CS103X: Discrete Structures
Homework Assignment 3

Due February 15, 2008

Exercise 1 (15 points)**.** For each of the following relations, state whether they fulfill each of the 4 main properties - reflexive, symmetric, antisymmetric, transitive. Briefly substantiate each of your answers.

(a) The coprime relation on $\mathbb{Z}$. (Recall that a, $b \in \mathbb{Z}$ are coprime if and only if $\gcd(a, b) = 1$.)

(b) Divisibility on $\mathbb{Z}$.

(c) The relation T on $\mathbb{R}$ such that aTb if and only if $ab \in Q$.

Solution

(a) It's definitely not reflexive, as no integer is coprime with itself except -1 and 1. It is symmetric because $\gcd(a, b) = \gcd(b, a)$, so $\gcd(a, b) = 1$ iff $\gcd(b, a) = 1$. Not antisymmetric — *every* coprime pair, such as (5,7) and (7,5), will show this. Not transitive — $\gcd(5, 7) = 1$, $\gcd(7, 10) = 1$, but $\gcd(5, 10) \neq 1$.

(b) It's reflexive since any integer divides itself. Not symmetric, for example $2 \mid 4$ but $4 \nmid 2$. It not antisymmetric on $\mathbb{Z}$, since $a \mid -a$ and $-a \mid a$, although it would be antisymmetric if restricted to $\mathbb{N}$. It is transitive — if $a \mid b$ then $b = ka$ for some $k \in \mathbb{Z}$, and if $b \mid c$ then $c = lb$ for some $l \in \mathbb{Z}$, thus $c = (lk)a$ and $(lk) \in \mathbb{Z}$ so $a \mid c$.

(c) Not reflexive, for example $\sqrt[4]{2}\sqrt[4]{2} = \sqrt{2}$ which is definitely not in $\mathbb{Q}$. Definitely symmetric since multiplication is commutative, $ab = ba$ always. Not antisymmetric, since $\sqrt{2}\sqrt{8} = \sqrt{8}\sqrt{2} = 4$ but $\sqrt{2} \neq \sqrt{8}$. Also not transitive — consider $a = \pi$, $b = \frac{1}{\pi}$, and $c = \pi$. $ab, bc \in \mathbb{Q}$ but $ac = \pi^2 \notin \mathbb{Q}$.

Exercise 2 (10 points)**.** In a partially ordered set, a chain is a totally ordered subset. For example, in the set 1, 2, 3, 4, 5, 6, the divisibility relation is a partial order and 1, 2, 4 and 1, 3, 6 are chains.

(a) What is the longest chain on the set $\{1, 2, \ldots, n\}$ using the divisibility relation? How many distinct chains have this length? For the second part, make sure to consider all positive values of n.

(b) What is the longest chain on the powerset of a set A with $|A| = n$ with the $\subseteq$ relation? How many distinct chains have this length?

Solution

(a) Longest chain is powers of 2 as high as they can go, length is $log_2 n + 1$. There is one chain of this length, except for $n = 3$ where there are two chains of length two.

(b) Each set in the chain must have distinct cardinality, so the longest chains are $n + 1$. The number of chains is the product of all binomial coefficients for n as they correspond to the number of sets of each cardinality.

Exercise 3 (25 points)**.** Formulate each of the below as a *single* statement (proposition or predicate), using only mathematical and logical notation that has been defined in class. For example, the use of logical quantifiers and connectives, and arithmetic, number-theoretic, and set-theoretic operations is allowed, as is the use of operators like gcd or sets like $\mathbb{Q}$, $\mathbb{R}$, etc., but *not* the use of English-language words or informal shorthand like $\{1, 2, \ldots, n\}$.

(a) There are infinitely many primes.

(b) If a and b are integers and $b \neq 0$, then there is a unique pair of integers q and r, such that $a = qb + r$ and $0 \leq r < |b|$.

(c) If a and n are coprime then there exists exactly one $x \in \mathbb{Z}_n$ for which $ax \equiv_n b$, for any $b \in \mathbb{Z}$.

(d) Two integers are coprime if and only if every integer can be expressed as their linear combination.

(e) The principle of strong induction

Solution

(a) $\forall n \in \mathbb{N}^+, \exists p \in \mathbb{N}^+ : (p > n \wedge (\forall k \in \mathbb{N}^+ : k < p \rightarrow gcd(p,k) = 1)$

(b) $\forall a, b \in \mathbb{Z} : (b \neq 0) \rightarrow \Big(\forall q, r, q', r' \in \mathbb{Z} : \Big((a = qb + r) \wedge (0 \leq r < |b|) \wedge (a = q'b + r') \wedge (0 \leq r < |b|)\Big)$
$\rightarrow (q = q') \wedge (r = r')\Big)$

(c) $\forall a, n \in \mathbb{Z} : \Big(gcd(a,n) = 1\Big) \rightarrow \Big(\forall b \in \mathbb{Z}, \forall x, x' \in \mathbb{Z}_n : \Big((ax \equiv_n b) \wedge (ax' \equiv_n b)\Big) \rightarrow (x = x')\Big)$

(d) $\forall a, b, \in \mathbb{Z} : (gcd(a,b) = 1 \leftrightarrow \forall n \in \mathbb{Z}, \exists x, y \in \mathbb{Z} : n = ax + by)$

(e) $\forall A \subseteq N^+ : \Big(1 \in A \wedge \Big(\forall k \in A : (\forall l \in N^+ \wedge (1 \leq l \leq k) : l \in A) \rightarrow k + 1 \in A\Big)\Big) \rightarrow (A = \mathbb{N}^+)$

Exercise 4 (25 points)**.** After completing the previous exercise, write the negation of each of your logical statements, such that the symbol $\neg$ does not appear in your statements. (That is, eliminate negated quantifiers and negated compounds as you have learned in class, and then replace statements such as $\neg(a|b)$ by statements like $a \not| b$.) Read the negations out in natural language and check for yourself that you understand why these are the right negations for the statements in the previous exercise.

Solution

(a)

$$\neg(\forall n \in \mathbb{N}^+, \exists p \in \mathbb{N}^+ : (p > n \wedge (\forall k \in \mathbb{N}^+ : k < p \rightarrow gcd(p,k) = 1))) \Leftrightarrow$$
$$\exists n \in \mathbb{N}^+, \forall p \in \mathbb{N}^+ : \neg(p > n \wedge (\forall k \in \mathbb{N}^+ : k < p \rightarrow gcd(p,k) = 1)) \Leftrightarrow$$
$$\exists n \in \mathbb{N}^+, \forall p \in \mathbb{N}^+ : (p \leq n \vee \neg(\forall k \in \mathbb{N}^+ : k < p \rightarrow gcd(p,k) = 1)) \Leftrightarrow$$
$$\exists n \in \mathbb{N}^+, \forall p \in \mathbb{N}^+ : (p \leq n \vee (\exists k \in \mathbb{N}^+ : \neg(k < p \rightarrow gcd(p,k) = 1))) \Leftrightarrow$$
$$\exists n \in \mathbb{N}^+, \forall p \in \mathbb{N}^+ : (p \leq n \vee (\exists k \in \mathbb{N}^+ : (k < p \wedge gcd(p,k) \neq 1)))$$

(b) $\exists a, b \in \mathbb{Z} : (b \neq 0) \wedge \Big(\exists q, r, q', r' \in \mathbb{Z} : \Big((a = qb + r) \wedge (0 \leq r < |b|) \wedge (a = q'b + r') \wedge (0 \leq r < |b|)\Big) \wedge \Big((q \neq q') \vee (r \neq r')\Big)\Big)$

(c) $\exists a, n \in \mathbb{Z} : \Big(gcd(a,n) = 1\Big) \wedge \Big(\exists b \in \mathbb{Z}, \exists x, x' \in \mathbb{Z}_n : \Big((ax \equiv_n b) \wedge (ax' \equiv_n b)\Big) \wedge (x \neq x')\Big)$

(d) $\exists a, b, \in \mathbb{Z} : (gcd(a,b) \neq 1 \leftrightarrow \forall n \in \mathbb{Z}, \exists x, y \in \mathbb{Z} : n = ax + by)$

(e) $\exists A \subseteq \mathbb{N}^+ : \Big(1 \in A \wedge \Big(\forall k \in A : (\forall l \in \mathbb{N}^+ \wedge (1 \leq l \leq k) : l \in A) \rightarrow k + 1 \in A\Big)\Big) \wedge (A \neq \mathbb{N}^+)$

Exercise 5 (15 points)**.** (a) Prove that the logical connectives $\{\neg, \vee\}$ are a universal set of connectives. That is, show that propositions like $P \rightarrow Q$, $P \leftrightarrow Q$, and $P \wedge Q$ can be expressed in terms of $\neg$ and $\vee$ alone.

(b) Prove that $\neg, \oplus$ are not a universal set.

Solution

(a) First, show that $\rightarrow$ is not needed - this is simple, by the lecture notes $A \rightarrow B \Leftrightarrow \neg A \vee B$. Similarly, $A \leftrightarrow B \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$. Finally, $(A \wedge B) \Leftrightarrow \neg(\neg A \vee \neg B)$. These show that any statement involving the discarded connectives can be expressed using $\neg, \vee$.

(b) $A \wedge B$ is true only for one of the four possible pairs of A, B. Any statement using $A \oplus B$ will always be true for two of the four possible pairs of A, B. To build an equivalent for $A \wedge B$ we need $C \oplus D$ where C, D are statements built from $A, B, \neg, \oplus$ such that C, D have opposite values when A,B both true and same values otherwise. Thus, without loss of generality, assume C is true, D false when A,B both true. There is no way for both C and D to be true for two combinations of A,B; and thus the problem recurses to finding a method of finding a C or D that is true for one combination of A,B or false for one combination of A,B, which is equivalent to the original problem. Thus $A \wedge B$ cannot be represented.

Exercise 6 (10 points)**.** You are given the following predicate on the set P of all people who ever lived:

Parent(x, y): true if and only if x is the parent of y.

(a) Rewrite in the language of mathematical logic (you may assume the equality/inequality operators):

All people have two parents.

Solution

$$\forall x \in P \;\; \exists y, z \in P : \big(\text{Parent}(y, x) \land \text{Parent}(z, x) \land y \neq z\big)$$

(b) We will recursively define the concept of *ancestor*:

An ancestor of a person is one of the person's parents or the ancestor of (at least) one of the person's parents.

Rewrite this definition using the language of mathematical logic. Specifically, you need to provide a necessary and sufficient condition for the predicate Ancestor(x, y) to be true. (Note that you can inductively use the Ancestor$(\cdot, \cdot)$ predicate in the condition itself.)

Solution

$$\forall x, y \in P : \Big(\text{Ancestor}(x, y) \leftrightarrow \big(\text{Parent}(x, y) \lor (\exists z \in P : (\text{Parent}(z, y) \land \text{Ancestor}(x, z)))\big)\Big)$$