REVIEW OF MATHEMATICAL PROOFS
415G 001 COMBINATORICS AND GRAPH THEORY

1. What is the purpose of a mathematical proof?

The purpose of a proof in mathematics is to assert the veracity/falsity of a logical statement (one that can be assigned the value of True/False) by means of a deductive exercise that starts with a set of axioms (statements that are assumed to be true without dispute) and other theorems (statements that have been proven true by the same deductive method within the same set of axioms). In the sciences (Physics, Chemistry, Social sciences, etc.) statements are not being proved but instead evidence is collected to increase its support. For example, in the scientific method we look to falsify a scientific hypothesis using any of its falsifiable conclusions and when the hypothesis is not falsified then it acquires greater support from the scientific community. A mathematical statement cannot be proven by gathering evidence that it holds in certain cases. However a mathematical statement can be proven false by showing a single example where the statement does not hold (a counterexample). So there is an asymmetry between proving a statement true or false. Showing that a statement is false is in general "easier" since normally amounts to exhibit a counterexample, on the other hand showing that a statement is true requires to prove it holds for every possible case. Of course a statement is either true or false and it is impossible to prove the opposite.

Example 1.1. Statement: Every natural number is divisible by 2. **Counterexample:** 3 is a natural number and 2 does not divide 3 hence the statement is false.

2. What to take into account when writing a mathematical proof?

(1) Remember that you write a proof to be read by someone else. So you need to take into account what is the background of your intended audience. For $415G$ you should assume that any of your fellow classmates will be reading your proof and should be able to understand it.
(2) Have very clear what is the statement that you are intending to prove and what is the technique or method that you are going to use to prove it. A useful approach is to put in writing at the beginning of your proof what are you going to show and how this will imply your theorem.
(3) State clearly what are the axioms and theorems that you are assuming to be true in your proof.
(4) Be clear, organized and frugal in your exposition: do more with less (but without sacrificing correctness and readability).
(5) Introduce all the notation that you are going to use unless it is widely known to all of your audience (this is almost never the case).
(6) Use delimiters that indicate to the reader whether you are stating a theorem, proving it or simply providing context to the reader. Use words like Theorem, Lemma, Proposition, Claim and Proof. It is a common practice to use some symbol to denote when a proof is finished. Probably the most common is the use of the "Halmos symbol" $\square$ at the end of a proof.

3. Proof techniques

We recall some of the most commonly used proof principles and techniques.

3.1. **Mathematical induction.** This is one of the most commonly used proof techniques in mathematics. We want to prove a statement of the form $P(n)$ that holds for every number $n \geq n_0$ where n_0 is a fixed natural number. For example the statement

$$P(n) : \forall n \geq 1 \left[\quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \right].$$

The technique involves two steps:

(1) **Initial step:** Prove that $P(n_0)$ is true for the minimal number n_0.
(2) **Inductive step:** Show that whenever $P(n-1)$ is true then $P(n)$ is also true.

Example 3.1. For the example above we have

(1) **Initial step:**

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}.$$

(2) **Inductive step:** Assume that $P(n-1)$ is true, that is

$$\sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}.$$

Then

$$\begin{aligned}
\sum_{i=1}^{n} i &= \sum_{i=1}^{n-1} i + n \text{ using the definition of } \sum \\
&= \frac{(n-1)n}{2} + n \text{ using the induction hypothesis} \\
&= \frac{(n-1)n + 2n}{2} \text{ using the properties of } \mathbb{R} \text{ as a field} \\
&= \frac{n(n+1)}{2}.
\end{aligned}$$

Hence by the principle of mathematical induction $P(n)$ is true for all $n \geq 1$.

Nonexample 3.2. Prove that

$$P(n) : \forall n \geq 1 \left[\quad \sum_{i=1}^{n} i = \frac{n^2+n+2}{2} \right].$$

(1) **Inductive step:** Assume that $P(n-1)$ is true, that is

$$\sum_{i=1}^{n-1} i = \frac{(n-1)^2 + (n-1) + 2}{2}.$$

Then

$$\begin{aligned}
\sum_{i=1}^{n} i &= \sum_{i=1}^{n-1} i + n \text{ using the definition of } \sum \\
&= \frac{(n-1)^2 + (n-1) + 2}{2} + n \text{ using the induction hypothesis} \\
&= \frac{n^2 - 2n + 1 + n - 1 + 2 + 2n}{2} \text{ using the properties of } \mathbb{R} \text{ as a field} \\
&= \frac{n^2 + n + 2}{2}.
\end{aligned}$$

Then the principle of mathematical induction would "imply" that $P(n)$ is true for all $n \geq 1$. Clearly this cannot be possible since it is not true that

$$\frac{n(n+1)}{2} = \sum_{i=1}^{n} i = \frac{n^2+n+2}{2}.$$

The problem is indeed that we missed to check that the hypothesis is true for the initial value of n. In fact,

$$1 \neq \frac{1^2+1+2}{2}.$$

This example illustrates that both the initial step and the inductive step are require to hold in order for an induction proof to be valid.

3.1.1. *Strong induction.* A slight modification of the principle above requires that we only prove the following:

(1) **Inductive step:** Show that for all $n \geq n_0$ if $P(k)$ is true for all the values of k such that $n_0 \leq k < n$ then $P(n)$ is also true.

Remark 3.3. Note that the statement above has to be proven for all $n \geq n_0$, including the initial value n_0. So it does not mean that in this form of the principle of induction initial values are not checked.

Example 3.4. A natural number $n \geq 2$ is said to be *prime* if whenever we express n as $n = ab$ then either $a = n$ or $b = n$. If $n \neq 1$ is not prime then is said to be *composite*. Prove that any natural number $n \geq 2$ can be expressed as a product of primes.

$$P(n) : \forall n \geq 2 \left[n = p_1 p_2 \cdots p_k \text{ where } p_i \text{ is prime } \forall i \right].$$

(1) **Inductive step:** Let $n \geq 2$ and assume that any k such that $2 \leq k < n$ is a product of primes.
   There are two cases:
   - If n is prime then trivially n is a product of 1 prime.
   - If n is not prime then n can be expressed as $n = n_1 n_2$ where n_1 and n_2 are not n and so $n_1 < n$ and $n_2 < n$. But then by the inductive hypothesis both n_1 and n_2 are products of primes and so it is n.

   These two cases cover all possible values of n with $n \geq 2$. Then by strong induction $P(n)$ is true for all $n \geq 2$.

3.2. **Constructive and nonconstructive proofs.** Sometimes we want to show that certain mathematical object with certain given properties *exists* (we want to prove *existence).* The purpose of a *constructive proof* is to show explicitly that such an object exists. On the other hand, if we are able to show that such an object must exist without explicitly exhibiting it, such a proof is said to be *nonconstructive.*

Example 3.5. Statement: There exists a pair of irrational numbers a and b such that a^b is rational.

- **Nonconstructive proof:** Let $a = b = \sqrt{2}$. If $a^b = \sqrt{2}^{\sqrt{2}}$ is not rational then we instead let $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$. We have that $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ that is rational. Note that we never concluded if our example for the theorem was $a = b = \sqrt{2}$ or $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.
- **Constructive proof:** Let $a = \sqrt{3}$ and $b = \log_3 4$. Note that b is irrational since otherwise $\log_3 4 = \frac{p}{q}$ for nonzero integers p and q and hence $4 = 3^{\frac{p}{q}}$ or $4^q = 3^p$ which is a contradiction. But then $a^b = \sqrt{3}^{\log_3 4} = 2$ that is rational. Note that here we explicitly showed a pair of objects that make the statement true.

3.3. **Proof by contradiction.** In a proof by contradiction we suppose (as if it were an additional axiom) that the statement P is false (not P is true) and look for deriving a contradiction. If we arrive to a contradiction this means that our initial supposition was wrong.

Example 3.6. Theorem: There are infinitely many prime numbers.

Proof: Suppose that the statement is false, that is, we assume that there are finitely many prime numbers $p_1, p_2, \ldots, p_k$. Now consider the number $m = p_1 p_2 \cdots p_k + 1$. None of $p_1, p_2, \ldots, p_k$ divides m that is a contradiction with the fact that m is a product of primes (we know this by our previous theorem). Then our supposition that there are finitely many prime numbers must be incorrect and the theorem is proved.

Example 3.7. Theorem: $\sqrt{2}$ is irrational.

For the proof we will assume that the following lemma has been proven.

Lemma 3.8 (Euclid's lemma)**.** *If p is a prime number and $p|ab$ then $p|a$ or $p|b$.*

Proof: Suppose that $\sqrt{2}$ is not irrational then $\sqrt{2} = p/q$ for some integers p and q that we can choose to be relatively prime ($\gcd(p, q) = 1$). Then $2 = p^2/q^2$ or $2q^2 = p^2$ implies $2|p$ (Euclid's lemma) and so $p = 2k$ for some k. But then $2q^2 = (2k)^2 = 4k^2$ or $q^2 = 2k^2$ and $2|q$ contradicting the fact that $\gcd(p, q) = 1$. Then $\sqrt{2}$ must be irrational.

3.4. **Contrapositive.** Sometimes when we want to prove a statement of the form "If P then Q" we can prove instead the logically equivalent statement "If Q is not true then P is not true".

Example 3.9. Statement: If the power set $\mathcal{P}(A) := \{B \mid B \subseteq A\}$ of a set A is finite then A is finite.

Contrapositive: If A is not finite then its power set $\mathcal{P}(A)$ is not finite.

Contrapositive(rephrased): If A is infinite then its power set $\mathcal{P}(A)$ is infinite.

Note that in this case the contrapositive is a bit easier to prove since there is an injective map $\phi : A \to \mathcal{P}(A)$ given by $a \mapsto \{a\}$ and so $|A| \leq |\mathcal{P}(A)|$.

3.5. **Uniqueness.** It is common in mathematics that we need to show that certain object (that we have already shown that exists either constructively or not) it is the unique object with its properties.

Example 3.10. Statement Show that the unique factorization $n = p_1 p_2 \cdots p_k$ is unique up to reordering of the prime factors.

Proof Assume that n is minimal with the property of having two different factorizations $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r$. Then $p_1 | q_1 q_2 \cdots q_r$ and using Euclid's lemma we conclude that p_1 divides some q_j and by reindexing we can assume without loss of generality that $p_1 | q_1$ and so $p_1 = q_1$. Now dividing n by $p_1 = q_1$ we have that $\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_r$. By the minimality of n (Strong induction) we have that any factorization of $\frac{n}{p_1}$ is unique so we have that $k - 1 = r - 1$ and after reindexing that all the primes $p_i = q_i$ for $i \geq 2$. Hence the prime factorization of n is unique up to reordering.

References

[1] Ralph P Grimaldi. *Discrete and Combinatorial Mathematics: An Applied Introduction, Fifth Edition.* Addison-Wesley, 2003.

[2] Michael Hutchings. Introduction to Mathematical Arguments. `https://math.berkeley.edu/~hutching/teach/proofs.pdf`. [Online; accessed 18-August-2015].

[3] Alan Tucker. *Applied combinatorics.* John Wiley & Sons, Inc., New York, third edition, 1995.

[4] Wikipedia. Constructive proof — Wikipedia, The Free Encyclopedia, 2015. [Online; accessed 10-August-2015].

[5] Wikipedia. Mathematical induction — Wikipedia, The Free Encyclopedia, 2015. [Online; accessed 10-August-2015].