Proofs

CIS008-2 Logic and Foundations of Mathematics

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

12:00, Friday 4th November 2011

Outline

1. Math Systems
2. Direct
3. Counterexamples
4. Contradiction
5. Contrapositive
6. Cases
7. Equivalence
8. Existance

Mathematical Systems

Axioms That which is assumed to be true.

Definitions Used to create new concepts in terms of existing ones.

Theorem A proposition that has been proved to be true.

Lemma A theorem that is not interesting in its own right, but useful in proving another theorem.

Corollary A theorem that follows easily from another theorem.

An Example of definitions and axioms

Example (*We present some **axioms** of real numbers*)

- For all real numbers x and y, $xy = yx$
- There is a subset **P** of real numbers satisfying
  - If x and y are in **P**, then $x + y$ and xy are in **P**.
  - If x is a real number, then exactly one of the following statements are true
    - x is in **P**.
    - $x = 0$.
    - $-x$ is in **P**.

Axioms That which is assumed to be true.

Definitions Used to create new concepts in therms of existing ones.

An Example of definitions and axioms

Example (*We present some **axioms** of real numbers*)

- For all real numbers x and y, $xy = yx$
- There is a subset **P** of real numbers satisfying
  - If x and y are in **P**, then $x + y$ and xy are in **P**.
  - If x is a real number, then exactly one of the following statements are true
    - x is in **P**.
    - $x = 0$.
    - $-x$ is in **P**.

- Multiplication is implicitly defined by the first axiom.
- The elements of **P** are called positive real numbers.
- The *absolute value* $|x|$ of a real number x is defined to be x if x is positive or 0 and $-x$ otherwise.

An Example of Theorems

Example (*We present some* ***theorems*** *of real numbers*)

- $x.0 = 0$ for every real number x.
- For all real numbers x, y and z, if $x \leq y$ and $y \leq z$, then $x \leq z$.
- If n is a positive integer, then either $n - 1$ is a positive integer or $n - 1 = 0$.

Theorem A proposition that has been proved to be true.

Lemma A theorem that is not interesting in its own right, but useful in proving another theorem.

Corollary A theorem that follows easily from another theorem.

PROOFS

R. Boas

"Only professional mathematicians learn anything from proofs. Other people learn from explanations."

Direct proofs

Theorem (example theorem)

For all $x_1, x_2, \ldots, x_n$*, if* $p(x_1, x_2, \ldots, x_n)$*, then* $q(x_1, x_2, \ldots, x_n)$.

A **direct proof** assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then, using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions, previously derived theorems, and rules of inference, shows directly that $q(x_1, x_2, \ldots, x_n)$ is true.

In a direct proof we assume the hypotheses and derive the conclusion.

Direct proof example

Definition of even and odd integers

An integer n is even if there exists an integer k such that $n = 2k$.
An integer n is odd if there exists an integer k such that $n = 2k - 1$.

Theorem (example theorem)

For all integers m and n, if m is odd and n is even, then $m + n$ is odd.

University of Bedfordshire

Direct proof example

HYPOTHESIS m is odd and n is even

PROOF . . .

CONCLUSION $m + n$ is odd

Direct proof example

HYPOTHESIS m is odd and n is even

DEFINITION there exists an integer k_1 such that $m = 2k_1 - 1$

DEFINITION there exists an integer k_2 such that $n = 2k_2$

PROOF ...

CONCLUSION $m + n$ is odd

Direct proof example

HYPOTHESIS m is odd and n is even

DEFINITION there exists an integer k_1 such that $m = 2k_1 - 1$

DEFINITION there exists an integer k_2 such that $n = 2k_2$

PROOF $m + n = (2k_1 - 1) + 2k_2 = 2(k_1 + k_2) - 1, \ldots$

CONCLUSION $m + n$ is odd

Direct proof example

HYPOTHESIS m is odd and n is even

DEFINITION there exists an integer k_1 such that $m = 2k_1 - 1$

DEFINITION there exists an integer k_2 such that $n = 2k_2$

PROOF $m + n = (2k_1 - 1) + 2k_2 = 2(k_1 + k_2) - 1$, thus there exists and integer $k = k_1 + k_2$ such that $m + n = 2k - 1$.

CONCLUSION $m + n$ is odd

University of Bedfordshire

Counterexample

If the following is true, prove it; otherwise give a counterexample.

Theorem

$$(A \cap B) \cup C = A \cap (B \cup C)$$

Counterexample

HYPOTHESIS A, B, and C are sets.

DEFINITION If $x \in (A \cap B) \cup C$ then $x \in (A \cap B)$ or $x \in C$

DEFINITION If $x \in A \cap (B \cup C)$ then $x \in A$ and $x \in (B \cup C)$

PROOF ...

CONCLUSION $(A \cap B) \cup C = A \cap (B \cup C)$

University of Bedfordshire

Counterexample

Hypothesis A, B, and C are sets.

Definition If $x \in (A \cap B) \cup C$ then $x \in (A \cap B)$ or $x \in C$

Definition If $x \in A \cap (B \cup C)$ then $x \in A$ and $x \in (B \cup C)$

Disproof "$x \in (A \cap B)$ or $x \in C$" is true if $x \in C$ and "$x \in A$ and $x \in (B \cup C)$" is false if $x \notin A$.

Conclusion $(A \cap B) \cup C \neq A \cap (B \cup C)$

Counterexample

Let $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$, and $C = \{3, 4, 5\}$ (from the previous disproof, we construct the sets such that there is an element in C that is not in A).

$$(A \cap B) \cup C = \{2, 3, 4, 5\}$$

$$A \cap (B \cup C) = \{2, 3\}$$

Therefore $(A \cap B) \cup C \neq A \cap (B \cup C)$.

Proof by contradiction

Theorem (example theorem)

For all $x_1, x_2, \ldots, x_n$*, if* $p(x_1, x_2, \ldots, x_n)$*, then* $q(x_1, x_2, \ldots, x_n)$*.*

A **proof by contradiction** assumes that $p(x_1, x_2, \ldots, x_n)$ is true and then, using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions, previously derived theorems, and rules of inference, shows a contradiction in that $q(x_1, x_2, \ldots, x_n)$ is **false**.

A proof by contradiction (sometimes call an indirect proof) is essentially the same as a direct proof, except we assume the the conclusion to be false (whereas we assume the conclusion true in a direct proof).

Proof by contradiction example

Definition of even and odd integers

An integer n is even if there exists an integer k such that $n = 2k$.
An integer n is odd if there exists an integer k such that $n = 2k - 1$.

Theorem (example theorem)

For every $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof by contradiction example

HYPOTHESIS n^2 is even

PROOF . . .

CONTRADICTION n is **not** even

Proof by contradiction example

HYPOTHESIS n^2 is even

DEFINITION there exists an integer k such that $n = 2k - 1$

PROOF ...

CONTRADICTION n is **not** even

Proof by contradiction example

HYPOTHESIS n^2 is even

DEFINITION there exists an integer k such that $n = 2k - 1$

PROOF $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(k^2 - 2k + 1) - 1, \ldots$

CONTRADICTION n is **not** even

Proof by contradiction example

Hypothesis n^2 is even

Definition there exists an integer k such that $n = 2k - 1$

Proof $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(k^2 - 2k + 1) - 1$, thus n^2 is odd.

Contradiction n is **not** even

n^2 is odd when n is odd, which contradicts the hypothesis n^2 is even. The proof by contradiction is complete. We have proved that for every $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof by Contrapositive

Suppose we are given a proof by contradiction of as in the previous example

Theorem (example theorem)

For all $x_1, x_2, \ldots, x_n$, if $p(x_1, x_2, \ldots, x_n)$, then $q(x_1, x_2, \ldots, x_n)$.

and we prove the contradiction, when $q(x_1, x_2, \ldots, x_n)$ is false. In effect we have proved that if $q(x_1, x_2, \ldots, x_n)$ is false, then $p(x_1, x_2, \ldots, x_n)$ is false. This special case of proof by contradiction is called **proof by contrapositive**.

The difference between the two is that a proof by contradiction can be devised, but a proof by contrapositive is requested.

Proof by Contrapositive example

Theorem (example theorem)

For all $x \in \mathbb{R}$, if x^2 is irrational, then x is irrational.

Proof by Contrapositive example

Contrapositive hypothesis x is **not** irrational

Proof . . .

Contrapositive conclusion x^2 is **not** irrational

Proof by Contrapositive example

Contrapositive hypothesis x is rational

definition $x = p/q$ for integers p and q.

proof ...

Contrapositive conclusion x^2 is rational

University of Bedfordshire

Proof by Contrapositive example

Contrapositive hypothesis x is rational

definition $x = p/q$ for integers p and q.

proof $x^2 = p^2/q^2$ is the quotient of integers, so x^2 is rational

Contrapositive conclusion x^2 is rational

University of Bedfordshire

Proof by Cases

Theorem (example theorem)

For all $x_1, x_2, \ldots, x_n$*, if* $p(x_1, x_2, \ldots, x_n)$*, then* $q(x_1, x_2, \ldots, x_n)$.

Proof by Cases example

Theorem (example theorem)

Prove that $2m^2 + 3n^2 = 40$ has no solution in positive integers.

(i.e. $2m^2 + 3n^2 = 40$ is false for all positive integers m and n)

Proof by Cases example

HYPOTHESIS $2m^2 + 3n^2 = 40$

PROOF ...

CONCLUSION $2m^2 + 3n^2 = 40$ has no solution in positive integers

Proof by Cases example

HYPOTHESIS $2m^2 + 3n^2 = 40$

DEFINITION $2m^2 \leq 40$

DEFINITION $3n^2 \leq 40$

PROOF ...

CONCLUSION $2m^2 + 3n^2 = 40$ has no solution in positive integers

Proof by Cases example

HYPOTHESIS $2m^2 + 3n^2 = 40$

DEFINITION $m^2 \leq 20$

DEFINITION $n^2 \leq 40/3$

CASE PROOF check $m = 1, 2, 3, 4$ and $n = 1, 2, 3$ in the table below

CONCLUSION $2m^2 + 3n^2 = 40$ has no solution in positive integers

All 16 possible cases below show that $2m^2 + 3n^2 = 40$ *has no solution in positive integers.*

	1	**2**	**3**	**4**
1	5	11	21	35
2	14	20	30	44
3	29	30	45	59

University of Bedfordshire

Proof by Equivalence

Theorem (example theorem)

p if and only if q

Theorems of this form are proved by equivalence, that is, to prove "p if and only if q", prove "if p then q" and "if q then p".

Existance Proofs

Theorem (example theorem)

Prove that there is a prime p such that $2^p - 1$ is composite (i.e. not prime)

By trial and error, we find that $2^p - 1$ is prime for $p = 2, 3, 5, 7$ but not for $p = 11$.

$$2^{11} - 1 = 2048 - 1 = 2047 = 23 \times 89$$