CSE 20, Discrete Mathematics, Spring 1997
Homework 2,
Answers to selected problems

definitions An integer x is a *factor* of an integer y if there is an integer z so that $xz = y$, or symbolically, if $\exists z \quad xz = y$. Use this definition to express the following in terms of predicate logic and then simplify the underlying logical forms, where the underlying universe is the positive integers:

1. x is not a factor of y
   Solution: From the above definition, x is a factor of $y \equiv \exists z \quad xz = y$. So x is not a factor of $y \equiv \neg\exists z[xz = y] \equiv \forall z[xz \neq y]$.
   Note that what we are doing here is defining a predicate in x and y, so x, y are "inputs" to the predicate or "free" variables in the expression, and do not need to be quantified. What we are saying is "what it means for some integer x not to be a factor of some integer y is as follows:". However, the definition will hold for all x and all y. The way to say this is not to say that the DEFINITION is $\forall x \forall y \exists z[xz \neq y]$, which is just a false statement for the integers, but to say "$\forall x \forall y$(the defined predicate is equivalent to the definition) " , e.g. $\forall x \forall y$ [x is not a factor of $y \equiv \forall z(xz \neq y)$]. The difference is that what is always true is that the two sides are the same; it is not the case that one side is always true or the other side is always true.

2. For two integers, x and y, x is relatively prime to y if and only if the only positive integer that is a factor of both x and y is 1. Express "x is not relatively prime to y".

   Answer: This one is a little tricky, because it uses the construction "the only value with property P is v" . This construction in English definitions occurs freqeuently, so let us first look at the issue abstractly, and see how to express it using quantifiers. What this is saying is " As a general rule, P is not true. However, there may be one exception v to this rule." Or in other words " The general rule that P is false applies to all elements of the universe that are not equal to v" . Thus, it should be translated as $\forall z[z \neq v \rightarrow \neg P(z)]$. Since this involves a lot of things not being true, it is usually simpler to use the logically equivalent contrapositive format: $\forall z[P(z) \rightarrow z = v]$.
   In this particular case, the property P is "z is a factor of x and z is a factor of y."
   From the above reasoning applied to the English definition, x is relatively prime to $y \equiv \forall z[((z|x) \wedge (z|y)) \rightarrow z = 1]$.

3. Express "All factors of x are also factors of y".
   This predicate of x, y is of the form "All A's are B." In other words, it is a general rule, where the rule is "z is a B", but only holds under the condition that z is an A. In other words, $\forall z$(z is an A) $\rightarrow$ (z is a B). Note that this is quite different from the translation of "Some A's are B's.", which translates to $\exists z$[z is an A$\wedge z$is a B]. In this case, we have $\forall z(z|x \rightarrow z|y)$, since $z|x$ means z is a factor of x.

Epp, Section 2.3, 30 Let $U(x)$ stand for "x understands human nature", $C(x)$ stand for "x is clever", $W(x, y)$ stand for x wrote book y, $S(x)$ for "x can stir the hearts of men", and $T(x)$ for "x is a true poet". The premises are

1. $\forall x(U(x) \rightarrow C(x))$
2. $\forall x(lnot S(x) \rightarrow \neg T(x))$
3. $W(Shakespeare, Hamlet)$
4. $\forall x(\neg U(x) \rightarrow \neg S(x))$
5. $\forall x(\neg T(x) \rightarrow \neg W(x, Hamlet))$

The proof is then

1. $\forall x(U(x) \rightarrow C(x))$
2. $\forall x(lnot S(x) \rightarrow \neg T(x))$
3. $W(Shakespeare, Hamlet)$
4. $\forall x(\neg U(x) \rightarrow \neg S(x))$

5. $\forall x(\neg T(x) \rightarrow \neg W(x, Hamlet))$
6. $T(Shakespeare)$ (3,5, Universal Modus Tollens)
7. $S(Shakespeare)$ (6, 2, Universal Modus Tollens)
8. $U(Shakespeare)$ (7,4, UMT)
9. $C(Shakespeare)$ (1,8, UM Ponens)

So Shakespeare was clever.

program correctness Use the predicates $h(x,t)$ to mean "the program halts on input x after t time steps" and let f be a function from inputs to outputs.

Assume that, for all inputs x, there is some t so that the program halts on x after t time steps, i.e. the program eventually halts on all inputs. Also assume that for all inputs x and times t, if the program halts after t time steps, then it outputs $f(x)$.

Formalize the above assumptions and use them to prove that, on any input x, the program outputs $f(x)$.

(Hint: do not get confused between the VALUE f(x), a number, and the PREDICATE "The program outputs f(x) on input x")

Following the hint, let $outputs(x, y)$ be the predicate, "on input x, the program outputs y." Be very careful to keep track of the *types* of objects or lines in a proof. For example, x is an *input*, $f(x)$ is a possible *output*, and $outputs(x, f(x))$ is a *predicate* in x,i.e. either true or false (possibly) depending on the input x. Make sure that you don't use operations intended for one type of object on another type. It doesn't make sense, for example, to say $f(x) \wedge h(x,t)$, since $f(x)$ is an object (a number, a file, whatever the program is supposed to output), not a fact.

Our premises are:

1. $\forall x[\exists t \;\; h(x,t)]$ and
2. $\forall x \forall t[h(x,t) \rightarrow outputs(x, f(x))]$.

We want to show, $\forall x[outputs(x, f(x))]$.

Discussion: Using the backwards method, we need to prove a universal statement, so we should use a proof by universal generalization. Such a proof begins by picking an arbitrary object of the right type, and showing that the statement is true for that specific but unknown object. So in this case, we want to show $outputs(x_0, f(x_0))$ for an arbitrary but specific input x_0. We then can go forwards by applying universal specification on the premises, using that object as the specific value. To use the second premise this way we would also need a value for t, but conveniently the first premise will give us such a value. This leads to the following proof:

1. $\forall x[\exists t h(x,t)]$ (Premiss)
2. $\forall x \forall t[h(x,t) \rightarrow outputs(x, f(x))]$ (Premise)
3. Let x_0 be an arbitrary input.
4. $\exists t[h(x_0,t)]$ (1, Universal specification $x = x_0$)
5. Pick t_0 so that $h(x_0,t_0)$ (4, Choice)
6. $h(x_0,t_0) \rightarrow outputs(x_0, f(x_0))$ (2, Univ. Spec., $x = x_0, t = t_0$)
7. $outputs(x_0, f(x_0))$ (5,6 Modus Ponens)
8. Since x_0 was arbitrary, $\forall x[outputs(x_0, f(x_0))]$ (3,7, Universal Generalization)

divisibility Prove that, for any integers x and y, if all numbers that divide x also divide y, then x divides y.

Discussion: As in the definitions problem above, we translate our goal as: $\forall x \forall y[(\forall z(z|x \rightarrow z|y)) \rightarrow x|y]$. Now, going backwards, we want to prove a universal statement in x, y, so we want to prove the inside for an arbitrary x_0, y_o. The inside is an implication, so we want to ASSUME the premise $\forall z(z|x_0 \rightarrow z|y_0)$ and prove the conclusion, $x_0|y_0$. To use the premise, we'll need to SPECIFY a value for z. One that matches the conclusion is $z = x_0$, since for that value of z we get $x_0|x_0 \rightarrow x_0|y_0$. To use this to conclude that $x_0|y_0$, we just need to show $x_0|x_0$, but since $x_0 = 1 * x_0$, this is true. This yields the following proof:

1. Let x_0 and y_0 be any positive integers.
2. Assume $\forall z(z|x_0 \to z|y_0)$
3. $x_0|x_0 \to x_0|y_0$ (2, US, $z = x_0$)
4. $x_0 = 1 * x_0$ (Algebra)
5. $\exists z[x_0 = z * x_0]$ (4,Example, z=1)
6. $x_0|x_0$ (5, defn of $|$)
7. $x_0|y_0$ (3,6, MP)
8. Therefore, $\forall z(z|x_0 \to z|y_0) \to x_o|y_0$ (2,7, syll.)
9. $\forall x \forall y[(\forall z(z|x \to z|y)) \to x|y]$. (1,8, Univ. Gen.)

Section 3.5, p. 153 13a.,b. (5 pts. total.) 13a.b. I'm going to be just slightly less formal with this one. We'll use the fact that $d|n \equiv n/d \in Z$ (n/d is an integer) and that $\lfloor x \rfloor \in Z$ for all real numbers x, and that for all $x \in Z$, $\lfloor x \rfloor = x$, since the greatest integer less than an integer is that integer.. a. Assume $d|n$. Then $n/d \in Z$, so $\lfloor n/d \rfloor = n/d$. Multiplying through by d, we get $n = \lfloor n/d \rfloor d$. b. Assume $n = \lfloor n/d \rfloor d$. Since $d \neq 0$, we can divide both sides by d to get $n/d = \lfloor n/d \rfloor \in Z$. Therefore, $n/d \in Z$,so $d|n$.

Epp., Section 5.2, p.301 Problem 13. 13. This statement is always true. We want to show that $A \subseteq B \to (A \cap C) \subseteq (B \cap C)$.

Discussion: Our goal is an implication, so we as always assume the premise $A \subseteq B$ and try to prove the conclusion, $A \cap C \subseteq B \cap C$. To continue to use the backwards forwards method, we translate the set-theory notation using the definitions. $A \subseteq B$ means $\forall x(x \in A \to x \in B)$. Similarly, our goal means $\forall x(x \in A \cap C \to x \in B \cap C)$ So we will need to use universal generalization to prove our goal. Pick x_0 an arbitrary element and prove the inside of our goal for $x = x_0$. This isss an implication, so agian we will assume the hypothesis and try to use that to prove the conclusion. This gives us the following proof:

1. Assume $A \subseteq B$
2. $\forall x[x \in A \to x \in B]$ (1,defn of subset)
3. Let x_0 be any element of the universe.
4. Assume $x_0 \in A \cap C$.
5. $x_0 \in A \wedge x_0 \in C$ (4, defn of $\cap$.)
6. $x_0 \in A \to x_0 \in B$ (2, US, $x = x_0$)
7. $x_0 \in B$ (5,6, MP)
8. $x_0 \in B \wedge x_0 \in C$ (5,7 , CA)
9. $x_0 \in B \cap C$ (8, defn of intersection)
10. $\forall x(x \in A \cap C \to x \in B \cap C)$ (3,9, U. Gen.)
11. $A \cap C \subseteq B \cap C$ (10, def of subset)
12. $A \subseteq B \to A \cap C \subseteq B \cap C$(11, 1, syll.)

Epp 5.2.19 If $A \subseteq B$ then $B^c \subseteq A^c$. Discussion: The overall form is an implication, so we should assume $A \subseteq B$, and then prove $B^c \subseteq A^c$. This last is equivalen to $\forall x(x \in B^c \to x \in A^c)$, so we should prove this using universal generalization. Proof:

1. Assume $A \subseteq B$
2. Let x_0 be any element of the universe.
3. Assume $x_0 \in B^c$.
4. $x_0 \notin B$ (3,defn of complement)
5. $\forall x(x \in A \to x \in B)$ (1,defn of subset)

6. $x_0 \in A \to x_0 \in B$.
7. $x_o \notin A$ (4, 6, Modus Tollens)
8. $x_0 \in A^c$ (7, defn of complement)
9. $x_0 \in B^c \to x_0 \in A^c$ (Assump. 3 implies 8)
10. Since x_0 was arbitrary, $\forall x(x \in B^c \to x \in A^c)$ (2,9, Univ. Gen.)
11. Therefore, $A \subseteq B \to B^c \subseteq A^c$. (Assump. 1 implies line 10)