Some Proof Techniques

There are many different techniques that can be used to prove a statement. While they are each equally worthy of proving a statement, some may be easier to use than others in a given scenario. Below is a list of several standard proof techniques that are commonly used to prove statements along with some examples of a given technique in a action. Most of the following exposition is taken directly from a book entitled,

A Transition to Advanced Mathematics (Third Edition) by Douglas Smith, Maurice Eggen, and Richard St.Andre.

(1) **Direct Proof :**

Direct Proof of $\mathbf{P \Rightarrow Q}$

Assume P.

$\vdots$

Therefore, Q.

Thus, $P \Rightarrow Q$.

Example : Suppose $x \in \mathbb{Z}$ (that is, x is an integer). Prove that if x is odd, then $x+1$ is even.

Proof. Assume that x is odd.
Then $x = 2k+1$ for some integer k.
Thus, $x+1 = (2k+1)+1 = 2(k+1)$ for some integer k.
Since $x+1$ is twice the integer $k+1$, it follows that $x+1$ is even. $\square$

Example : If x and y are odd integers, then xy is odd.

Proof. Assume x is odd and y is odd. Then, integers m and n exist so that $x = 2m+1$ and $y = 2n+1$. Thus, $xy = (2m+1)(2n+1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$. Thus xy is an odd integer. $\square$

(2) **Contrapositive :** Remember that we proved using truth tables that the statement $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$. So, if we want to prove the statement $P \implies Q$ it suffices to use a direct proof to prove $\sim Q \Rightarrow \sim P$. It seems like this is a little bizarre but it can be *very* helpful. Try to prove the example below directly and notice that it is a lot more tricky than using the contrapositive proof.

Contraposition Proof of $\mathbf{P} \Rightarrow \mathbf{Q}$

Suppose $\sim Q$.

$\vdots$

Therefore, $\sim P$ (via a direct proof).

Thus, $\sim Q \Rightarrow \sim P$.

Therefore, $P \Rightarrow Q$.

Example : Let m be an integer. Prove that if m^2 is odd, then m is odd.

Proof. Suppose that m is not odd. <*Suppose* $\sim Q$.> Then m is even. Thus, $m = 2k$ for some integer k. Then $m^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since m^2 is twice the integer $2k^2$ it follows that m^2 is even. <*Deduce* $\sim P$.> Thus, if m is even, then m^2 is even; so, by contraposition, if m^2 is odd, then m is odd. $\square$

Example : If x and y are odd integers, then xy is odd.

Proof. <*To prove (x is odd $\wedge$ y is odd)$\Rightarrow$ xy is odd, we show xy is even $\Rightarrow$ (x is even $\vee$ y is even).*> Assume xy is even. Thus, 2 is a factor of xy. But since 2 is a prime number and 2 divides the product xy, then either 2 divides x or 2 divides y. < *We use a well-known fact about the division of a product by a prime.*> Thus, either x is even or y is even. We have shown that if xy is even then either x is even or y is even. Thus, if x and y are odd, then xy is odd. $\square$

(3) **Contradiction :** Proofs by contradiction tend to have a similar feel to a proof by contrapositive. The idea is that we want to prove some statement R, so we show that the statement $\sim R$ is always false. Then, we have shown $R \equiv \sim (\sim R) = \sim (F) = T$.

Proof of R by contradiction

Suppose $\sim R.$

$\vdots$

Therefore, $S.$

$\vdots$

Therefore, $\sim S.$

Hence, $S \wedge \sim S,$ a contradiction.

Thus, $R.$

I should take the time to note that many times the proposition R will be an implication. In that case the we assume $\sim (P \Rightarrow Q)$ and deduce a contradiction. Recall that the negation of an implication is $\sim (P \Rightarrow Q) \equiv P \wedge \sim Q$.

Example : Prove that $\sqrt{2}$ is an irrational number.

Proof. Suppose that $\sqrt{2}$ is a rational number. $<$ *Assume* $\sim P.$ $>$ Then $\sqrt{2} = s/t$, where s and t are integers. Thus, $2 = s^2/t^2$, and $2t^2 = s^2$. Since s^2 and t^2 are squares, s^2 contains an even number of $2'$s as factors. $<$*This is our S statement.*$>$, and t^2 contains an even number of $2'$s. But then $2t^2$ contains an odd number of $2'$s as factors. Since $s^2 = 2t^2$, s^2 has an odd number of $2'$s. $<$*This is the statement* $\sim S$.$>$ This is a contradiction. We conclude that $\sqrt{2}$ is irrational. □

Example : If x and y are odd integers, then xy is odd.

Proof. Suppose x and y are odd and xy is even. Since x and y are odd, then $x = 2m + 1$ and $y = 2n + 1$ for some integers m and n. Thus, $xy = (2m + 1)(2n + 1) = 2(2mn + m + n) + 1$. Then $2(2mn+m+n)$ is even and the next integer $2(2mn+m+n)+1 = xy$ is even because we assumed xy was even. This is impossible since there are no two consecutive integers that are both even. Because the supposition that xy leads to a contradiction, we conclude that xy is odd. □

(4) **Existential Statement :** The most direct approach is to find an element that satisfies the statement. For example, to prove that the number 4294967297 is not a prime to prove the statement there exists an nonzero integer $x \neq 1$ so that x divides 4294967297. We can prove this directly by noticing that $4294967297 = 641 \cdot 6,700,417$. That is we found an x (actually we found 2 such x's) that divides 4294967297. How did we get the number? Who knows, but we found it. Many times a proof by contradiction is more helpful.

Proof of $\exists \mathrm{xP}(\mathrm{x})$ by contradiction

Suppose $\sim (\exists x P(x))$.

Then, $\forall x \sim P(x)$.

$\vdots$

Therefore , $S \wedge \sim S,$ a contradiction.

Hence, $\sim (\exists x P(x))$ is false; so $\exists x P(x)$ is true.

Example : Prove that the polynomial $p(x) = x^{71} - 2x^{39} + 5x - 1$ has a real zero.

Proof. Suppose that there is no such x. By the fundamental theorem of algebra we know that the polynomial has exactly 71 roots, some may be complex roots and some may be real roots. It is a fact that complex roots always come in pairs. That is if $a + bi$ is a root of $p(x)$ then $a - bi$ must also be a root. SO, it there are no real roots then that means that they must all be complex roots. Since they are all complex roots, there must be an even number of roots. 71 ain't even so this is a contradiction. Therefore, there must be at least one real root. $\square$

(5) **Existential Implications :**

Direct proof of $\exists \mathbf{x} \mathbf{P}(\mathbf{x}) \Rightarrow \mathbf{R}$

Assume $\exists x P(x)$.

Let t be an object such that $P(t)$ is true.

$\vdots$

Therefore , R.

Hence, $\exists x P(x) \Rightarrow R$.

Example : If there exists a test score of yours that is a zero, then you can not make an A in the course.

Proof. Suppose that one of your test grades is a zero. Then since there are only three in class exams this means that your test average is at most $66.\bar{6}\%$. Since your test average accounts for 45% of your grade this will only allow for $(66.\bar{6})(0.45) = 30$ points of your final grade to come from tests instead of the maximum of 45. So, the highest grade that could be earned is an 85% which is not sufficient for an A. $\square$

This begs the use of some terminology we talked about at the beginning of class that we have not used yet. Recall that a corollary is in immediate result of a theorem. Many times corollaries are immediate from the proof of a theorem, as is the case with the following,

Corollary 1. *If your test average is less than or equal to* $66.\bar{6}\%$ *you can not earn an A.*

(6) **Universal Proposition :**

Direct proof of $\forall \mathbf{x} \mathbf{P}(\mathbf{x})$

Let x be any arbitrary element in the universe of discourse.

(The universe should be named or its objects described.)

$\vdots$

Hence , $P(x)$ is true.

Since x was arbitrary, $\forall x P(x)$ is true.

Example : For all even integers x its square, x^2, is even.

Proof. Let x be any even integer. Then $x = 2k$ for some k. So, $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$, so x^2 is even. Since our choice of even integer was arbitrary, we deduce that the square of any even integer is an even integer. $\square$

(7) **Universal Proposition (Contradiction) :**

Proof of $\forall \mathbf{x} \mathbf{P}(\mathbf{x})$ by contradiction.
Suppose $\sim \forall x P(x)$.
Then $\exists x \sim P(x)$.
Let t be an object such that $\sim P(t)$.

$\vdots$

Therefore, $S \wedge \sim S$.
Thus, $\exists x \sim P(x)$ is false; so its denial $\forall x P(x)$ is true.

(8) **Uniqueness :**

Proof of $\exists!\mathbf{x}\mathbf{P}(\mathbf{x})$.
Prove that $\exists x P(x)$ is true by any method *first*.
Then assume that t_1 and t_2 are objects in the universe such that $P(t_1)$ and $P(t_2)$ are true.

$\vdots$

Therefore, $t_1 = t_2$.
We conclude, $\exists! x P(x)$.

Example : The polynomial $r(x) = x - 3$ has a unique zero.

Proof. First, observe that $r(3) = 3 - 3 = 0$. So, 3 is a zero of $r(x)$, so we have shown that there exists a zero of $r(x)$. It remains to show that there is a unique zero. So, suppose that t_1 and t_2 are zeros of $r(x)$. Then,

$$\begin{aligned} r(t_1) &= 0 = r(t_2) \\ \Rightarrow r(t_1) &= r(t_2) \\ \Rightarrow t_1 - 3 &= t_2 - 3 \\ \Rightarrow t_1 - 3 + 3 &= t_2 - 3 + 3 \\ \Rightarrow t_1 &= t_2. \end{aligned}$$

Therefore, $r(x)$ has a unique zero. $\square$