Introduction to Proofs

Section 1.6

Definition

- Proof: is a valid argument that establishes the truth of a mathematical statement.

- It may use axioms, hypothesis, rules of inference, other propositions (facts), lemmas, corollaries, & theorems.

Proof

Formal

Long

Difficult to construct & read

Informal

Short

Easy to construct & read

Definitions

- Axioms (postulates) are statements that can be assumed to be true.
- Theorem: is a statement that can be proven to be true.
- Conjecture: is a statement that one believe it is true, but has not been proven yet.
- Less Important theorems are called
  - Proposition
  - Lemma: if used to prove other theorems
  - Corollary: if concluded from a theorem

Remark

- Mathematicians usually don’t use universal quantifiers (or universal instantiation or generalization) explicitly.

Example

- $\forall x \ (P(x) \rightarrow Q(x))$ will be written as

If P(x), then Q(x) where x belongs to its domain.

- When we try to prove it, we should show that $P(c) \rightarrow Q(c)$ for arbitrary c in the domain.

Proof Techniques

1. Direct Proofs
2. Indirect Proofs
    1. Proof by contraposition
    2. Proof by contradiction

Direct Proofs

- For: "$p \rightarrow q$" Or $\forall x \ (P(x) \rightarrow Q(x))$

To prove such statements

- assume that p (or P(c)) is true
- use all possible facts, lemmas, theorems, and rules of inferences
- and try to show that q (or Q(c)) is true.

Definition

1. $n \in Z$ is even $\leftrightarrow \exists\, k \in Z$ s.t. $n = 2k$
2. $n \in Z$ is odd $\leftrightarrow \exists\, k \in Z$ s.t. $n = 2k+1$
3. $n \in Z$ is a perfect square $\leftrightarrow n = k^2$ for some $k \in Z$.

Note: $n \in Z \rightarrow$ n is even $\oplus$ n is odd

Theorem

If $n \in Z$ is odd, then n^2 is odd,

i.e., $\forall\, n \in Z\ (n \text{ is odd} \rightarrow n^2 \text{ is odd})$

Proof. (Direct)

- Assume that $n \in Z$ is odd, then by definition $\exists\, k \in Z$ s.t. $n=2k+1$
- Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$

$$= 2(2k^2 + 2k) + 1 = 2m + 1$$

And so n^2 is odd.

Theorem

If n, m $\in$ Z are perfect squares, then nm is also a perfect square.

Proof. (direct)

- Let n, m be perfect squares.
- Then $n=k^2$ and $m=l^2$ for some k, l $\in$ Z.
- Then $nm=k^2 l^2= (k\,l)^2$.
- And so nm is a perfect square.

Indirect Proofs.

Proof by contraposition:

- Note that $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- So to prove $p \rightarrow q$ we need to assume $\neg q$ and try to prove $\neg p$

Examples

1. If $n \in Z$ and $3n+2$ is odd, then n is odd

Proof. (by contraposition)

- Assume that n is even
- Then $n = 2k$ for some integer k
- So $3n+2 = 6k + 2 = 2(3k+1) = 2m$
- Thus $3n+2$ is even

Examples

2. If $n = a\,b$ where a & b are positive integers, then

$$a \le \text{sqrt}(n) \quad \text{or} \quad b \le \text{sqrt}(n)$$

Proof. (by contraposition)

- assume $a > \text{sqrt}(n)$ & $b > \text{sqrt}(n)$
- Then $a\,b > n$, i.e., $a\,b \neq n$

Vacuous & Trivial Proofs

Consider $p \rightarrow q$

- Vacuous Proof: if p is false then the statement is always true.

- Trivial Proof: if q is true then the statement is always true.

Examples

- If $0>1$, then $n^2 > n$ for any integer n.

(vacuous)

- If $a > b$, then $a^2 \geq 0$.

(trivial)

Definition

- Any real number r is rational iff there are two integers n and m s.t. $m \neq 0$ and $r = n/m$.
- r is irrational iff it is not rational.

- We write Q for the set of all rational.

Theorem

$\forall$ x, y$\in$Q, x + y$\in$Q

Or $\forall$ x, y$\in$R (x,y $\in$Q $\rightarrow$ x + y$\in$Q)

Proof. (direct)

- Let x, y$\in$Q.
- Then $x = n_1/m_1$ and $y = n_2/m_2$,
  and $m_1 \neq 0 \neq m_2$
- Then $x+y = n_1/m_1 + n_2/m_2$
  $= (n_1m_2 + n_2m_1)/(m_1m_2)$
- So x + y$\in$Q

Theorem

If $n \in Z$ and n^2 is odd, then n is odd

Proof

Direct: $n^2 = 2k+1$, and so

$n = sqrt(2k+1)$, and then ....???

Contraposition:

n is even $\rightarrow n = 2k \rightarrow n^2 = 4\,k^2 = 2(2k^2)$

$\rightarrow n^2$ is even

Proofs by contradiction

- To prove that p is true, we show that $\neg p$ leads to some kind of a contradiction=F proposition like $(r \wedge \neg r)$=F.
- To prove that $p \rightarrow q$ by contradiction, we assume that p is true & q is false and try to get a contradiction, i.e., $(p \wedge \neg q) \rightarrow$F.

Example

Sqrt(2) is irrational.

Proof. (by contradiction)

- Assume not, i.e., sqrt(2) = n/m for some integers n and $m \neq 0$.
- We can assume that n and m have no common factors.
- Then $2 = n^2/m^2$, or indeed $2\ m^2 = n^2$
- Which means that n^2 is even
- So n is even (by theorem)

Continue ..

- So $n = 2k$ and hence $n^2 = 4k^2 = 2m^2$
- Or $2k^2 = m^2$, and so m^2 is even
- This means that both n and m are even,
- i.e., they have a common factors! Which is a contradiction with what we have assume at the beginning.

Theorem

- n is even iff n^k is even for any integer k>1.
- n is odd iff n^k is odd for any integer k>1.
- Proof.
- Exercise

Theorem

At least 4 of any 22 days must fall on the same day of week

Proof: (by contradiction)

- Assume not, i.e., each day of the week is repeated at most 3 times.
- Then the number of days is $\leq 3 \times 7 = 21$ days, which is a contradiction.

Theorem

The following are equivalent

- P: n is even
- Q: n-1 is odd
- R: n^2 is even

- This means that $P \leftrightarrow Q \leftrightarrow R$
- OR $(P \rightarrow Q) \wedge (Q \rightarrow R) \wedge (R \rightarrow p)$

Proof

- (P) n is even $\rightarrow$ n = 2k

$\rightarrow$ n-1 = 2k-1 = 2(k-1) + 1

$\rightarrow$ n-1 is odd (Q)

- (Q) n-1 is odd $\rightarrow$ n-1 = 2k+1

$\rightarrow$ n = 2(k+1) $\rightarrow$ $n^2 = 2\ (2\ (k+1)^2)$

$\rightarrow$ n^2 is even (R)

- (R) n^2 is even $\rightarrow$ n is even (P)

Counter Examples

- Every positive integer is the sum of the squares of two integers.
- Not true:

Proof: (by counter example)

- Consider 3 and notice that 3=2+1=3+0
- And so it's not a sum of two squares.

Mistakes in Proofs

Be careful of

- Fallacy of affirming the conclusion
- Fallacy of denying the hypothesis
- Fallacy of begging the question (or circular reasoning)

- Read about this in section 1.6.

Mistakes in Proofs

- Theorem: 1 = 2
- Proof:
- Let a and b be equal integers
- Then $a = b$ and so $a^2 = ab$
- so $a^2 – b^2 = ab – b^2$
- $(a-b)(a+b) = b(a-b)$
- $a+b = b$
- $2b = b$
- 2=1 !!!