Foundations of Computer Science
Lecture 4

Proofs

Proving "IF ... THEN ..." (Implication): Direct proof; Contraposition
Contradiction
Proofs About Sets

Last Time

1. How to make precise statements.
2. Quantifiers which allow us to make statements about many things.

Today: Proofs

1. Proving "IF . . . , THEN . . . ".
2. Proof Patterns
   - Direct Proof

Implications: Reasoning in the Absence of Facts

Reasoning:

It rained last night (fact); the grass is wet ("deduced").

Reasoning in the absense of facts:

IF it rained last night, THEN the grass is wet.

- We like to prove such statements even though, at this moment, it is not much use.
- Later, you may learn that it rained last night and *infer* the grass is wet

More Relevant Example: Friendship cliques and radio frequencies.

IF we can quickly find the largest friend-clique in a friendship network,

THEN we can quickly determine how to assign non-conflicting frequencies to radio stations using a minimum number of frequencies.

More Mathematical Example: Quadratic formula.

IF $ax^2 + bx + c = 0$ and $a \neq 0$, THEN $x = \dfrac{-b + \sqrt{b^2 - 4ac}}{2a}$ or $x = \dfrac{-b - \sqrt{b^2 - 4ac}}{2a}$.

Proving an Implication

$$\text{IF } \underbrace{x \text{ and } y \text{ are rational}}_{p}, \quad \text{THEN} \quad \underbrace{x+y \text{ is rational}}_{q}.$$

$$\forall (x,y) \in \mathbb{Q}^2 : \underbrace{x+y \text{ is rational}}_{P(x,y)}.$$

Proof. We must show that the row $p = \text{T}$, $q = \text{F}$ can't happen.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Let us see what happens if $p = \text{T}$: $x, y \in \mathbb{Q}$.

$x = \frac{a}{b}$ and $y = \frac{c}{d}$, where $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{N}$.

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \in \mathbb{Q}.$$

That means q is T.

The row $p = \text{T}$, $q = \text{F}$ *cannot* occur and the implication is proved. ■

Template for Direct Proof of an Implication $p \to q$

Proof. We prove the implication using a direct proof.

1: Start by assuming that the statement claimed in p is T.
2: Restate your assumption in mathematical terms.
3: Use mathematical and logical derivations to relate your assumption to q.
4: Argue that you have shown that q must be T.
5: End by concluding that q is T. ■

Theorem. If $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$.

Proof. We prove the theorem using a direct proof.

1: Assume that $x, y \in \mathbb{Q}$, that is x and y are rational.
2: Then there are integers a, c and natural numbers b, d such that $x = a/b$ and $y = c/d$ (because this is what it means for x and y to be rational).
3: Then $x + y = (ad + bc)/bd$ (high-school algebra).
4: Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, $(ad + bc)/bd$ is rational.
5: Thus, we conclude (from steps 3 and 4) that $x + y \in \mathbb{Q}$. ■

A Proof is a Mathematical Essay

A proof must be well written.

The goal of a proof is to convince a reader of a theorem. A badly written proof that leaves a reader with some doubts has failed.

Steps for Writing Readable Proofs

I. **State your strategy.** Start with the proof type. Structure long proofs into parts and *tie up the parts at the end*. The reader must have *no* doubts.
II. **The proof should have a logical flow.** It is difficult to follow movies that jump between story lines or back and forth in time. A reader follows a proof linearly, from beginning to end.
III. **Keep it simple.** Make the idea at the heart of your proof clear. Avoid excessive symbols and unnecessary notation.
IV. **Justify your steps.** The reader must have no doubts. Avoid phrases like "It's obvious that …" If it is so obvious, explain.
V. **End your proof.** Explain why what you set out to show is true.
VI. **Read your proof.** Finally, check correctness; edit; simplify.

Example: Direct Proof

Let x be any real number, i.e. $x \in \mathbb{R}$.

$$\text{IF } \underbrace{4^x - 1 \text{ is divisible by } 3}_{p}, \text{ THEN } \underbrace{4^{x+1} - 1 \text{ is divisible by } 3}_{q}.$$

Proof. We prove the claim using a direct proof.

1: Assume that p is T, that is $4^x - 1$ is divisible by 3.

2: This means that $4^x - 1 = 3k$ for an integer k, or that $4^x = 3k + 1$.

3: Observe that $4^{x+1} = 4 \cdot 4^x$. Using $4^x = 3k + 1$,

$$4^{x+1} = 4 \cdot (3k + 1) = 12k + 4.$$

Therefore $4^{x+1} - 1 = 12k + 3 = 3(4k + 1)$ is a multiple of 3 ($4k + 1$ is an integer).

4: Since $4^{x+1} - 1$ is a multiple of 3, we have shown that $4^{x+1} - 1$ is divisible by 3.

5: Therefore, the statement claimed in q is T. ∎

Question. Is $4^x - 1$ divisible by 3?

We Made No Assumptions About x

$$P(x) : \text{“}\textsc{if } 4^x - 1 \text{ is divisible by } 3, \textsc{ then } 4^{x+1} - 1 \text{ is divisible by } 3\text{”}$$

Since we made no assumptions about x, we proved:

$$\forall x \in \mathbb{R} : P(x)$$

Exercise. Prove: For all pairs of odd integers m, n, the sum $m + n$ is an even integer.

Practice. Exercise 4.2.

Disproving an Implication

$$\text{IF } \underbrace{x^2 > y^2}_{p}, \text{ THEN } \underbrace{x > y}_{q}.$$

FALSE!

Counter-example: $x = -8, y = -4$.

$$x^2 > y^2 \qquad \text{SO, } p = \text{T}$$

$$x < y \qquad \text{SO, } q = \text{F}$$

The row $p = \text{T}, q = \text{F}$ has occurred!

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

A single **counter-example** suffices to disprove an implication.

Contraposition

$$\text{IF } \underbrace{x^2 \text{ is even}}_{p}, \text{ THEN } \underbrace{x \text{ is even}}_{q}.$$

Proof. We must show that the row $p = \texttt{T}$, $q = \texttt{F}$ can't happen.

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

Let us see what happens if $q = \texttt{F}$.

x is odd, $x = 2k + 1$.

$$\begin{aligned} x^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \qquad \leftarrow \text{odd} \end{aligned}$$

That means p is $\texttt{F}$.

The row $p = \texttt{T}$, $q = \texttt{F}$ *cannot* occur!

The implication is proved. ■

Template: Contraposition Proof of an Implication $p \to q$

Proof. We prove the theorem using contraposition.

1: Start by assuming that the statement claimed in q is F.
2: Restate your assumption in mathematical terms.
3: Use mathematical and logical derivations to relate your assumption to p.
4: Argue that you have shown that p must be F.
5: End by concluding that p is F. ■

Theorem. If x^2 is even, then x is even.

Proof. We prove the theorem by contraposition.

1: Assume that x is odd.
2: Then $x = 2k + 1$ for some $k \in \mathbb{Z}$ (that's what it means for x to be odd)
3: Then $x^2 = 2(2k^2 + 2k) + 1$ (high-school algebra).
4: Which means x^2 is 1 plus a multiple of 2, and hence is odd.
5: We have shown that x^2 is odd, concluding the proof. ■

Exercise. Prove: IF r is irrational, THEN $\sqrt{r}$ is irrational.

Equivalence: . . . IF AND ONLY IF. . .

p and q are equivalent means they are either both T or both F.

p IF AND ONLY IF q or $p \leftrightarrow q$

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

- You are a US citizen IF AND ONLY IF you were born on US soil.
- Sets A and B are equal IF AND ONLY IF $A \subseteq B$ and $B \subseteq A$.
- Integer x is divisible by 3 IF AND ONLY IF x^2 is divisible by 3.

To prove $p \leftrightarrow q$ is T, you must prove:

1. Row $p = T, q = F$ cannot occur: that is $p \rightarrow q$.
2. Row $p = F, q = T$ cannot occur: that is $q \rightarrow p$.

Integer x is divisible by 3 IF AND ONLY IF x^2 is divisible by 3.

$$\underbrace{x \text{ is divisible by } 3}_{p} \quad \text{IF AND ONLY IF} \quad \underbrace{x^2 \text{ is divisible by } 3}_{q}.$$

Proof. The proof has two main steps (one for each implication):

(i) **Prove $p \to q$: if x is divisible by 3, then x^2 is divisible by 3.**

We use a direct proof. Assume x is divisible by 3, so $x = 3k$ for some $k \in \mathbb{Z}$.

Then, $x^2 = 9k^2 = 3 \cdot (3k^2)$ is a multiple of 3, and so x^2 is divisible by 3.

(ii) **Prove $q \to p$: if x^2 is divisible by 3, then x is divisible by 3.**

We use contraposition. Assume x is not divisible by 3. There are two cases for x,

Case 1: $x = 3k + 1 \;\to\; x^2 = 3k(3k + 2) + 1$ (1 more than a multiple of 3).

Case 2: $x = 3k + 2 \;\to\; x^2 = 3(3k^2 + 4k + 1) + 1$ (1 more than a multiple of 3).

In all cases, x^2 is not divisible by 3, as was to be shown. ■

- IF AND ONLY IF proof contains the proofs of *two* implications.
- Each implication may be proved differently.

Contradictions

$$1 = 2; \qquad n^2 < n \text{ (for integer } n); \qquad |x| < x; \qquad p \wedge \neg p.$$

Contradictions are **FISHY**. In mathematics you cannot derive contradictions.

Principle of Contradiction. If you derive something **FISHY**, something's wrong with your derivation.

1: **Assume $\sqrt{2}$ is rational.**
2: This means $\sqrt{2} = a_*/b_*$; b_* is the smallest denominator (well-ordering).
3: That is, a_* and b_* cannot have 2 as a common factor.
4: We have: $2 = a_*^2/b_*^2 \to a_*^2 = 2b_*^2$, or a_*^2 is even. Hence, a_* is even, $a_* = 2k$. [we proved this]
5: Therefore, $4k^2 = 2b_*^2$ and so $b_*^2 = 2k^2$, or b_*^2 is even. Hence, b_* is even, $b_* = 2\ell$.
6: Hence, a_* and b_* are both divisible by 2. **(FISHY)**

What could possibly be wrong with this derivation? It must be step 1.

Template: Proof by Contradiction that p is T

- You can use contradiction to prove *anything*. Start by assuming it's false.
- Powerful because the starting assumption gives you something to work with.

Proof.

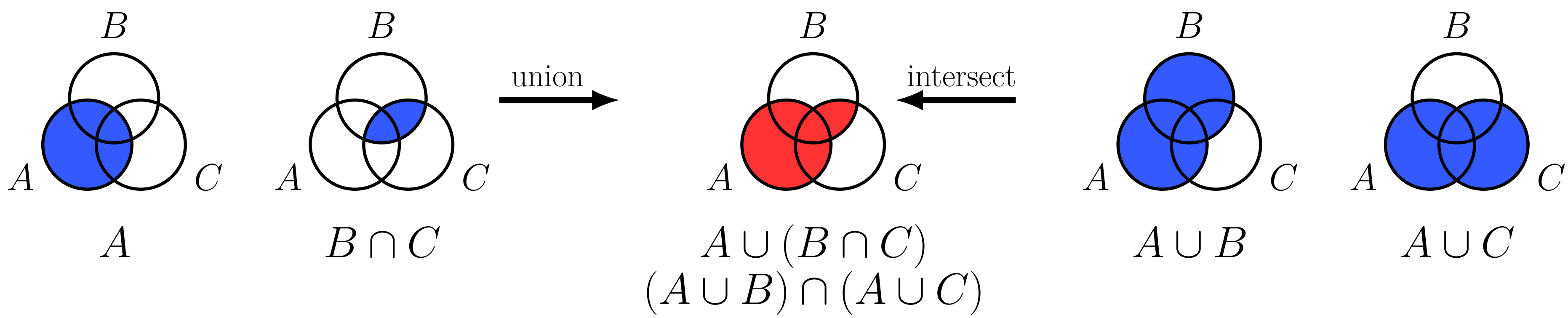
1: To derive a contradiction, assume that p is F.
2: Restate your assumption in mathematical terms.
3: Derive a **FISHY** statement – a contradiction that must be false.
4: Therefore, the assumption in step 1 is false, and p is T. ■

DANGER! Be especially careful in contradiction proofs. Any small mistake can easily lead to a contradiction and a false sense that you proved your claim.

Exercise. Let a, b be integers. Prove that $a^2 - 4b \neq 2$.

Proofs about Sets

Venn diagram proofs: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.



Formal proofs:

- One set is a subset of another, $A \subseteq B$: $x \in A \rightarrow x \in B$
- One set is a not a subset of another, $A \not\subseteq B$: $\exists x \in A : x \notin B$
- Two sets are equal, $A = B$: $x \in A \leftrightarrow x \in B$

Exercise. $A = \{\text{multiples of } 2\}$; $B = \{\text{multiples of } 9\}$; $C = \{\text{multiples of } 6\}$. Prove $A \cap B \subseteq C$.

Picking a Proof Template

Situation you are faced with	Suggested proof method
1. Clear how result follows from assumption	**Direct proof**
2. Clear that if result is false, the assumption is false	**Contraposition**
3. Prove something exists	**Show an example**
4. Prove something does not exist	**Contradiction**
5. Prove something is unique	**Contradiction**
6. Prove something is *not true* for *all* objects	**Show a counter-example**
7. Show something is *true* for *all* objects	**Show for general object**

Practice. Exercise 4.8.