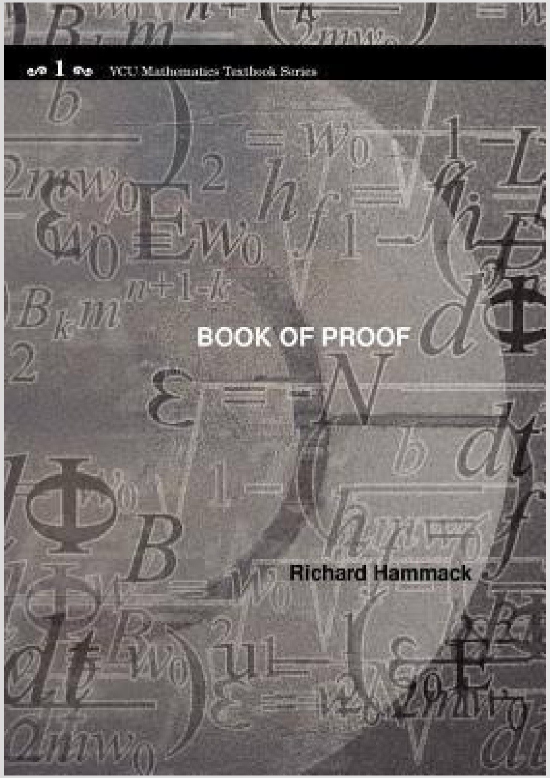
EDAA40

Discrete Structures in Computer Science

8: A few words on proofs

Jörn W. Janneck, Dept. of Computer Science, Lund University



This lecture is based on parts II and III of Richard Hammack's "Book of Proof".

definitions, theorems, proofs

A definition is a statement that gives a precise meaning to a term or a symbol.

$$A \subseteq B \text{ iff } \forall x\ (x \in A \to x \in B)$$

$$n \in \mathbb{Z} \text{ is } \textit{even} \text{ iff } \exists k \in \mathbb{Z}\ (n = 2k)$$

$$n \in \mathbb{Z} \text{ is } \textit{odd} \text{ iff } \exists k \in \mathbb{Z}\ (n = 2k + 1)$$

A theorem is a statement that needs to be proven based on definitions (and axioms).

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

$$\#(\mathbb{N}) < \#(2^{\mathbb{N}})$$

There are infinitely many prime numbers.

Other words for theorem: proposition, lemma, corollary.

A proof is a is a chain of logical reasoning showing the truth of a theorem.

kinds of proofs

Proofs come in different flavors, which depend on the form of the theorem, and the chain of reasoning best suited to prove it.

Many theorems are conditional statements, i.e. they have the form "premise implies conclusion, or

$$P \to C$$

$$\forall x \in \mathbb{Z}\ (x \text{ is odd } \to x^2 \text{ is odd})$$

$$\forall a, b, c \in \mathbb{Z}\ ((a|b \wedge b|c) \to a|c)$$

P	C	$P \to C$
T	T	T
T	F	F
F	T	T
F	F	T

direct proof

Theorem: If P, then C.

Proof: Suppose P.

…

Therefore C.

Theorem:

$$x \text{ is odd } \to x^2 \text{ is odd}$$

Proof:

Suppose x is odd.

Therefore, there is an integer k such that $x = 2k + 1$.

Thus $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Note that $2k^2 + 2k$ is an integer.

Thus there is an integer n such that $x^2 = 2n + 1$.

Therefore x^2 is odd.

direct proof with cases

Sometimes, the premise consists of several *cases*, and it becomes easier to study each case by itself.

n	$1+(-1)^n(2n-1)$
1	0
2	4
3	-4
4	8
5	-8
6	12

Theorem: If $n \in \mathbb{N}$ then $1+(-1)^n(2n-1)$ is a multiple of 4.

Proof: Suppose $n \in \mathbb{N}$. Then n is either even or odd.

Case 1: Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$.
Thus $1+(-1)^{2k}(2(2k)-1) = 1+1^k(4k-1) = 4k$.
That is a multiple of 4.

Case 2: Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$.
Thus $1+(-1)^{2k+1}(2(2k+1)-1) = 1-(4k+2-1) = -4k$.
That is also a multiple of 4.

The result in both cases is a multiple of 4.

contrapositive proof

In some cases, it is easier to reason about a theorem in *contrapositive* form.

Theorem:

If $x^2 - 6x + 5$ is even, then x is odd.

Proof:

Suppose $x^2 - 6x + 5$ is even, i.e. there exists an integer a such that $x^2 - 6x + 5 = 2a$.

...

Thus there is an integer b such that $x = 2b + 1$.

Therefore b is odd.

direct proof:

Theorem: If P, then C.

Proof: Suppose P.

…

Therefore C.

contrapositive proof

Contrapositive form: $\neg C \rightarrow \neg P$

P	C	$P \rightarrow C$	$\neg C$	$\neg P$	$\neg C \rightarrow \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Theorem: If P, then C.

Proof: Suppose not C.

…

Therefore not P.

Theorem:

If $x^2 - 6x + 5$ is even, then x is odd.

Proof:

Suppose x is even.

There is an integer a such that $x = 2a$.

$x^2 - 6x + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$

So there is an integer b s.t. $x^2 - 6x + 5 = 2b + 1$.

Therefore $x^2 - 6x + 5$ is not even.

proof by contradiction

Suppose we want to prove a proposition P, not necessarily in conditional form.

Proof by contradiction uses the fact that if we can show that not P results in a logical contradiction, e.g. it implies some conclusion C as well as its opposite, not C, then not P cannot be true, and so P must be true.

P	C	$\neg P$	$C \wedge \neg C$	$\neg P \to C \wedge \neg C$
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

Theorem:

$$\text{If } a, b \in \mathbb{Z} \text{ then } a^2 - 4b \neq 2.$$

Proof:

Suppose there are $a, b \in \mathbb{Z}$ s.t. $a^2 - 4b = 2$.

Since this implies $a^2 = 4b + 2 = 2(2b + 1), a^2$ is even.

Hence a is even, so $a = 2c$ for some integer c.

Thus $4c^2 - 4b = 2$, i.e. $2c^2 - 2b = 1$.

Therefore $2(c^2 - b) = 1$ with $c^2 - b \in \mathbb{Z}$.

So 1 is even.

Theorem: P.

Proof: Suppose not P.

…

Or any other false proposition!

Therefore C and not C.