http://www-math.ucdenver.edu/~wcherowi/courses/m3000/lecture3a12.pdf

Proof Methods

What is a proof?

Proofing as a social process, a communication art.

Theoretically, a proof of a mathematical statement is no different than a logically valid argument starting with some premises and ending with the statement. However, in the real world such logically valid arguments can get so long and involved that they lose their "punch" and require too much time to verify.

In mathematics, the purpose of a proof is to *convince* the reader of the proof that there is a logically valid argument in the background. Both the writer and the reader must be convinced that such an argument can be produced – if needed.

What is a Proof?

Writing mathematical proofs is therefore an art form (the art of convincing) and a social process since it is directed at people (the readers).

A mathematical proof of a statement strongly depends on who the proof is written for. Proofs for a research audience are quite different from those found in textbooks. And even textbook proofs look different depending on the level of the audience (high school vs. college vs. graduate school).

To simplify our task in this course, you will write all of your proofs with a specific audience in mind:

ME!

What is a Proof?

That is, you are writing to convince me that you could drop down to the logic level and provide all the details, if I asked you to do so.

Rigor in proofs.

The above remarks should not be construed to mean that you can get sloppy with your proofs – your audience requires clarity, precision and, above all, correctness.

Phrases such as "clearly" or "it is easy to see that" are neither clear nor easy for this audience.

When you say something follows from a definition, I want to know "the definition of what?"

General Hints

The importance of definitions.

It can not be overemphasized how important definitions are. Without a clear and crisp understanding of a definition, you will not be able to use it in a proof. You have to be able to recall a definition precisely when it is needed – vague familiarity will not work for you.

Working backwards.

There is a big difference between discovering a proof and presenting a proof. In presenting a proof you must be convincing, and things need to follow in a logical order. To discover a proof, you are under no such restrictions and often the best procedure is to work the problem backwards.

Methods of Proof

We will survey the basic proof methods. In doing so, our examples to illustrate the techniques should not be very complicated ... so we will restrict them to fairly simple statements which do not need a great deal of background to understand.

The Theory of Numbers provides an excellent source for such examples ... so most of our examples will deal with numbers in this section. Remember that our aim is not to learn more about the theory of numbers, most of the examples will be statements that you know are true, rather we are interested in the way that the proofs are constructed... so, concentrate on the techniques.

Direct Proof

In a direct proof one starts with the premise (hypothesis) and proceed directly to the conclusion with a chain of implications. Most simple proofs are of this kind.

Definitions:

An integer n is ***odd*** iff there exists an integer k so that $n = 2k+1$.

An integer n is ***even*** iff there exists an integer s so that $n = 2s$.

Example of a direct proof:

If n is an odd integer then n^2 is odd.

Pf: Let n be an odd integer.

There exists an integer k so that $n = 2k+1$.

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \Rightarrow n^2 = 2(2k^2 + 2k) + 1$

Since $2k^2 + 2k$ is an integer, n^2 is odd.

The Empty Set

We will use a direct proof here ... but later we will use another technique to prove this.

Thm: *The empty set is unique*.

Pf: Suppose that A and B are empty sets.
Since A is an empty set, the statement $x \in A$ is false for all x, so $(\forall x)(x \in A \Rightarrow x \in B)$ is true! That is, $A \subseteq B$.
Since B is an empty set, the statement $x \in B$ is false for all x, so $(\forall x)(x \in B \Rightarrow x \in A)$ is also true. Thus, $B \subseteq A$.
Since $A \subseteq B$ and $B \subseteq A$ we have $A = B$. ❑

Contrapositive Proof

When proving a conditional, one can prove the contrapositive statement instead of the original – this is called a ***contrapositive proof***. It is still a direct proof method.

Example:

If n^2 is an odd integer, then n is odd.

Pf: Suppose n is an even integer.

There exists an integer k so that $n = 2k$.

$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$

Since $2k^2$ is an integer, n^2 is even.

The Universal Subset

Thm: *The empty set is a subset of every set.**

Pf: Let A be a set.
Since $x \in \varnothing$ is false for all x,
$(\forall x)(x \in \varnothing \Rightarrow x \in A)$ is true.
Thus, $\varnothing \subseteq A$.
Since A was arbitrary, $\varnothing$ is a subset of every set. ❑

* Observe that the statement is a quantified statement:

$(\forall A, A \text{ a set})(\varnothing \subseteq A)$

To prove a "for all" statement, one starts with an arbitrary element of the universe for the variable ... assuming no properties other than membership, and show that the statement is true for it.

Another For All Theorem

Thm: *For every set A, $A \subseteq A$.*

Pf: Let A be an arbitrary set.

Since $x \in A \Rightarrow x \in A$ for all x (whether $x \in A$ is true or not)

$(\forall x)(x \in A \Rightarrow x \in A)$ is true.

So, $A \subseteq A$ for all sets A. ❑

Transitivity

Thm: Let A, B and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Pf: Let $x \in A$.

Since $A \subseteq B$, $x \in B$.

Since $B \subseteq C$, $x \in C$.

Thus, for all x, $x \in A \Rightarrow x \in C$.

So, $A \subseteq C$. ❑

We refer to this result as the "transitivity of subset inclusion".

Contradiction Proofs

This proof method is based on the Law of the Excluded Middle. Essentially, if you can show that a statement can not be false, then it must be true. In practice, you assume that the statement you are trying to prove is false and then show that this leads to a contradiction (any contradiction).

This method can be applied to ***any type of statement***, not just conditional statements.

There is ***no way to predict*** what the contradiction will be.

Contradiction Proof

Definition: A real number r is ***rational*** iff it can be written as r = a/b with a and b integers and b ≠ 0. A real number is ***irrational*** if it is not rational.

Example:

The $\sqrt{2}$ is irrational.

Pf: BWOC assume that $\sqrt{2}$ is rational.
There exist integers p and q so that $\sqrt{2} = p/q$.
We may assume that the fraction is reduced,
i.e. no integer divides both p and q.
$2 = p^2/q^2 \Rightarrow 2q^2 = p^2$, so p^2 is even.
Thus, p is even.

$\sqrt{2}$ is irrational

There exists an integer k so that $p = 2k$.

$2q^2 = p^2 = (2k)^2 = 4k^2 \Rightarrow q^2 = 2k^2$.

So, q^2 is even and therefore q is even.

Since 2 divides both p and q we have a contradiction

$\rightarrow\leftarrow$

So, $\sqrt{2}$ is not rational.

This proof is due to Euclid, but the theorem dates back to Pythagoras and the Pythagorean brotherhood.

The method is wide-spread and is often found in short segments of larger proofs.

The Empty Set

Thm: *The empty set is unique*.

Pf: BWOC suppose that A and B are distinct empty sets.
Since A is an empty set, the statement $x \in A$ is false for all x, so $(\forall x)(x \in A \Rightarrow x \in B)$ is true! That is, $A \subseteq B$.
Since B is an empty set, the statement $x \in B$ is false for all x, so $(\forall x)(x \in B \Rightarrow x \in A)$ is also true. Thus, $B \subseteq A$.
Since $A \subseteq B$ and $B \subseteq A$ we have $A = B$. $\rightarrow\leftarrow$ ❑

The contradiction method in this case does not add anything to the argument, it just puts an unnecessary layer over the basic direct method ... this is not wrong, its just in bad taste!!

Proofs of Biconditionals

A proof of a $P \Leftrightarrow Q$ statement usually uses the tautology

$$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

That is, we prove an iff statement by seperately proving the "if" part and the "only if" part.

Example:

Integer a is odd if and only if a+1 is even.

Pf: (Sufficiency, if a is odd then a+1 is even)

Suppose a is an odd integer.

There exists an integer k so that $a = 2k + 1$.

$a+1 = (2k+1) + 1 = 2k+2 = 2(k+1)$

Since k+1 is an integer, a+1 is even.

Proofs of Biconditionals

Example:

Integer a is odd if and only if a+1 is even.

Pf: (Necessity, if a+1 is even then a is odd)

Suppose a+1 is an even integer.

There exists an integer k so that $a+1 = 2k$.

$a = a + 1 - 1 = (2k) - 1 = (2(k-1) + 2) - 1 = 2(k-1) + 1$

Since k-1 is an integer, a is odd.

Power Sets

Thm: If a set S has n elements then $\mathcal{P}(S)$ has 2^n elements.

We will provide at least two proofs of this important result in later sections when we talk about the techniques used.

Examples:

If $S = \varnothing$ then $\mathcal{P}(\varnothing) = \{\varnothing\}$ which is **not** the empty set!

S contains 0 elements, and $\mathcal{P}(\varnothing)$ has $2^0 = 1$ element.

If $S = \{a\}$, then $\mathcal{P}(S) = \{\varnothing, \{a\}\}$ and has $2^1 = 2$ elements.

If $S = \{a,b\}$ then $\mathcal{P}(S) = \{\varnothing, \{a\}, \{b\}, \{a,b\}\}$ and has $2^2 = 4$ elements.

Power Sets

Thm: Let A and B be sets. Then $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Pf: ($\Rightarrow$ Sufficiency)

Let $C \in \mathcal{P}(A)$, then $C \subseteq A$.

Since $A \subseteq B$ we have by transitivity that $C \subseteq B$.

Thus, $C \in \mathcal{P}(B)$.

Since C was arbitrary, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

($\Leftarrow$ Necessity)

Let $x \in A$. Then $\{x\} \subseteq A$.

Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, $\{x\} \in \mathcal{P}(B)$, so $\{x\} \subseteq B$.

Thus $x \in B$, and since x was arbitrary, $A \subseteq B$. ❑

Both parts of this proof illustrate the method of "***element chasing***" used frequently in proofs involving sets.

Power Sets

Thm: Let A and B be sets. Then $A \subseteq B$ iff $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

An alternate proof the the necessity of this theorem can be given which does not involve element chasing:

($\Leftarrow$ Necessity)

Since $A \in \mathcal{P}(A)$ and $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, we have that $A \in \mathcal{P}(B)$.

Thus, $A \subseteq B$. ❑

Compare this with the previous proof:

($\Leftarrow$ Necessity)

Let $x \in A$. Then $\{x\} \subseteq A$.

Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, $\{x\} \in \mathcal{P}(B)$, so $\{x\} \subseteq B$.

Thus $x \in B$, and since x was arbitrary, $A \subseteq B$. ❑

Uniqueness Proofs

Proofs of existentially quantified statements ($\exists x\ P(x)$) can be constructive – in which case you produce an x which makes P(x) true, or non-constructive – when you use contradiction to show that $\sim(\exists x\ P(x))$ is false.

Definition: To say that there is one and only one x which makes the predicate P(x) true, we write ($\exists! x\ P(x)$) (there exists a unique x such that P(x)).

To prove a ($\exists! x\ P(x)$) statement, we first prove ($\exists x\ P(x)$) and then show that if P(x) and P(y) are both true, we must have x = y.

Uniqueness Proofs

Definition: Let a and b be two positive integers. If n is a positive integer and a|n and b|n, then we call n a ***common multiple*** of a and b. If n is a common multiple of a and b, and if for every other common multiple, m, of a and b we have that n|m, we say that n is a ***least common multiple*** of a and b. In this case, we write n = LCM(a,b).

Example:

For all positive integers a and b, LCM(a,b) is unique.

Pf: (We shall omit the proof of the existence of the LCM and just show it's uniqueness, assuming that it exists.)

Let a and b be positive integers.

Suppose m_1 and m_2 are two LCM's for a and b.

Since m_1 is an LCM and m_2 is a common multiple, $m_1 | m_2$, so $m_1 \leq m_2$.

Since m_2 is an LCM and m_1 is a common multiple, $m_2 | m_1$, so $m_2 \leq m_1$.

Therefore, $m_1 = m_2$.

Propositions

Prop: a) $\varnothing \cap A = \varnothing$ and $\varnothing \cup A = A$

b) $A \cap B \subseteq A$

c) $A \subseteq A \cup B$

d) $A \cup B = B \cup A$ and $A \cap B = B \cap A$

e) $A \cup (B \cup C) = (A \cup B) \cup C$
and $A \cap (B \cap C) = (A \cap B) \cap C$

f) $A \cup A = A = A \cap A$

g) If $A \subseteq B$ then $A \cup C \subseteq B \cup C$
and $A \cap C \subseteq B \cap C$.

$\varnothing \cap A = \varnothing$

Pf: To prove set equality we need to show that $\varnothing \cap A \subseteq \varnothing$, and $\varnothing \subseteq \varnothing \cap A$. However, we have already proved that this second containment is true, so we only need to prove the first.

To prove $\varnothing \cap A \subseteq \varnothing$, we have to show that

$(\forall x \in U)(x \in \varnothing \cap A \Rightarrow x \in \varnothing)$.

$\varnothing \cap A = \{x \mid x \in \varnothing \wedge x \in A\}$,

but since $x \in \varnothing$ is false for all x, $x \in \varnothing \wedge x \in A$ is always false.

Thus, $x \in \varnothing \cap A$ is always false, so $x \in \varnothing \cap A \Rightarrow x \in \varnothing$ is true for all x. ❑

A better proof: BWOC suppose $\varnothing \cap A \neq \varnothing$.

Then $\exists x\ (x \in \varnothing \cap A)$.

Which implies, by the definition of intersection, that

$\exists x\ (x \in \varnothing)$ $\rightarrow\leftarrow$ ❑

$\varnothing \cup A = A$

Pf: We first show that $\varnothing \cup A \subseteq A$.

Let $x \in \varnothing \cup A$.

By the definition of union, $x \in \varnothing \vee x \in A$.

Since $x \in \varnothing$ is always false, we must have $x \in A$ is true.

Thus, $\forall x\,(x \in \varnothing \cup A \Rightarrow x \in A)$ and so, $\varnothing \cup A \subseteq A$.

STOP!!!! ... we are being sloppy.

This statement is supposed to be true for **all** sets A.

$(\forall A)\,(\varnothing \cup A = A)$ (hidden quantifier)

What if A is = $\varnothing$? We have used the statement "$x \in A$ is true" in this "proof", but if A is the empty set, that is **false!!**

To fix this problem, we deal with the special case of $A = \varnothing$ first.

$\varnothing \cup A = A$ (again)

Pf: If $A = \varnothing$, then $\varnothing \cup \varnothing = \{x \mid x \in \varnothing \vee x \in \varnothing\} = \varnothing$, since the condition is a contradiction. Thus, $\varnothing \cup A = A$ is true in this case.

We may therefore assume that $A \neq \varnothing$.

We first show that $\varnothing \cup A \subseteq A$.

Suppose $x \in \varnothing \cup A$.

By the definition of union, $x \in \varnothing \vee x \in A$.

Since $x \in \varnothing$ is always false, we must have $x \in A$ is true.

Thus, $\forall x (x \in \varnothing \cup A \Rightarrow x \in A)$ and so, $\varnothing \cup A \subseteq A$.

Now we show that $A \subseteq \varnothing \cup A$.

Let $x \in A$.

By the definition of union, $x \in \varnothing \cup A$.

Thus, $\forall x (x \in A \Rightarrow x \in \varnothing \cup A)$ and so, $A \subseteq \varnothing \cup A$. ❑

$A \cap B \subseteq A$

Pf: If $A \cap B = \varnothing$, then the statement is true for any set A.
Thus we may assume that $A \cap B \neq \varnothing$.
Let $x \in A \cap B$.
By the definition of intersection, $x \in A$ and $x \in B$.
In particular, $x \in A$.
So, $(\forall x)(x \in A \cap B \Rightarrow x \in A)$ and we have $A \cap B \subseteq A$. ❑

If $A \subseteq B$ then $A \cup C \subseteq B \cup C$

Pf: If $A \cup C = \emptyset$ then the statement is true, so we may assume that $A \cup C \neq \emptyset$.

Let $x \in A \cup C$.

Case I: $x \in A$.

Since $A \subseteq B$, $x \in A \Rightarrow x \in B$.

$x \in B \Rightarrow x \in B \cup C$.

Case II: $x \in C$.

$x \in C \Rightarrow x \in B \cup C$.

Thus, in either case, $x \in A \cup C \Rightarrow x \in B \cup C$.

So, $(\forall x)(x \in A \cup C \Rightarrow x \in B \cup C)$ and we have $A \cup C \subseteq B \cup C$. ❑

Propositions

Prop:

a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$

b) $\overline{\overline{A}} = A$

c) $A - B = A \cap \overline{B}$

d) $A \subseteq B$ iff $\overline{B} \subseteq \overline{A}$.

The complement $\overline{A}$ was written earlier as $A^{\sim}$ or A^{c}.

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$$

Pf: $\overline{A \cup B} = U - (A \cup B) = \{x \mid x \in U \wedge x \notin A \cup B\}$

$= \{x \mid x \in U \wedge \sim(x \in A \cup B)\}$

$= \{x \mid x \in U \wedge \sim(x \in A \vee x \in B)\}$

$= \{x \mid x \in U \wedge (\sim x \in A \wedge \sim x \in B)\}$

$= \{x \mid x \in U \wedge (x \notin A \wedge x \notin B)\}$

$= \{x \mid (x \in U \wedge x \notin A) \wedge (x \in U \wedge x \notin B)\}$

$= \{x \mid (x \in U - A) \wedge (x \in U - B)\}$

$= \{x \mid (x \in \overline{A}) \wedge (x \in \overline{B})\}$

$= \overline{A} \cap \overline{B}$ ❑

$A - B = A \cap \overline{B}$

Pf: If $A-B = \emptyset$ then $(\forall x \in A)(\sim(x \notin B))$ thus
$A \cap \overline{B} = \{x \in U | x \in A \wedge x \notin B\} = \emptyset$, and the statement is true.

We may therefore assume that $A-B \neq \emptyset$.

Let $x \in A-B$.

Then $x \in A$ and $x \notin B$.

$x \in U \wedge x \notin B \Rightarrow x \in \overline{B}$, i.e. $x \in A \cap \overline{B}$.

So, $A - B \subseteq A \cap \overline{B}$.

If $A \cap \overline{B} = \emptyset$ then $(\forall x \in A)(\sim(x \notin B))$, so $A-B = \emptyset$ and the statement is true.

We may therefore assume that $A \cap \overline{B} \neq \emptyset$.

Let $y \in A \cap \overline{B}$. Thus, $y \in A$ and $y \in \overline{B}$.

$y \in \overline{B} \Rightarrow y \in U \wedge y \notin B$.

So $y \in A$ and $y \notin B$, i.e. $y \in A - B$.

Hence, $A \cap \overline{B} \subseteq A - B$ and we have $A - B = A \cap \overline{B}$. ❑

$$A \subseteq B \text{ iff } \overline{B} \subseteq \overline{A}$$

Pf: $A \subseteq B$ iff $(\forall x \in U)(x \in A \Rightarrow x \in B)$

iff $(\forall x \in U)(\sim(x \in B) \Rightarrow \sim(x \in A))$

iff $(\forall x \in U)(x \in \overline{B} \Rightarrow x \in \overline{A})$

iff $\overline{B} \subseteq \overline{A}$ ❑