

Proof Techniques - direct proofs

Here's what you know:

Ellen is a math major or a CS major.

If Ellen does not like discrete math, she is not a CS major.

If Ellen likes discrete math, she is smart.

Ellen is not a math major.

Can you conclude Ellen is smart?

$M \vee C$

$\neg D \rightarrow \neg C$

$((M \vee C) \wedge (\neg D \rightarrow \neg C) \wedge (D \rightarrow S) \wedge (\neg M)) \rightarrow S$

?

Proof Techniques - direct proofs

In general, to prove $p \rightarrow q$, assume p and show that q follows.

$$((M \vee C) \wedge (\neg D \rightarrow \neg C) \wedge (D \rightarrow S) \wedge (\neg M)) \rightarrow S$$

?

Proof Techniques - direct proofs

1. $M \vee C$	<i>Given</i>
2. $\neg D \rightarrow \neg C$	<i>Given</i>
3. $D \rightarrow S$	<i>Given</i>
4. $\neg M$	<i>Given</i>
5. C	DS (1,4)
6. D	MT (2,5)
7. S	MP (3,6)

Ellen is smart!

Proof Techniques - vacuous proofs

In general, to prove $p \rightarrow q$, assume p and show that q follows.

But $p \rightarrow q$ is also TRUE if p is FALSE.

Suggests proving $p \rightarrow q$ by proving $\neg p$.

*Ex. p : There is good Chinese food in CU.
 q : I'll give you each \$10.*

Since p is FALSE, $p \rightarrow q$ is TRUE
(but we don't know a thing about q)

Proof Techniques - trivial proofs

In general, to prove $p \rightarrow q$, assume p and show that q follows.

But $p \rightarrow q$ is also TRUE if q is TRUE.

Suggests proving $p \rightarrow q$ by proving q .

*Ex. p : there is good Chinese food in CU
 q : I'm drinking coffee*

Since q is TRUE, $p \rightarrow q$ is TRUE
(the truth or falsity of p is irrelevant)

Proof Techniques - indirect proofs

Recall that $p \rightarrow q \equiv \neg q \rightarrow \neg p$ (the contrapositive)

So, we can prove the implication $p \rightarrow q$ by first assuming $\neg q$, and showing that $\neg p$ follows.

Example: Prove that if a and b are integers, and $a + b \geq 15$, then $a \geq 8$ or $b \geq 8$.

$$(a + b \geq 15) \rightarrow (a \geq 8) \vee (b \geq 8)$$

(Assume $\neg q$) Suppose $(a < 8) \wedge (b < 8)$.

(Show $\neg p$) Then $(a \leq 7) \wedge (b \leq 7)$,

and $(a + b) \leq 14$,

and $(a + b) < 15$.

Proof Techniques - proof by contradiction

To prove a proposition p , assume not p and show a contradiction.

Suppose the proposition is of the form $p \rightarrow q$, and recall that $p \rightarrow q \equiv q \vee \neg p \equiv \neg(\neg q \wedge p)$. So assuming the opposite is to assume $\neg q \wedge p$.

Proof Techniques - proof by contradiction

Example:

*Rainy days make gardens grow.
Gardens don't grow if it is not hot.
When it is cold outside, it rains.*

~~Prove~~ *that it's hot.*

$$\neg H \rightarrow \neg G$$

$$\neg H \rightarrow R$$

Show: H

$$((R \rightarrow G) \wedge (\neg H \rightarrow \neg G) \wedge (\neg H \rightarrow R)) \rightarrow H$$

?

Proof Techniques - proof by contradiction

Given: $R \rightarrow G$

$\neg H \rightarrow \neg G$

$\neg H \rightarrow R$

Show: H

1. $R \rightarrow G$

Given

2. $\neg H \rightarrow \neg G$

Given

3. $\neg H \rightarrow R$

Given

4. $\neg H$

assume to the contrary

5. R

MP (3,4)

6. G

MP (1,5)

7. $\neg G$

MP (2,4)

8. $G \wedge \neg G$

contradiction

$\therefore H$

Proof Techniques - proof by contradiction

Classic proof that $\sqrt{2}$ is irrational.

Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$

for some integers a and b
 $\sqrt{2} = a/b$ implies
(relatively prime).

$$2 = a^2/b^2$$

$$2b^2 = a^2$$

a^2 is even, and so a is even ($a = 2k$ for some k)

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

$$b^2 = 2k^2$$

b^2 is even, and so b is even ($b = 2k$ for some k)

But if a and b are both even, then they are not relatively prime!

Proof Techniques - proof by contradiction

You're going to let me get away with that?
 a^2 is even, and so a is even ($a = 2k$ for some k)??

Suppose to the contrary that a is not even.

Then $a = 2k + 1$ for some integer k

Then $a^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1$

and a^2 is odd.

contradiction

So a really is even.

Proof Techniques - proof by cases

*Suppose we want to prove a theorem
of the form: $p_1 \vee p_2 \vee \dots \vee p_n \rightarrow q$*

*We can prove it in pieces
corresponding to the cases, but*

$$A: (p_1 \rightarrow q) \vee (p_2 \rightarrow q) \vee \dots \vee (p_n \rightarrow q)$$

$$B: (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$$

Proof Techniques - proof by cases

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$$

Proof for $n=2$:

$$\begin{aligned}(p_1 \vee p_2) \rightarrow q &\equiv \neg(p_1 \vee p_2) \vee q && \text{Defn of } \rightarrow \\ &\equiv (\neg p_1 \wedge \neg p_2) \vee q && \text{DeMorgan's} \\ &\equiv (\neg p_1 \vee q) \wedge (\neg p_2 \vee q) && \text{Distributivity} \\ &\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) && \text{Defn of } \rightarrow\end{aligned}$$

Proofs - something for everyone...

"if x is a perfect square, and x is even, then x is divisible by 4."

Formally: $(p \wedge q) \rightarrow r$

Contrapositive: $\neg r \rightarrow \neg(p \wedge q) \equiv \neg r \rightarrow (\neg p \vee \neg q)$

Suppose x is not divisible by 4.

Then $x = 4k + 1$, or $x = 4k + 2$, or $x = 4k + 3$.

Now structure looks like $(u_1 \vee u_2 \vee u_3) \rightarrow (\neg p \vee \neg q)$

Case 1 (&3): $x = 4k + 1$, odd, corresponds to $\neg q$

Case 2: $x = 4k + 2$, even, so must not be a perfect square.

Proofs - something for everyone...

"if x is a perfect square, and x is even, then x is divisible by 4."

Subgoal, prove Case 2:

Case 2: $x = 4k + 2$, even (so we have to show not square).

$$\text{But } x = 4k + 2 = 2(2k + 1)$$

x is the product of 2 and an odd number.

So, x is not a perfect square.

Proofs - something for everyone...

If Boris becomes a pastry chef, then if he gives in to his desire for chocolate mousse, then his waistline will suffer. If his waistline suffers, then his dancing will suffer. Boris gives in to his desire for chocolate mousse.

*However, I
suffered
become*

- a) I could have done this on my own.
- b) I worked it out with my partner, but I couldn't have done it alone.
- c) My partner and I couldn't do it.

Proof Techniques-Quantifiers: Existence Proofs

Two ways of proving $\exists x P(x)$.

Either build one, or show one can be built.

Constructive

Non-constructive

Two examples, both involving $n!$

For the examples, think of $n!$ as a list of factors.

Proof Techniques - **CONSTRUCTIVE** Proofs

Example: Prove that for all integers n , there exist n consecutive composite integers.

**Composite =
not prime**

$\forall n$ (integer), $\exists x$ so that $x, x+1, x+2, \dots, x+n-1$ are all composite.

Proof: Let n be an arbitrary integer.
 $(n+1)! + 2$ is divisible by 2, \therefore composite.
 $(n+1)! + 3$ is divisible by 3, \therefore composite.

\vdots

$(n+1)! + (n+1)$ is divisible by $n+1$, \therefore composite.

$$x = (n+1)! + 2$$

Proof Techniques-Quantifiers: Existence Proofs

Example: Prove that for all integers n , there exists a prime p so that $p > n$.

Infinitely many primes!

$\forall n$ (integer), $\exists p$ so that p is prime, and $p > n$.

Proof: Let $n!$ be an arbitrary integer, and consider its prime factorization $(n! = p_1 \cdot p_2 \cdot \dots \cdot p_k)$. If $(n! + 1)$ is prime, we are done since $(n! + 1) > n$. But what if $(n! + 1)$ is composite?

Proof Techniques **NON-CONSTRUCTIVE** Proofs

$\forall n$ (integers), $\exists p$ so that p is prime,
and $p > n$.

Proof: Let n be an arbitrary integer,
and consider $n! + 1$. If $(n! + 1)$ is
prime, we are done since $(n! + 1) > n$.
But what if $(n! + 1)$ is composite?

If $(n! + 1)$ is composite then it has a
prime factorization, $p_1 p_2 \dots p_n = (n! + 1)$

Consider the smallest p_i , and call it p .
How small can it be?

So, $p > n$, and we are done. BUT WE
DON'T KNOW WHAT p IS!!!

Can it be 2?

Can it be 3?

Can it be 4?

Can it be n ?

Set Theory - Definitions and notation

A set is an unordered collection of elements.

Some examples:

$\{1, 2, 3\}$ is the set containing "1" and "2" and "3."

$\{1, 1, 2, 3, 3\} = \{1, 2, 3\}$ since repetition is irrelevant.

$\{1, 2, 3\} = \{3, 2, 1\}$ since sets are unordered.

$\{1, 2, 3, \dots\}$ is a way we denote an infinite set (in this case, the natural numbers).

$\emptyset = \{\}$ is the empty set, or the set containing no elements.

Note: $\emptyset \neq \{\emptyset\}$

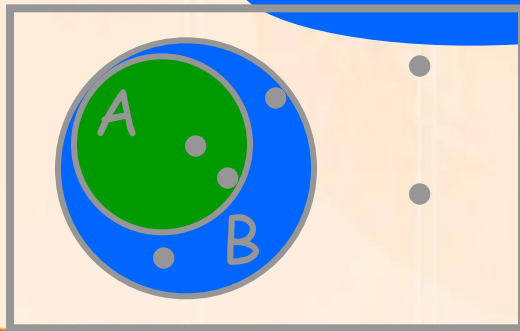
Set Theory - Definitions and notation

$x \in S$ means "x is an element of set S."

$x \notin S$ means "x is not an element of set S."

$A \subseteq B$ means "A is a subset of B."

Venn Diagram



or, "B contains A."

or, "every element of A is also in B."

or, $\forall x ((x \in A) \rightarrow (x \in B))$.

Set Theory - Definitions and notation

$A \subseteq B$ means "A is a subset of B."

$A \supseteq B$ means "A is a superset of B."

$A = B$ if and only if A and B have exactly the same elements.

iff, $A \subseteq B$ and $B \subseteq A$

iff, $A \subseteq B$ and $A \supseteq B$

iff, $\forall x ((x \in A) \leftrightarrow (x \in B))$.

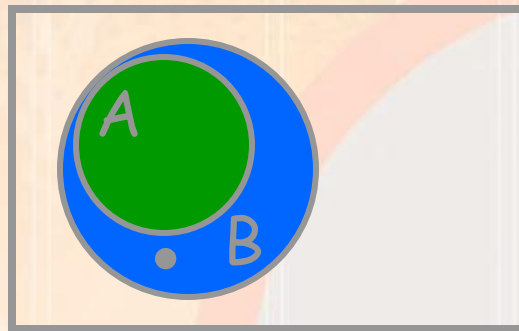
So to show equality of sets A and B, show:

- $A \subseteq B$
- $B \subseteq A$

Set Theory - Definitions and notation

$A \subset B$ means "A is a proper subset of B."

- $A \subseteq B$, and $A \neq B$.
- $\forall x ((x \in A) \rightarrow (x \in B)) \wedge \neg \forall x ((x \in B) \rightarrow (x \in A))$
- $\forall x ((x \in A) \rightarrow (x \in B)) \wedge \exists x \neg (\neg(x \in B) \vee (x \in A))$
- $\forall x ((x \in A) \rightarrow (x \in B)) \wedge \exists x ((x \in B) \wedge \neg(x \in A))$
- $\forall x ((x \in A) \rightarrow (x \in B)) \wedge \exists x ((x \in B) \wedge (x \notin A))$



Set Theory - Definitions and notation

Quick examples:

- $\{1,2,3\} \subseteq \{1,2,3,4,5\}$
- $\{1,2,3\} \subset \{1,2,3,4,5\}$

Is $\emptyset \subseteq \{1,2,3\}$?

Yes! $\forall x (x \in \emptyset) \rightarrow (x \in \{1,2,3\})$ **Vacuously**
holds, because $(x \in \emptyset)$ is false. (empty,
hollow)

Is $\emptyset \in \{1,2,3\}$? No!

Is $\emptyset \subseteq \{\emptyset,1,2,3\}$? Yes!

Is $\emptyset \in \{\emptyset,1,2,3\}$? Yes!

Set Theory - Definitions and notation

Quiz time:

Is $\{x\} \subseteq \{x\}$?

Yes

Is $\{x\} \in \{x, \{x\}\}$?

Yes

Is $\{x\} \subseteq \{x, \{x\}\}$?

Yes

Is $\{x\} \in \{x\}$?

No

Set Theory - Ways to define sets

- Explicitly: {John, Paul, George, Ringo}
- Implicitly: {1,2,3,...}, or {2,3,5,7,...} : and | are read "such that" or "where"
- Set builder: { x : x is prime }, { x : $x > 10$ }
In general { x : $P(x)$ is true }, where $P(x)$ is some description of the set.

Ex. Let $D(x,y)$ denote "x is divisible by y."

Give another name for

$$\{ x : \forall y ((y > 1) \wedge (y < x)) \rightarrow \neg D(x,y) \}.$$

Primes

Can we use any predicate P to define a set

$$S = \{ x : P(x) \}?$$

Set Theory - Russell's Paradox

Can we use any predicate P to define a set

$$S = \{x : P(x)\}?$$

No!

Define $S = \{x : x \text{ is a set where } x \notin x\}$

Then, if $S \in S$, then by defn of S , $S \notin S$.

So S must not be in S , right?

But, if $S \notin S$, then by defn of S , $S \in S$.

ARRRGH!

There is a town with a barber who shaves all the people (and only the people) who don't shave themselves.

Who shaves the barber?

Set Theory - Cardinality

If S is finite, then the cardinality of S , $|S|$, is the number of distinct elements in S .

If $S = \{1, 2, 3\}$, $|S| = 3$.

If $S = \{3, 3, 3, 3, 3\}$, $|S| = 1$.

If $S = \emptyset$, $|S| = 0$.

If $S = \{ \emptyset, \{ \emptyset \}, \{ \emptyset, \{ \emptyset \} \} \}$, $|S| = 3$.

If $S = \{0, 1, 2, 3, \dots\}$, $|S|$ is infinite. (more on this later)

Set Theory - Power sets

If S is a set, then the power set of S is

$$2^S = \{x : x \subseteq S\}.$$

aka $P(S)$

If $S = \{a\}$, $2^S = \{\emptyset, \{a\}\}.$

If $S = \{a,b\}$, $2^S = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}.$

If $S = \emptyset$, $2^S = \{\emptyset\}.$

If $S = \{\emptyset, \{\emptyset\}\}$, $2^S = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}.$

We say, "P(S) is the set of all subsets of S."

Fact: if S is finite, $|2^S| = 2^{|S|}$. (if $|S| = n$, $|2^S| = 2^n$)