Introduction to Proofs

Ali Reza Khanteymoori

Department of Computer Engineering
University of Zanjan

Khanteymoori@znu.ac.ir

These slides are mainly taken from http://www.cs.laurentian.ca/jdompierre/html/MATH2056E_W2011/index.html

Definition: 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 $n = 2k + 1$.

Note that an integer is either even or odd, and no integer is both even and odd.

Definition

The real number r is **rational** if there exists integers a and b with $b \neq 0$ such that $r = a/b$. A real number that is not rational is called **irrational**.

Theorems in Mathematics

In mathematics, we often see theorems like

> *"if n is odd, then n^2 is odd."*

The universal quantification is generally forgotten. The precise statement is

> *"For all positive integers n, if n is odd, then n^2 is odd."*

If $P(n)$ is defined as "n is odd" and $Q(n)$ as "n^2 is odd", and if the universe of discourse is the set $\mathbb{N}$ of all positive integers, then this theorem is written as

$$\forall n\,(P(n) \rightarrow Q(n)).$$

Formal Proofs

In a **formal proof** of the theorem $\forall n\,(P(n) \rightarrow Q(n))$, each step of the proof are given with proper justification. Generally, there are three main steps:

1. Universal instantiation is used to transform the proposition $\forall n\,(P(n) \rightarrow Q(n))$ into the proposition $P(c) \rightarrow Q(c)$ where c is an arbitrary element of the universe of discourse without any specific assumption.
2. Then we prove $P(c) \rightarrow Q(c)$ for that arbitrary element c. Note that $p \rightarrow q$ is always true except when p is true and q is false. We only have to check that this case never happens. To show this, it is sufficient to suppose that if p is true, then it will make q to be also true and then the conditional statement $p \rightarrow q$ will be true.
3. As the element c of the universe of discourse is completely arbitrary and free of any specific assumption, then we can use the universal generalisation to deduce that the implication $P(c) \rightarrow Q(c)$ is true for all elements of the universe of discourse.

Informal Proofs

Usually, textbooks contains **informal proofs**, where more than one rule of inference may be used at each step, where steps may be skipped, where axioms being assumed and the rule of inference used are not explicitly stated. Also, the first step of universal instantiation and the last step of universal generalisation are also usually skipped.

Formal proofs are long, tedious and annoying. Informal proofs are for human consumption. They skip what the reader should be able to provide by himself and they focus on the key idea of the proof.

Methods for Proving Theorems

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, we need to show that the conditional statement $P(c) \rightarrow Q(c)$ is true for an arbitrary element c of the universe of discourse. Different proof methods can be used:

- direct proof,
- proof by contraposition,
- proof by contradiction,
- trivial proof,
- vacuous proof,
- proof by cases.

Direct Proof

A **direct proof** of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using definitions, axioms, previously proven theorems, together with rules of inference, we show that q must also be true.

The idea behind a direct proof is to show that the conditional statement $p \rightarrow q$ is true by showing that if p is true, then q must also be true, so that the combination p true and q false never occurs.

Proof by Contraposition

Proof by contraposition of the conditional statement $p \rightarrow q$ make use of the fact that this statement is equivalent to its contrapositive $\neg q \rightarrow \neg p$. This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive $\neg q \rightarrow \neg p$ is true. We take $\neg q$ as a hypothesis, subsequent steps are constructed using definitions, axioms, previously proven theorems, together with rules of inference, we show that $\neg p$ must also be true.

Proof by Contradiction — First Kind

There are two "kinds" of proofs by contradiction.

To prove by **contradiction** that a proposition p is true, we assume that it is false and we show that this assumption implies a contradiction, i.e., $\neg p \longrightarrow \mathrm{F}$. We conclude that the proposition p cannot be false, so it is true.

Remark: Usually, we are looking for a contradiction of the form $r \wedge \neg r$ which is false whenever r is a proposition.

$\sqrt{2}$ Is an Irrational Number

We want to prove that $\sqrt{2}$ is an irrational number. This proof by contradiction is known since Pythagoras. We start by assuming the opposite.

1. $\sqrt{2}$ is a rational number, there exist integers a and b, $b \neq 0$, such that $\sqrt{2} = a/b$ and such that a and b have no common factors (so that the fraction a/b is in lowest terms).
2. $2 = a^2/b^2$ by squaring both sides of the equation in 1.
3. $2b^2 = a^2$ by algebraic manipulation.
4. a^2 is an even number because it is equal to 2 times an integer.
5. a is an even number because of a previously proved theorem (if n^2 is even then n is even).
6. $a = 2k$ for some integer k by defintion of an even number.
7. $2b^2 = a^2 = (2k)^2 = 4k^2$ by algebraic manipulation with steps 3 and 6.

$\sqrt{2}$ Is an Irrational Number (continued)

8. $b^2 = 2k^2$ by dividing by 2 the equation of step 7.
9. b^2 is an even number because it is equal to 2 times an integer.
10. b is an even number because of a previously proved theorem (if n^2 is even then n is even).
11. a and b are both even numbers, by steps 5 and 10, that is 2 divides both a and b.
12. a and b have a common factor which is 2, which is a contradiction of hypothesis of step 1. $\sqrt{2}$ is a rational number must be false. So $\sqrt{2}$ is a irrational number must be true.

Q.E.D.

Proof by Contradiction — Second Kind

In the case where the proposition to prove is the conditional statement $p \longrightarrow q$, to suppose that it is false is equivalent to suppose that $\neg(p \longrightarrow q)$ is true, that $\neg(\neg p \vee q)$ is true, and finally, to suppose that $p \wedge \neg q$ is true.

In short, if you want to prove the conditional statement $p \longrightarrow q$ by contradiction, start by assuming that $p \wedge \neg q$ is true.

Example of Proof by Contradiction

Here, x and y are integers. Consider the following theorem: "*If x and y are odd integers, then $x - y$ is even.*" Give a proof by **contradiction**.

- The proposition a is "x is odd."
- The proposition b is "y is odd."
- The proposition c is "$x - y$ is even."
- The theorem is "$(a \wedge b) \rightarrow c$."

The proof by contradiction consists of making the assumption that $(a \wedge b) \rightarrow c$ is false, i.e., $\neg((a \wedge b) \rightarrow c)$ is true. This is logically equivalent to $\neg(\neg(a \wedge b) \vee c)$, and using De Morgan law, logically equivalent to $(a \wedge b) \wedge \neg c$. In short, the proof by contradiction starts with "x is odd" **and** "y is odd" **and** "$x - y$ is odd."

Example of Proof by Contradiction (continued)

We are looking for a contradiction

1. x is odd. By hypothesis.
2. y is odd. By hypothesis.
3. $x - y$ is odd. By hypothesis.
4. $x = 2k + 1$ for some integer k. By definition of an odd integer.
5. $y = 2l + 1$ for some integer l. By definition of an odd integer.
6. $x - y = (2k + 1) - (2l + 1) = 2k - 2l = 2(k - l)$. By using step 4 for x, step 5. for y and with some algebraic manipulations.
7. $x - y = 2m$ where $m = k - l$. From step 6.
8. $x - y$ is even. From step 7 using the definition of an even number. This is in contradiction with step 3.

Q.E.D.

Trivial Proof

If we already know that the conclusion q is true, then the conditional statement $p \rightarrow q$ is true whenever the truth value of p. A proof of $p \rightarrow q$ that use the fact that q is true is called a **trivial proof**.

Note that the hypothesis is not needed in a trivial proof.
Example: "If Martians exist, then $2 + 2 = 4$". This implication is true because the conclusion $2 + 2 = 4$ is true whatever Martians exist or not.

Vacuous Proof

We can quickly prove that the conditional statement $p \rightarrow q$ is true when we know that the hypothesis p is false, because $p \rightarrow q$ must be true when p is false. Consequently, if we can show that p is false, then we have a proof, called a **vacuous proof**, of the conditional statement $p \rightarrow q$.

Example:
If it rains and it does not rain, then Martians exist.

If the hypothesis is false, the implication is true whatever the truth value of the conclusion.

Proof of Equivalence

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. The validity of this approach is based on the tautology

$$(p \leftrightarrow q) \equiv ((p \rightarrow q) \wedge (q \rightarrow p))$$

For example, suppose that n is a positive integer. To prove that

"n is odd if and only if n^2 is odd"

is equivalent to prove that

"if n is odd, then n^2 is odd"

and conversely

"if n^2 is odd, then n is odd".

Fallacy Using Circular Reasoning

Many incorrect arguments are based on a fallacy called **begging the question**. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved. In other words, this fallacy arises when a statement is proved using itself, or a statement equivalent to it. That is why this fallacy is also called **circular reasoning**.

Proof by Cases

We want to prove the implication $p \rightarrow q$. When the hypothesis p can be put into an expression

$$p_1 \vee p_2 \vee \ldots \vee p_n,$$

then showing the implication

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

becomes equivalent to prove each of the n conditional statements

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q).$$

This proof method, called **proof by cases**, comes from the tautology

$$((p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q) \equiv ((p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)).$$

Exhaustive Proof

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called **exhaustive proofs**, because these proofs proceed by exhausting all possibilities. An exhausting proof is a special type of proof by cases where each case involves checking a single example.

Existence Proof Methods

Many theorems are assertions that objects of a particular type exist. A theorem of this type is a proposition of the form $\exists x\, P(x)$, where P is a predicate. A proof of a proposition of the form $\exists x\, P(x)$ is called an **existence proof**. There are several ways to prove a theorem of this type:

- Constructive existence proof
- Non constructive existence proof
- Proof of non existence by counterexample

Constructive Existence Proof

To prove that $\exists x\, P(x)$,

- find an element c in the universe of discourse such that $P(c)$ is true.
- Then, $\exists x\, P(x)$ is true using existential generalization.

Theorem

There exists an integer solution to the equation $x^2 + y^2 = z^2$.

Sketch of proof: Choose $x = 3$, $y = 4$ and $z = 5$.

Non Constructive Existence Proof

It can be shown that $\exists x\, P(x)$ without providing an element c such that $P(c)$ is true. The existence proof is then said to be non constructive.

A proof by contradiction can be used, i.e. by showing that the negation of the existential quantification implies a contradiction.

Proof of Non Existence by Contradiction

It can be shown that $\neg\exists x\, P(x)$ (which is equivalent to $\forall x\, \neg P(x)$) using a proof by contradiction. It is assumed there exists a c such that $P(c)$, and a contradiction is deduced from this assumption.

(Last) Fermat's Theorem

Many advances in mathematics have been made by people trying to solve famous unsolved problems. The most famous one is from Pierre de Fermat (1601–1665) and was unsolved for more than 300 years.

Theorem

The equation

$$x^n + y^n = z^n$$

has no integer solution for x, y and z with $xyz \neq 0$, for any integer n such that $n > 2$.

The $3x + 1$ Mapping

Let T be the mapping : every even integer x is sent into $x/2$ and every odd integer x is sent into $3x + 1$. The conjecture says that, given any positive integer x, when the mapping T is iterated, it eventually reaches the integer 1.

Example. When $x = 11$, one has $T(11) = 3 \cdot 11 + 1 = 34$;
$T(34) = 34/2 = 17$; $T(17) = 3 \cdot 17 + 1 = 52$; $T(52) = 52/2 = 26$;
$T(26) = 26/2 = 13$; $T(13) = 3 \cdot 13 + 1 = 40$; $T(40) = 40/2 = 20$;
$T(20) = 20/2 = 10$; $T(10) = 10/2 = 5$; $T(5) = 5 \cdot 3 + 1 = 16$;
$T(16) = 16/2 = 8$; $T(8) = 8/2 = 4$; $T(4) = 4/2 = 2$;
$T(2) = 2/2 = 1$.

Goldbach Conjecture (1742)

Christian Goldbach (1690–1764)

All positive even integers $>= 4$ can be expressed as the sum of two primes.

Examples: $4 = 2 + 2$. $6 = 3 + 3$. $8 = 5 + 3$. $10 = 7 + 3$.
$12 = 7 + 5$. $14 = 7 + 7$. $16 = 13 + 3$. $18 = 11 + 7$. $20 = 13 + 7$.
$22 = 19 + 3$. $24 = 19 + 5$. $26 = 23 + 3$. Etc

Twin Prime Conjecture

Prime numbers are called twins when they differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, 4967 and 4969.

The twin prime conjecture says there are an infinite number of such pairs.