1 Proof of set properties, concluded

We can use logic to describe set properties in interesting ways, by associating statements with membership of a named object x in the various sets. Let us consider giving specific names to statements asserting membership, i.e. for sets A and B, let P be the statement $x \in A$, and Q be the statement $x \in B$. Then, we can translate many statements about sets to logical combinations of these statments.

In particular, the statement $A \subseteq B$ asserts that for any $x \in A$, it follows that $x \in B$; in other words, as long as P is true, Q must be true, which logically is equivalent to the statement $P \Rightarrow Q$. From this equivalency it's easy to derive that the statement $A = B$ is equivalent to asserting that both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true, or in other words asserting that $P \Leftrightarrow Q$ is true. We have simple ways of describing membership in the set operations as well: the assertion that $x \in A \cup B$, is equivalent to asserting that either $x \in A$ or $x \in B$; in terms of our statements, this would be $P \vee Q$. Likewise, $x \in A \cap B$ can be shown to equate to $P \wedge Q$, and $x \in A - B$ equates to $P \wedge \neg Q$. Using rephrasing of set-membership as logical statements, we have a more tidy way to prove the proposition from last week.

Proposition 1. *For any sets A, B, and C, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.*

Proof. For an arbitrary x, let us consider the statement $x \in A \cup (B \cap C)$. By expanding the meaning of membership in a union, this is equivalent to the logical statement $(x \in A) \vee (x \in B \cap C)$; the membership in an intersection displayed here expands to $(x \in A) \vee [(x \in B) \wedge (x \in C)]$. Let us denote the statements $x \in A$, $x \in B$, and $x \in C$, for brevity, as P, Q, and R respectively. Thus, the statement asserting membership of x in $A \cup (B \cap C)$ is logically equivalent to $P \vee (Q \wedge R)$.

Now let us consider the statement $x \in (A \cup B) \cap (A \cup C)$. Again we expand the definition of membership in an intersection to find that this statement is logically equivalent to $(x \in A \cup B) \wedge (x \in A \cup C)$; expanding each of these intersections yields equivalence of the above statements to $[(x \in A) \vee (x \in B)] \wedge [(x \in A) \vee (x \in C)]$, or, more succinctly, $(P \vee Q) \wedge (P \vee Q)$.

Note that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ is equivalent to the assertion that $[x \in A \cup (B \cap C)] \Leftrightarrow [x \in (A \cup B) \cap (A \cup C)]$ is always true. Since each of these has itself been expressed as a propositional-calculus statement in terms of the statements P, Q, and R, the desired result is logically equivalent to the specific statement:

$$[P \vee (Q \wedge R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$$

which we can demonstrate to be tautological with a particularly wearisome truth table:

P	Q	R	$P \vee (Q \wedge R)$	$(P \vee Q) \wedge (P \vee R)$	$[P \vee (Q \wedge R)] \Leftrightarrow [(P \vee Q) \wedge (P \vee R)]$
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	T	T	T
F	T	F	F	F	T
F	F	T	F	F	T
F	F	F	F	F	T

Since our assertion which was demonstrated to be logically equivalent to the statement to be proven is true, the proof is complete. □

2 Proof by contradiction

So far we have seen two proof techniques for proving a statement of the form $P \Rightarrow Q$:

Direct proof Assume P; argue by logical steps to Q.

Contrapositive Assume $\neg Q$; argue by logical steps to $\neg P$.

However there is a third technique, which shares particular elements with the contrapositive. Recall that, in order to show that $P \Rightarrow Q$, all we *really* need to do is ensure that the prospect that P is true and Q is false cannot occur. One easy way to show that something *cannot occur* is to show that it leads to a contradiction, which gives us our third method:

Contradiction Assume that both P and $\neg Q$ are true; argue by logical steps to a universally false statement (i.e. a contradiction).

This is both a very powerful technique (since we start with both P and $\neg Q$ in our premise toolbox) and a fun one (since the argument to a false statement often takes us from the sublime to the ridiculous). We can in fact dispense with the implication entirely, and if we wish to prove a single statement R, we can argue from $\neg R$ to a contradiction.

We can start with a cute, simple result on the real numbers.

Proposition 2. *There is no positive real number which is less than every other positive real number.*

Proof. We prove this result by contradiction. Let us thus suppose that there is a smallest positive real number, which we shall call x; thus since $\frac{x}{2}$ is positive, $\frac{x}{2}$ cannot be less than x, so $\frac{x}{2} \geq x$. Multiplying both sides of this inequality by the positive quantity $\frac{2}{x}$, we get the result $2 \geq 1$, a patent absurdity. □

The most straightforward exhibit of this powerful technique is a classic proof, attributed to an unknown Pythagorean, possibly Hippasus. We shall start with a simple lemma, previously presented in a different form:

Lemma 1. *For an integer n, $2 \mid n^2$ if and only if $2 \mid n$.*

Proof. The implication in one direction is easy: if $2 \mid n$, then n is equal to $2k$ for some integer k, so $n^2 = (2k)^2 = 2(2k^2)$, so n^2 is also even.

In the opposite direction, however, we are given that $2 \mid n^2$. Thus $n \cdot n = 2k$ for some integer k. Since any two equal multiplications of integers can be broken down into prime terms and recombined, then there must be a decomposition of $n^2 = pqrs$ with p, q, r, and s positive integers such that $pq = n$, $rs = n$, $pr = 2$, and $qs = k$. We shall specifically focus on the fact that $pr = 2$: since 2 is prime and $p \mid 2$, we know that either $p = 2$ (in which case $r = 1$) or $r = 2$ (in which case $p = 1$). In the first case, $n = pq = 2q$, so $2 \mid n$; in the second, $n = rs = 2s$, so $2 \mid n$, so it must follow that $2 \mid n$. □

There is a much easier proof of this using the contrapositive and a consideration of the square of an odd itneger, but this result is more generalizable to divisors other than 2 (and thus more relevant to the problem set!).

Theorem 1. *The square root of 2 is irrational.*

Proof. The statement could be rephrased as an explicit implication: if $x^2 = 2$, then x is irrational. Let us proceed by contradiction, and take as our premise the statement that $x^2 = 2$ and x is not irrational (i.e., x is rational). Then, by the definition of a rational number, x may be expressed as a fraction $\frac{p}{q}$ in lowest terms; that is, $x = \frac{p}{q}$ where p and q are integers sharing no divisors greater than 1. Since $2 = x^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$, we may see that $p^2 = 2q^2$. Thus $2 \mid p^2$, and from the above lemma $2 \mid p$; let $p = 2k$. Then $(2k)^2 = 2q^2$, which simplifies algebraically to $2k^2 = q^2$. Thus $2 \mid q^2$, so $2 \mid p$. However, since both p and q are divisible by 2, our presumption that $\frac{p}{q}$ is in lowest terms is directly contradicted. □