Foundations of Computer Science
Lecture 4
Proofs
Proving "IF ... THEN ... " (Implication): Direct proof; Contraposition
Contradiction
Proofs About Sets

Today: Proofs

- Proving “IF ... , THEN ... ”.
- Proof Patterns
  - Direct Proof
  - Contraposition
  - Equivalence, ... IF AND ONLY IF ...
- Contradiction
- Proofs about sets.

Implications: Reasoning in the Absence of Facts

Reasoning:
It rained last night (fact); the grass is wet (“deduced”).

Reasoning in the absence 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 \( x = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \) or \( x = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \).
Proving an Implication

If \( x \) and \( y \) are rational, then \( x + y \) is rational.

\[
\forall (x, y) \in \mathbb{Q}^2 : x + y \text{ is rational.}
\]

Proof. We must show that the row \( p = T, q = F \) can’t happen. Let us see what happens if \( p = T, q = F \), 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 \( q = T \).

The row \( p = T, q = F \) cannot occur and the implication is proved.

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:

- **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.
- **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.
- **Keep it simple.** A proof is not a sequence of equations with a few words sprinkled here and there. Avoid excessive use of symbols and don’t introduce new notation unless it is absolutely necessary. Make the idea clear.
- **Justify your steps.** The reader must have no doubts. Avoid phrases like “It’s obvious that . . . ” If it is so obvious, give a short explanation.
- **End your proof.** Explain why what you set out to show is true.
- **Read your proof.** Finally, check correctness; edit; simplify.

Example: Direct Proof

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

\[
\text{If } 4^x - 1 \text{ is divisible by } 3, \text{ then } 4^{x+1} - 1 \text{ is divisible by } 3.
\]

Proof. We prove the claim using a direct proof.

1. Assume that \( x \) is an integer, 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 \( x + y = (ac + bd)/bd \) (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 \( x + y \in \mathbb{Q} \).

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 \( x + y \in \mathbb{Q} \).

Question. Is \( 4^x - 1 \) divisible by 3?
We Made No Assumptions About $x$

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

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

$$\text{If } x^2 > y^2, \text{ then } x > y.$$  

FALSE!

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

$x^2 > y^2$ so, $p = T$

$x < y$ so, $q = F$

The row $p = T, q = F$ has occurred!

A single counter-example suffices to disprove an implication.

Contraposition

$$\text{If } x^2 \text{ is even, then } x \text{ is even.}$$

Proof. We must show that the row $p = T, q = F$ can’t happen.

Let us see what happens if $q = F$.

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

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \quad \leftarrow \text{ odd}$$

That means $p$ is $F$.

The row $p = T, q = F$ cannot occur!

The implication is proved.

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 $F$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \leftrightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

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

Contradictions

1 = 2; $n^2 < n$ (for integer $n$); $|x| < x$; $p \land \neg p$.
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, $a_1$ and $b_1$ cannot have 2 as a common factor.
4: We have: $2 = a_1^2/b_1^2 \rightarrow a_1^2 = 2b_1^2$ or $a_1^2$ is even. Hence, $a_1$ is even, $a_1 = 2k$.
5: Therefore, $4k^2 = 2b_1^2$ and so $b_1^2 = 2k^2$, or $b_1^2$ is even. Hence, $b_1$ is even, $b_1 = 2\ell$.
6: Hence, $a_1$ and $b_1$ are both divisible by 2. (FISHY)

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

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

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

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

- **Prove $p \rightarrow q$:** 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, $x^2 = 9k^2 = 3(3k^2)$ is a multiple of 3, and so $x^2$ is divisible by 3.

- **Prove $q \rightarrow p$:** 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: $x = 3k + 1 \rightarrow x^2 = 9k^2 + 6k + 1$ (1 more than a multiple of 3).
  Case 2: $x = 3k + 2 \rightarrow x^2 = 9k^2 + 12k + 4$ (1 more than a multiple of 3).
  In all cases, $x^2$ is not divisible by 3, as was to be shown.

**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, \( A \nsubseteq B \): 
  \[ \exists x \in A : x \notin B \]
- 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

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

**Practice.** Exercise 4.8.