Session 14: Proof Examples

- Examples for direct and indirect proofs
- Other proof methods
- Mistakes in proofs

Theorem on Even and Odd Integers

Definition: The integer n is **even** if there exists an integer k such that $n = 2k$, and n is **odd** if there exists an integer k, such that $n = 2k + 1$.

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

Example: n = 3 is odd, then $3^2 = 9$ is odd.

Note: every integer is either even or odd and no integer is both even and odd.
Strictly speaking, this requires a proof.

Direct Proof

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

Proof: n is odd

therefore, there exists k, s.t. $n = 2k+1$ (Def.)

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

$k' = 2k^2 + 2k$ is an integer

therefore $n^2 = 2k' + 1$ and is odd ◁ (Def.)

QED

Theorem on Sum of Rational Numbers

Definition: The real number r is **rational** if there exist integers p and q where $q \neq 0$ such that $r = p/q$

Theorem: The sum of two rational numbers is rational.

Direct Proof

Theorem: The sum of two rational numbers is rational.

Proof: r_1, r_2 are rational

Therefore $r_1 = \frac{p_1}{q_1}, r_2 = \frac{p_2}{q_2}, q_1, q_2 \neq 0$ (Def)

$$r_1 + r_2 = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 \cdot q_2}$$

$p' = p_1 q_2 + p_2 q_1$, $q' = q_1 q_2$ are integers and $q' \neq 0$

Therefore $r_1 + r_2 = \frac{p'}{q'}$, and is rational (Def)

Proof by Contraposition

$p \rightarrow q$

Theorem: If n is an integer and $3n + 2$ is odd, then n is odd.

Proof: $\neg q$: assume n is even

Therefore exists k, such that $n = 2k$

$3n + 2 = 3 \cdot 2 \cdot k + 2 = 2(3k + 1)$

by definition therefore $3n+2$ is even

so we have shown $\neg p$

since we have show $\neg q \rightarrow \neg p$

we also have shown $p \rightarrow q$ ◭

Proof by Contraposition

Theorem: For an integer *n*, if n^2 is odd, then *n* is odd.

Proof: assume n is even, i.e. $n = 2k$ for some integer k

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

$k' = 2k^2$ is an integer, and $n^2 = 2k'$

Therefore n^2 is even

So we have shown $\neg q \Rightarrow \neg p$ ◭

Proof by Contradiction

Theorem: If more than N items are distributed in any manner over N bins, there must be a bin containing at least two items (pigeonhole principle).

Proof:

p : more than N items distributed over N bins

q : one bin contains at least 2 items

$\neg q$: all bins contain at most 1 item

$\neg q$ implies there exist at most N items, nr_items $\leq N$

p : says there are more than N items, nr_items $> N$

$p \wedge \neg q \equiv p \wedge \neg p \equiv F$ $\lightning$ ∎

Contraposition vs. Contradiction

- The previous proof can also be interpreted as proof by contraposition.
- Assuming ¬q is true we made a direct proof of ¬p, and thus proved ¬q → ¬p
- More generally, any proof by contraposition can be tansformed in a proof by contradiction, but not vice versa:
  - If you assume that p and ¬q are true and you have a direct proof for ¬q → ¬p then you have shown that $(p \wedge \neg q) \rightarrow (p \wedge \neg p) \equiv \mathbf{F}$
- General proofs by contradiction use some other statement r that produces the contradiction, i.e., we prove $(p \wedge \neg q) \rightarrow (r \wedge \neg r)$

Example of a genuine proof by contradiction

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

Proof: by contradiction

Suppose $\sqrt{2}$ is rational $(\neg q)$

there exist integers $a, b, b \neq 0$ s.t. $\sqrt{2} = \frac{a}{b}$, | a, b have no common factors | (r)

then $2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow a^2$ is even $\Rightarrow a$ is even $\Rightarrow a = 2c$ for some integer c

then $2b^2 = 4c^2 \Rightarrow b^2 = 2c^2 \Rightarrow b^2$ is even $\Rightarrow b$ is even $\Rightarrow b = 2d$ for some integer d

$\Rightarrow$ | a and b have 2 as common factor | $(\neg r)$

$\Rightarrow r \wedge \neg r$ ↯ therefore $\sqrt{2}$ is irrational

Proofs for Biconditional Statements

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.

Theorem: If n is an integer, then n is odd if and only if n^2 is odd.

Proof:

We have already shown that both $p \rightarrow q$ and $q \rightarrow p$.

Therefore we can conclude $p \leftrightarrow q$.

Proof by Cases

To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

use the tautology

$$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow$$
$$[(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$$

Each of the implications $p_i \rightarrow q$ is a **case**.

Example

Theorem: if n is an integer, then $n^2 \geq n$.

Proof:

Case $n = 0$: $0^2 \geq 0$ ✓

Case $n \geq 1$: $n \geq 1 \Rightarrow n^2 \geq n$ ✓

Case $n \leq -1$: $n \leq -1 \Rightarrow n^2 \geq 0 \Rightarrow n^2 \geq n$ ✓

WLOG = without loss of generality

In context of proof by cases: if one case is show, another follows trivially (e.g. by swapping roles of variables)

Example: if x, y are integers and both xy and $x+y$ are even, then both x and y are even

Proof: by contraposition, if not x and y are even, then either x or y are odd.

WLOG: assume x is odd (the other case that y is odd would be proven the same way with roles of x and y exchanged)

→ syntactically swapping x and y

Proof by Counterexample

To establish that $\neg\forall x P(x)$ is true (or $\forall x P(x)$ is false) find a *c* such that $\neg P(c)$ is true or $P(c)$ is false.

Reminder: $\exists x \neg P(x) \equiv \neg\forall x P(x)$

In this case *c* is called a **counterexample** to the assertion $\forall x P(x)$.

Example:

Show that the statement "Every positive integer is the sum of the squares of 2 integers." is False.

$1 = 1^2 + 0^2$

$2 = 1^2 + 1^2$

$3 = ?$ not possible, since $3 = 2+1$ or $3 = 3+0$, but both 2 and 3 are not squares

Summary

- Examples of direct and indirect proofs
- Proofs for Biconditional Statements
- Proof by Cases
- Counterexamples
- Mistakes in Proofs

Existence Proofs — proof for $\exists x P(x)$

2 possibilities

1. Constructive Proof: find an element c, such that P(c), then apply existential generalization

Example

Theorem: There exists a positive integer that can be written as sum of cubes in two ways.

Proof: $1729 = 10^3 + 9^3 = 12^3 + 1^3$

Remark: Ramanujan observed that this is the smallest integer with that property

2. Non-constructive proof:

find c_1, c_2 such that $P(c_1) \vee P(c_2)$

$$P(c_1) \vee P(c_2)$$

$$P(c_1) \rightarrow \exists x\, P(x)$$

$$P(c_2) \rightarrow \exists x\, P(x)$$

$$(P(c_1) \vee P(c_2)) \rightarrow \exists x\, P(x)$$

Same tautology as used in proof by cases

We do not know which of the two c_1, c_2 hold.

Example

Theorem: There exist irrational numbers x and y, such that x^y is rational.

Proof: consider $\sqrt{2}^{\sqrt{2}}$: if it is rational, $x = \sqrt{2}$, $y = \sqrt{2}$ is a witness

if $\sqrt{2}^{\sqrt{2}}$ is irrational, take $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$

Then $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$, and we found witnesses x, y

After providing this proof, we do not know which are the "right" x, y

→ non-constructive