \in \mathbb{Z}^+ \setminus \{1, x\} \; [y \mid x] \right]$.

(b) $\exists x \in \mathbb{Z}^+ \left[\text{isPrime}(x) \to \text{isOdd}(x+1) \right]$.

(c) $\forall x \in \mathbb{Z}^+ \left[\text{isPrime}(x) \to (x = 2) \vee \text{isEven}(x+1) \right]$.

(d) $\forall x \in \mathbb{Z}^+ \left[\text{isPrime}(x) \to \Big((x > 2) \to \text{isEven}(x+1) \Big) \right]$.

(e) $\forall x \in \mathbb{Z}^+ \; \exists y \in \mathbb{Z}^+ \left[(y > 1) \wedge (y^2 \mid x) \right]$.

(f) $\forall x \in \mathbb{Z}^+ \; \exists y \in \mathbb{Z}^+ \; \forall z \in \mathbb{Z}^+ \setminus \{1\} \left[(y > x) \wedge (z^2 \mid y) \right]$.

(g) $\forall x \in \mathbb{Z}^+ \; \forall z \in \mathbb{Z}^+ \setminus \{1\} \; \exists y \in \mathbb{Z}^+ \left[(y > x) \wedge (z^2 \mid y) \right]$.

* **3.** An open interval (in $\mathbb{R}$) is a subset (of $\mathbb{R}$) of the form $(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$ for some $a < b$. A closed interval is a subset of the form $[a, b] := \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$ for some $a < b$. A subset A of $\mathbb{R}$ is called open if for all $x \in A$ there exists an open interval (a, b) containing x and contained in A. A subset B of $\mathbb{R}$ is called closed if its complement in $\mathbb{R}$ is open. Prove that:

(a) An open interval is an open set.

(b) A closed interval is a closed set.

(c) The union of an arbitrary number of open sets is again open.

(d) The intersection of a finite number of open sets is again open.

(e) The intersection of an infinite number of open sets need not be open.

4. Construct an explicit bijection between the sets $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$.

5. Let A, B be finite sets with $|A| = m$ and $|B| = n$. Determine the numbers of:

(a) functions $A \to B$,

(b) injective functions $A \to B$ (provided that $m \leqslant n$),

** **(c)** surjective functions $A \to B$ (provided that $m \geqslant n$),

(d) bijective functions $A \to B$ (provided that $m = n$),

(e) symmetric relations on A,

(f) reflexive and symmetric relations on A.

6. Let $f : A \to B$ and $g : B \to C$ be functions.

(a) If f and g are both injective, prove that $g \circ f$ is injective too.

(b) If f and g are both surjective, prove that $g \circ f$ is surjective too.

(c) If f and g are both bijective, prove that $g \circ f$ is bijective too. Show also that in this case we have $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(d) If $g \circ f$ is injective, prove that f is injective too.

(e) If $g \circ f$ is surjective, prove that g is surjective too.

(f) Give an example in which g is not injective, but $g \circ f$ is injective.

(g) Give an example in which f is not surjective, but $g \circ f$ is surjective.

7. Let A be a set of cardinality $n := |A|$ and $f : A \to A$ a function.

(a) If n is finite, show that f is injective if and only if f is surjective.

(b) If $n = \infty$, demonstrate by examples that neither of the implications of Part (a) is true.

8. Let $f : A \to B$ be a function. For $S \subseteq A$ define the set $f(S) := \{f(x) \mid x \in S\} \subseteq B$. Also for $T \subseteq B$ define $f^{-1}(T) := \{x \in A \mid f(x) \in T\} \subseteq A$. Let S, S_1, S_2 be subsets of A and T, T_1, T_2 subsets of B. Prove the following assertions:

(a) If $S_1 \subseteq S_2$, then $f(S_1) \subseteq f(S_2)$.

(b) If $T_1 \subseteq T_2$, then $f^{-1}(T_1) \subseteq f^{-1}(T_2)$.

(c) $S \subseteq f^{-1}(f(S))$.

(d) $f(f^{-1}(T)) \subseteq T$.

(e) $f(f^{-1}(f(S))) = f(S)$.

(f) $f^{-1}(f(f^{-1}(T))) = f^{-1}(T)$.

*** 9.** Let $f : A \to A$ be a bijection. Assume that there exists a positive integer r such that the r-fold composition f^r of f is the identity map ι_A. The smallest such (positive) r is called the order of f. If no such r exists, we say that f is of infinite order.

Take $A := \mathbb{Z}$ and consider the following functions $\mathbb{Z} \to \mathbb{Z}$:

$$f(n) := \begin{cases} n+1 & \text{if } n \text{ is even,} \\ n-1 & \text{if } n \text{ is odd.} \end{cases}$$
$$g(n) := \begin{cases} n-1 & \text{if } n \text{ is even,} \\ n+1 & \text{if } n \text{ is odd.} \end{cases}$$

Prove the following assertions:

(a) Both f and g are bijections on $\mathbb{Z}$.

(b) Both f and g are of order 2.

(c) $g \circ f$ is of infinite order.

10. Take some fixed $n \in \mathbb{Z}^+$ and let $\mathcal{M}$ denote the set of all $n \times n$ matrices with real entries. Two matrices $A, B \in \mathcal{M}$ are called similar if $B = PAP^{-1}$ for some invertible (i.e., nonsingular) matrix $P \in \mathcal{M}$. Verify that similarity is an equivalence relation on $\mathcal{M}$.

11. We generalize the notion of congruence as follows: Let m, n be positive integers. For $a, b \in \mathbb{Z}$ define $a \equiv b \pmod{m, n}$ if and only if $a - b = km + ln$ for some $k, l \in \mathbb{Z}$. Prove that:

(a) This generalized congruence is an equivalence relation on $\mathbb{Z}$.

*** (b)** $a \equiv b \pmod{m, n}$ if and only if $a \equiv b \pmod{d}$, where d is the gcd of a and b. (**Hint:** You may use without proof the fact that there exist integers u, v such that $d = um + vn$.)

12. Let A denote the set of all functions $\mathbb{N} \to \mathbb{N}$. Define a relation $\preceq$ on A as follows: $f \preceq g$ if and only if $f(n) \leqslant g(n)$ for all $n \in \mathbb{N}$. Argue that $\preceq$ is a partial order on A. Is $\preceq$ also a total order on A?

13. Construct an explicit well-ordering of $\mathbb{Z}$. Also of $\mathbb{Z} \times \mathbb{Z}$ and of $\mathbb{Q}$.