Lecture-7

Methods of proofs

Some terminology

- **Theorem**: a statement that can be shown to be true (sometimes referred to as facts or results).
- Less important theorems are often called **propositions**.
- A **lemma** is a less important theorem, used as an auxiliary result to prove a more important theorem.
- A **corollary** is a theorem proven as an easy consequence of a theorem.
- A **conjecture** is a statement that is being proposed as a true statement. If later proven, it becomes a theorem, but it may be false.

Some terminology

- **Axiom** (or postulates) are statements that we assume to be true (algebraic axioms specify rules for arithmetic like commutative laws).
- A **proof** is a valid argument that establishes the truth of a theorem.
- **Rules of inference**: The statements used in a proof include axioms, hypotheses (or premises), and previously proven theorems., together with definition of terms, are used to draw conclusions from other assertions, tying together the steps of a proof.

Methods of proving theorems

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, we use the steps:

1. Take an arbitrary element c of the domain and show that $(P(c) \rightarrow Q(c))$ is true.
2. Apply universal generalization to conclude $\forall x(P(x) \rightarrow Q(x))$.

3 Methods of showing statements of the type $p \rightarrow q$ to be true

1. **Direct proofs**: Assume p is true; the last step establishes q is true.
2. **Proof by Contraposition**: Uses a direct proof of the contrapositive of $p \rightarrow q$, which is $\neg q \rightarrow \neg p$. That is, assume $\neg q$ is true; the last step established $\neg p$ is true.
3. **Proof by Contradiction**: To prove that P is true, we assume $\neg P$ is true and reach a contradiction, that is that $(r \wedge \neg r)$ is true for some proposition r. In particular, to prove $(p \rightarrow q)$, we assume $(p \rightarrow q)$ is false, and get as a consequence a contradiction. Assuming that $(p \rightarrow q)$ is false $= (\neg p \vee q)$ is false $= (p \wedge \neg q)$ is true.

Direct Proofs

A formal direct proof of a conditional statement p → q works as follows:

assume p is true, build steps using inference rules, with the final step showing that q is true.

In a (informal) direct proof, we assume that p is true, and use axioms, denitions and previous theorems, together with rules of inference to show that q must be true.

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.

Give a direct proof of the following theorem.

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

Observations: We want to show that $\forall x(P(x) \rightarrow Q(x))$,

where P(x) is “n is an odd integer" and Q(x) is “n^2 is odd".

Proof:

Let n be an odd integer.

By definition of odd, we know that there exists an integer k such that

$n = 2k + 1$.

Squaring both sides of the equation, we get

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

Since $n^2 = 2k0 + 1$, where $k0 = 2k^2 + 2k$, by the definition of odd we conclude n^2 is odd.

Exercise:

Prove the following theorem using a direct proof.

Theorem

If m and n are both perfect squares, then mn is also a perfect square.

Definition

An integer a is a perfect square if there is an integer b such that $a = b^2$.

Proof by Contraposition

This method of proof makes use of the equivalence

$(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$.

In a proof by contraposition that $p \rightarrow q$, we assume $\neg q$ is true, and using axioms, definitions and previously proven theorems, together with inference rules, we show that $\neg p$ must be true.

(It is a direct proof of the contrapositive statement!)

Prove the Theorem by contraposition

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

Proof: We prove the statement by contraposition.

Assume n is even (assuming $\neg q$). Then, by definition,

$n = 2k$ for some integer k.

Thus, $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.

So, we have that $3n + 2 = 2k0$ where $k0 = 3k + 1$,

which means $3n + 2$ is an even number.

This is the negation of the hypothesis of the theorem ($\neg p$),

which concludes our proof by contraposition.

When to use each type of proof?

Usually try a direct proof. If it doesn't work, try a proof by contraposition

Prove that for any integer number n, if n^2 is odd, then n is odd. using direct as well as proof by contraposition

Trying a direct proof.

Let n be an integer number. Assume that n^2 is odd. We get next that there exists an integer k such that $n^2 = 2k + 1$. Solving for n produces the equation

$$n = \pm\sqrt{2k+1}$$

which is not very useful to show that n is odd.

Try a prove by contraposition.

Let n be an integer number. Assume n is not odd. This means that n is even, and so there exists an integer k such that $n = 2k$. Thus, $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. So, taking $k0 = 2k^2$, we see that $n^2 = 2k0$ and so n^2 is even. This concludes our proof by contraposition.

Proof by Contradiction

- In a proof by contradiction, we prove that a proposition p is true, by showing that there exists a contradiction q such that $\neg p \rightarrow q$.

- We can prove that p is true by showing for instance that $\neg p \rightarrow (r \wedge \neg r)$, for some proposition r.

Proof by Contradiction

- **If n is an integer and 3n + 2 is odd, then n is odd.**
- p: 3n + 2 is odd
- q: n is odd
- Let $\neg q$ is true that is n is even.
- Then n = 2k for some integer k
- It follows that 3n+2 = 3(2k) + 2 = 6k+2 = 2(3k+1)
- Therefore 3n+2 is even which contradict with p .

Thank you