VANDERBILT UNIVERSITY School of Engineering

Discrete Structures

CS 2212

(Fall 2020)

7 – Proofs

Proofs – By Contradiction

General Approach:

1. Suppose the statement to be proved is false, that is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Proofs – By Contradiction

General Approach:

We need to show $P \rightarrow Q$.

Assume $\neg Q$.

contradiction

Then, we show that $(P \land \neg Q) \rightarrow (r \land \neg r)$ for some statement r.

Why this approach works?

- We showed that $P \land \neg Q$ is always false (as it leads to a contradiction).
- Since P is given and is true, so $\neg Q$ must be false.
- That means Q is true, which is the desired statement.

Proofs – By Contradiction

General Approach:

We need to show $P \rightarrow Q$.

Assume $\neg Q$.

Then, we show that $(P \wedge \neg Q) \rightarrow (r \wedge \neg r)$ for some proposition r.

- Do you see any similarity / difference with the **proof by contraposition?**
- Which one is more general?
- Proof by contradiction is a very useful approach.

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement) Assume there is at least one integer n that is both even and odd.
(Now try to deduce a contradiction) Thus, $n = 2a$ for some integer a (by the definition of even integer)
Similarly, $n = 2b + 1$ for some integer b (by the definition of odd)
Consequently, $2a = 2b + 1$
And so, $2a - 2b = 1$
$2(a - b) = 1$
$a - b = 1/2$
Since, a and b are integers, their difference must be integer. But, here $(a - b)$ is not an integer, which is a contradiction. Hence, the given statement is true.

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)
So, $\frac{a}{b} + i = \frac{c}{d}$
$i = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$
Since a,b,c,d are integers, $(bc - ad)$ is an integer and bd is also an integer. Moreover, $bd \neq 0$ (by the zero product property).
This means that i is a rational number, which is a contradiction.
Thus, the given statement is true.

Proofs – By Contradiction

Prove:

$\sqrt{2}$ is an irrational number

Proofs – By Contradiction

Prove:

There is no greatest integer.

Proofs – By Cases

Approach:

Simply break down the domain into a few different classes and then give a proof for each class.

Examples:

1. Odd/even
2. < 0, =0, >0
3. Rational/irrational

Proofs – By Cases

Prove: For **every integer** x, the integer (x^2-x) is even.

We divide our domain into even and odd integers, prove the statement separately.

Case 1: x is even

1. Assume x is even
2. $x = 2k$ for some integer k
3. (rest of proof for case of x is even…substitute and solve)

Case 2: x is odd

1. Assume x is odd
2. $x = 2k+1$ for some integer k
3. (rest of proof for case of x is odd…substitute and solve)

Since we have demonstrated that x^2-x is an even integer in all possible cases, we can conclude that it is even. QED.

Proofs – By Cases

Prove: For any real numbers x and y, $|x+y| \leq |x| + |y|$

Recall:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{otherwise} \end{cases}$$

We consider two separate cases: $x+y \geq 0$ and $x+y < 0$.

Case 1: $x+y \geq 0$

Then,

$$\begin{aligned} |x+y| &= x+y \\ &\leq |x| + y \\ &\leq |x|+|y|. \end{aligned}$$

Case 2: $x+y < 0$

Then,

$$\begin{aligned} |x+y| &= -(x+y) \\ &= (-x) + (-y) \\ &\leq |x| + (-y) \\ &\leq |x|+|y|. \end{aligned}$$

If and Only If (Iff) Proofs

Prove:

P if and only if Q

$$P \leftrightarrow Q$$

P and Q are equivalent statements

Approach:

We need to prove both "directions", that is

$$P \rightarrow Q$$

and

$$Q \rightarrow P.$$

If and Only If (Iff) Proofs

Prove: x is an odd integer if and only if x^2 is an odd integer

If x is an odd integer, then x^2 is an odd integer (P → Q)

x is odd, which means $x = 2k + 1$. Thus,

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

Since $(2k^2 + 2k)$ is an integer, x^2 is odd by the definition of odd integer.

If x^2 is an odd integer, then x is an odd integer (Q → P)

We can prove it using any of the approaches we learned, but by contraposition works nicely here. How?

We rather prove: if x is even, then x^2 is even. (pretty easy)

Then, by contraposition, we have shown that, if x^2 is odd then x is odd.

This way we have proven in both directions, and hence the given statement is true.

Counterexamples

- We can **disprove** a statement by finding an example/case for which the statement is false. Such an example is called a **counterexample**.
- In other words, we can **prove** the statement

  "$\forall x$ P(x) is false"

  by finding a value of x for which P(x) is false. Such a value of x constitute a counterexample.

(By the way, can we prove a statement "$\forall x$ P(x) is true" through some examples?)

Counterexamples

Prove that the statement "Every positive integer is the sum of the squares of two integers" is **false**.

- Since we are trying to "disprove" a statement, we can try to look for a counterexample.
- Here **3** is a counterexample.
- Note that we have to formally show why **3** is a counterexample?
- In other words, we need to show that **3** cannot be written as the sum of the squares of two integers.

Counterexample Proof

Interesting and fun example: A 200 year old problem posed by Euler, was settled in 1966 by finding a counterexample. The paper also qualifies for one of the shortest (serious) papers in Mathematics.

COUNTEREXAMPLE TO EULER'S CONJECTURE ON SUMS OF LIKE POWERS

BY L. J. LANDER AND T. R. PARKIN

Communicated by J. D. Swift, June 27, 1966

A direct search on the CDC 6600 yielded

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

as the smallest instance in which four fifth powers sum to a fifth power. This is a counterexample to a conjecture by Euler [1] that at least n nth powers are required to sum to an nth power, $n > 2$.

REFERENCE

1. L. E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1952, p. 648.

Published in the Bulletin of the American Mathematical Society 72.6 (1966)

Some Proof Mistakes

What is wrong with this “proof”?

Theorem: If n^2 is positive, then n is positive.

“ Proof ”

Suppose that n^2 is positive. Because the conditional statement

“If n is positive, then n^2 is positive” is true,

we can conclude that n is positive.

(We are assuming if $(P \rightarrow Q)$, then $(Q \rightarrow P)$, which is incorrect in general.)

Some Proof Mistakes

What is wrong with this "proof"?

Theorem: If n is not positive, then n^2 is not positive.

" Proof "

Suppose that n is not positive. Because the conditional statement

"If n is positive, then n^2 is positive" is true,

we can conclude that n^2 is not positive.

(We are assuming if $(P \rightarrow Q)$, then $(\neg P \rightarrow \neg Q)$, which is incorrect in general.)

Example of a Simple Elegant Proof

Finally, lets conclude and treat ourselves by looking at one of the simplest, most elegant proofs (presented some 2000 years ago).

Theorem: There are infinitely many primes.

Lets prove it ….

(Also observe the flavor of contradiction, cases)

Example of a Simple Elegant Proof

Main Idea:

Assume we have a finite list of primes: $p_1, p_2, \ldots, p_n$

Lets consider a number $N = (p_1 p_2 \ldots p_n) + 1$.

Now this number is either prime or not.

Case 1: N is prime.

It means our finite list was missing a prime.

Case 2: N is not a prime.

It means N is divisible by some prime p_i. If p_i is not in our list, we again get a new prime and our list was not complete. So, we assume p_i is in our list. Then,

$$\frac{N}{p_i} = \frac{(p_1 p_2 \ldots p_n) + 1}{p_i} = \frac{(p_1 p_2 \ldots p_n)}{p_i} + \frac{1}{p_i} = \text{(not an integer)}$$

Thus, no prime in the list divides N. So, our list of primes is incomplete.

Subproof *

At some point in a proof, you decide you'd like to be able to derive a conditionality $X \to Y$ on a line, but you can't figure out how.

1. Add an assumption line consisting of X, then proceed using the rules.
2. Since X was only assumed (for the sake of showing $X \to Y$), shift the lines of the derivation to the right.
3. Keep deriving lines until you derive Y. At this point, we don't know whether X is actually true, since we just assumed it, but we have shown that:

   if X were true, then Y would be true.

So the subproof shows that the conditional statement $X \to Y$ can be validly inferred.

* Not in ZyBook.

Sub-proofs (Examples)

Prove: If a person has the flu then the person has fever and headache. Therefore, a person with the flu has a fever.

L: Person has the flu. **F**: Person has fever. **H**: Person has headache.

Prove: $(L \rightarrow (F \wedge H)) \rightarrow (L \rightarrow F)$

Statements	Assumptions	Reasons
1. $L \rightarrow (F \wedge H)$		Premise
2.	L	Premise $[L \rightarrow F]$
3.	$F \wedge H$	Modus Ponens, 1, 2
4.	F	Simplification, 3
5. $L \rightarrow F$		

Indicate the intent

Sub-proof: none of these lines can be used in the rest of the proof. Remember, we do not know the truth value of these propositions.

Sub-proofs*

Writing Style:

- When doing a sub-proof, **indent** the statements of the sub-proof.
- When you reach the conclusion, write down the sub-proof conclusion without indentation.
- Note that when the sub-proof is complete, the premise (of the sub-proof) is **discharged**.

Nested Subproofs:

As long as the rules for subproofs are followed, a single proof can have more than one subproof, and can even have subproofs within subproofs.

* Not in ZyBook.

Sub-proofs (Examples)

Prove: $(A \to B) \wedge (B \vee C \to D) \to (A \to D)$

Statements	**Assumptions**	**Reasons**
1. $A \to B$		Premise
2. $B \vee C \to D$		Premise
3.	A	Premise $[A \to D]$
4.	B	MP, 1, 3
5.	$B \vee C$	Addition, 4
6.	D	MP, 2, 5
7. $A \to D$		

Sub-proof