1 10110000100 0 10110000100 0 10110000100 0 10110000100 0 10110000100 0 1

CSCI 2824: Discrete Structures

Lecture 10: Introduction to Proofs

Rachel Cox

Department of Computer Science

Midterm 1 October 1st 6:30-8pm

Moodle : 30 Sept - 6 Oct

- Concept Guide
- Moodle problem set

Assume $a = b$ and neither are equal to 0.

$$ab = b^2$$

$$ab - a^2 = b^2 - a^2$$

$$a(b-a) = (b-a)(b+a)$$

$$a = b + a$$

$$a = a + a \quad \text{(since a=b)}$$

$$a = 2a$$

$$\therefore 1 = 2$$

*Check out exam archive on Piazza Resources tab

0 10110000100 0 10110000100 0 10110000100 0 10110000100 0 10110000100 0 0

Introduction to Proofs

So how do we prove a statement of the form $\forall x\ (P(x) \to Q(x))$?

1. Prove $P(c) \to Q(c)$ for **arbitrary** c
2. Conclude $\forall x\ (P(x) \to Q(x))$ by universal generalization

This is what we really do, but we don't usually verbalize Step 2

OK, so how to we prove $P(c) \to Q(c)$?

- Direct or Conditional Proof
- Contrapositive Proof
- Proof by Contradiction

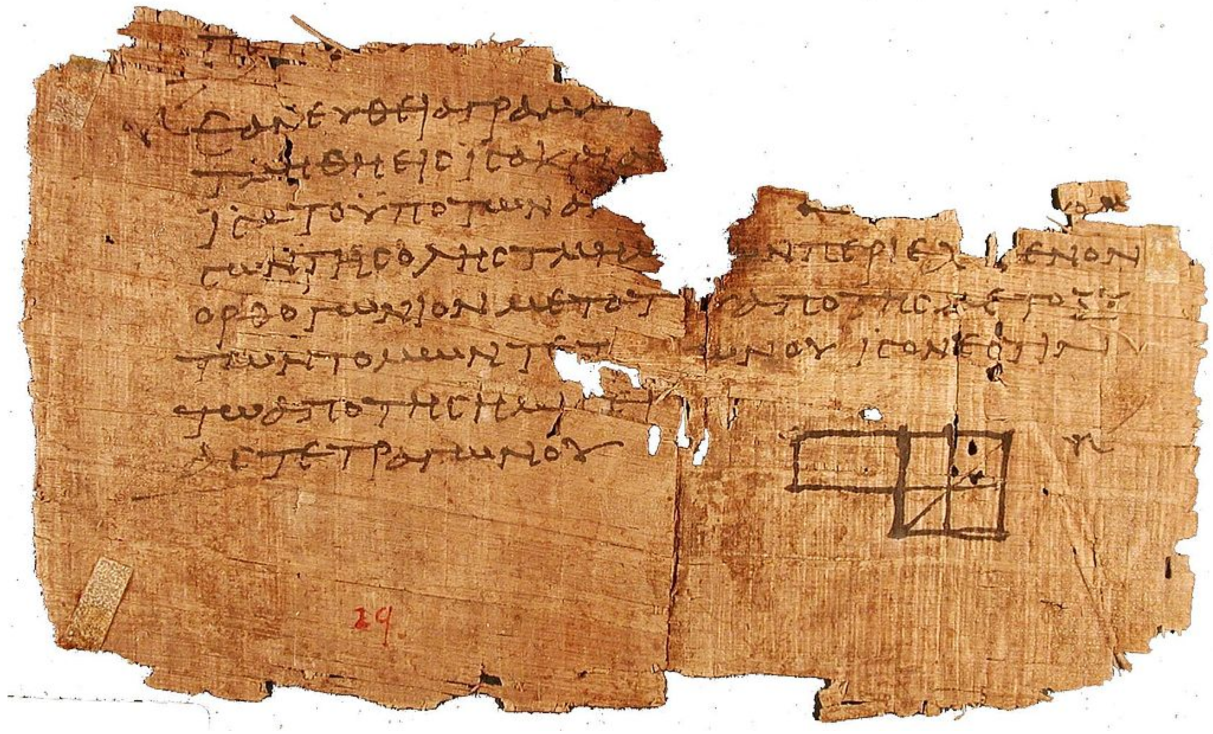
Introduction to Proofs

Direct Proof: We want to show that $p \to q$ is true.

check out appendix 1

Strategy:

- Assume p is true.
- Proceed through rules of inference, mathematical facts, axioms, etc. as necessary until we find that q is true.



A fragment from Euclid's *Elements*

Introduction to Proofs

Example: If a divides b and b divides c, then a divides c.

We will use a direct proof. Assume p, deduce q.

Proof: Assume that a divides b and b divides c. } Starting Assumption ①

$\frac{b}{a} = k$ and $\frac{c}{b} = m$ for some integers k, m and for arbitrary $a, b,$ and c. $a, b \neq 0$

② mathemat. facts & axioms

$b = a \cdot k$ $\quad c = b \cdot m$

$c = a \cdot k \cdot m$

$\frac{c}{a} = km$ where $km = \ell$ is an integer

$\Rightarrow \frac{c}{a} = \ell$

$\Rightarrow a$ divides c, as desired. ∎

③ concluding statement

Introduction to Proofs

Direct Proof.

Example: If n is a four–digit palindrome then n is divisible by 11.

palindrome
10101
3443

Pf: Assume that n is a four_digit palindrome.

$n = abba$ where $a = 1, 2, 3, 4, 5, 6, 7, 8, 9$ and
$b = 0, \ldots 9$

$$n = 1000a + 100b + 10b + a$$
$$= 1001a + 110b$$
$$= 11(91a + 10b)$$

since $91a + 10b = m$ for some integer m

then $n = 11m$ which implies that $\frac{n}{11} = m$.

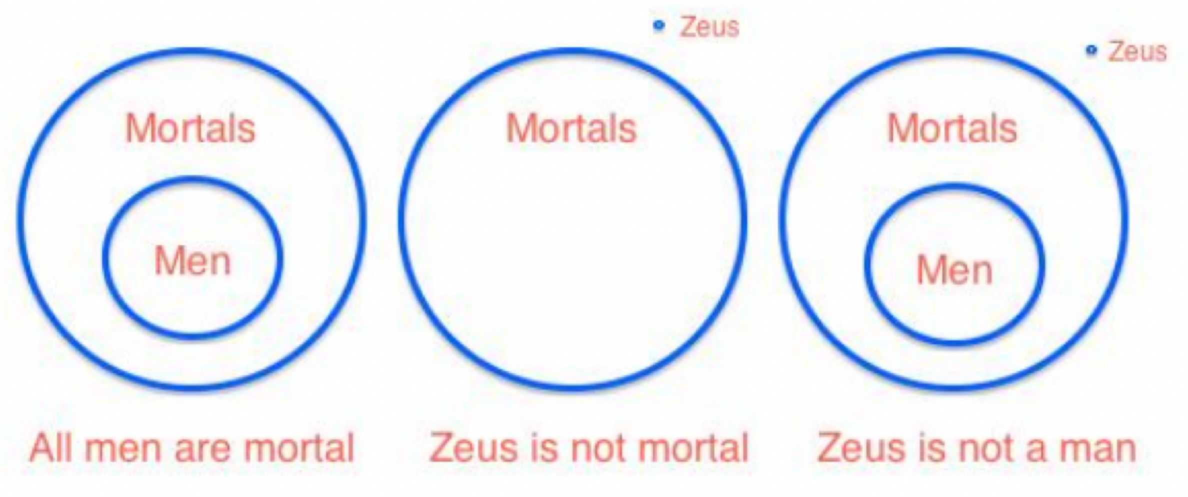
Thus n is divisible by 11 and the claim is proven. ∎

Introduction to Proofs

Contraposition Proof: We want to show that $p \rightarrow q$ is true. If that is difficult to show directly, we apply a direct proof to prove the logically equivalent contrapositive statement $\neg q \rightarrow \neg p$

Strategy:

- Assume $\neg q$ is true.
- Proceed through rules of inference, mathematical facts, axioms, etc. as necessary until we find that $\neg p$ is true.



If $p \rightarrow q$, then $\neg q \rightarrow \neg p$

Introduction to Proofs

contrapositive proof

Example: If $\underbrace{n = ab}_{p}$, where a and b are positive integers, then $\underbrace{a \leq \sqrt{n} \text{ or } b \leq \sqrt{n}}_{q}$.

$$p \to q \equiv \neg q \to \neg p$$

Assume "$\neg q$". $\neg(a \leq \sqrt{n}$ or $b \leq \sqrt{n})$

$a > \sqrt{n}$ and $b > \sqrt{n}$

Pf: $\left.\begin{array}{l}\text{Assume that for arbitrary positive integers } a, b \\ a > \sqrt{n} \text{ and } b > \sqrt{n}.\end{array}\right\}\neg q$

$ab > \sqrt{n} \cdot \sqrt{n} = n$

$ab > n$

$\Rightarrow n \neq ab \quad \}\neg p$

Since we've shown that the contrapositive "if $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n \neq ab$", we have proven the original claim. ∎

Introduction to Proofs

Contrapositive Proof

Example: If $\underbrace{x^2(y+3) \text{ is even}}_{p}$, then $\underbrace{x \text{ is even or } y \text{ is odd}}_{q}$.

$p \longrightarrow q$

Instead of a direct proof, we will prove the equivalent contrapositive claim: If x is odd and y is even, then $x^2(y+3)$ is odd.

Pf: We will prove this claim with contraposition.

Assume that x is odd and y is even.

Let $x = 2k+1$ and $y = 2m$ where k, m are some integers.

$$
\begin{aligned}
x^2(y+3) &= (2k+1)^2(2m+3) \\
&= (4k^2+4k+1)(2m+3) \\
&= 8k^2m + 8km + 2m + 12k^2 + 12k + 3 \\
&= 8k^2m + 8km + 2m + 12k^2 + 12k + 2 + 1 \\
&= 2(4k^2m + 4km + m + 6k^2 + 6k + 1) + 1
\end{aligned}
$$

let $l = 4k^2m + 4km + m + 6k^2 + 6k + 1$

be some integer.

Therefore $x^2(y+3) = 2l + 1$

Thus $x^2(y+3)$ is odd.

Therefore if $x^2(y+3)$ is even, then x is even or y is odd, as desired. $\blacksquare$

Introduction to Proofs

Proof by Contradiction: We want to show that $p \rightarrow q$ is true. Assume p is true and $\neg q$ is true, then derive a contradiction. Alternatively, when proving p is true, assume ¬p and derive a contradiction.

Strategy:

- Assume p and $\neg q$, derive a contradiction.
- Alternatively, when proving p is true, assume $\neg p$, then derive a contradiction.

Proof by Contradiction assumption $p \wedge \neg q$

conclude $\neg(p \wedge \neg q) \equiv \neg p \vee q$

$\equiv p \rightarrow q$

Proof by Contradiction

Example: Prove that if $3n + 2$ is odd, then n is odd.

p q $\neg q$

Pf: Assume that $3n+2$ is odd and n is not odd.

Since n is even, it can be represented as $n = 2k$ for some integer k.

$$3n+2 = 3(2k) + 2$$
$$= 6k + 2$$
$$= 2(3k+1)$$

This means $3n+2$ is even.

However, this contradicts our assumption.

Thus it is not the case that $3n+2$ is odd and n is even.

$\therefore$ If $3n+2$ is odd, then n is odd. $\blacksquare$

Introduction to Proofs

We wanted to prove $p \to q$

The argument form that we just used looked as follows

$$((p \land \neg q) \to \mathbf{F}) \to (p \to q)$$

p	q	$\neg q$	$p \land \neg q$	$(p \land \neg q) \to \mathbf{F}$	$p \to q$	$((p \land \neg q) \to \mathbf{F}) \to (p \to q)$
T	T	F	F	T	T	T
T	F	T	T	F	F	T
F	T	F	F	T	T	T
F	F	T	F	T	T	T

The argument is a **tautology** so it is valid

Introduction to Proofs

Example: Prove that $\sqrt{2}$ is irrational. P

Proof: Assume that $\sqrt{2}$ is rational for a contradiction. $\neg P$

$\sqrt{2} = \frac{a}{b}$ for some integers a, b which do not have any common factors and $b \neq 0$.

$2 = \dfrac{a^2}{b^2}$

$\implies 2b^2 = a^2$

$\implies a^2$ is even

If a^2 is even, then $\boxed{\text{a is even}}$

Subproof:

Assume a is odd

$a = 2k+1$

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

$= 4k^2 + 4k + 1$

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

Therefore, $\underbrace{a = 2c}$ for some integer c.

$2b^2 = a^2 = (2c)^2 = 4c^2$

$b^2 = 2c^2 \implies b^2$ is even $\implies \boxed{b \text{ is even}}$

So we have deduced that a and b are both even.
This means that a and b share a factor of 2.
Since this contradicts the original assumption, it must be that $\sqrt{2}$ is irrational.

Introduction to Proofs

- **Proving a biconditional**: $p \leftrightarrow q$ is logically equivalent to $(p \to q) \land (q \to p)$

Example: Integer n is even if and only if $3n + 5$ is odd.

For a biconditional proof, we need to prove the forward and backward directions.

Forward direction: If n is even, then $3n+5$ is odd. $(\Longrightarrow)$ Direct proof

Backward direction: If $3n+5$ is odd, then n is even. $(\Longleftarrow)$ contrapositive proof

contrapositive: If n is odd, then $3n+5$ is even.

Pf: $(\Longrightarrow)$ Assume n is even

Let $n = 2k$ for some integer k.

$$3n+5 = 3(2k) + 5$$
$$= 6k+5$$
$$= 6k+4+1$$

$3n+5 = 2(3k+2) + 1$

Thus $3n+5$ is odd.

($\Leftarrow$)

Next we prove the backward direction with contraposition.

Assume. n is odd.

Let $n = 2m+1$ for some integer m

$$3n+5 = 3(2m+1) + 5$$
$$= 6m+3 + 5$$
$$= 6m + 8$$
$$= 2(3m+4)$$

Thus $3n+5$ is even. $\blacksquare$

Extra Practice

direct assume: $p \rightsquigarrow q$

contrapositive: assume $\neg q \rightsquigarrow \neg p$

contradiction: assume $p \wedge \neg q$

Example 1: Let n be a three digit number where all three digits are the same digit from chosen from 1-9, then if you divide n by the sum of the three digits you get 37

Example 2: If $x + y$ is even, then x and y have the same parity

Example 3: There are no positive integer solutions to $x^2 - y^2 = 10$

Example 4: Integer n is even if and only if $3n + 6$ is even

Solutions

Example 1: Let n be a three digit number where all three digits are the same digit from chosen from 1-9, then if you divide n by the sum of the three digits you get 37

Proof: Suppose n's digits are $a.a.a$. We can write n as

$$n = a \cdot 100 + a \cdot 10 + a \cdot 1 = 111a$$

The sum of the digits is $3a$. Dividing, we have

$$\frac{n}{3a} = \frac{111a}{3a} = \frac{111}{3} = 37$$

Example 2: If $x + y$ is even, then x and y have the same parity

Proof: We'll prove the contrapositive statement If x and y have different parity then $x + y$ is odd

1. Without loss of generality, assume that x is the odd one and y is the even one, so take $x = 2a + 1$ and $y = 2b$

2. Then $x + y = 2a + 1 + 2b = 2(a + b) + 1 = 2m + 1$

3. Thus $x + y$ is odd and we've proved the contrapositive statement

Note: It seems like we should prove that both x odd, y even and x even, y odd both lead to the desired result, but since x and y both appear in the same way in $x + y$ it's not necessary to check both cases. When something like this happens we say "Without Loss of Generality" or WLOG and do just one case

Example 3: There are no positive integer solutions to $x^2 - y^2 = 10$

Proof: We'll use Proof by Contradiction here, so we'll assume the result is false and then show that it leads to a contradiction

1. Assume (FSOC) there **are** integers x and y s.t. $x^2 - y^2 = 10$

2. Factorizing the lefthand side: $(x + y)(x - y) = 10$

3. Since x and y are positive integers we must have $x + y = 10$ and $x - y = 1$ or $x + y = 5$ and $x - y = 2$.

4. Adding $x + y$ and $x - y$ gives $2x$, so the two cases give, respectively, $x = \frac{11}{2}$ and $x = \frac{7}{2}$

5. This contradicts our assumption that x is an integer, thus our original assumption is false and there are no positive integer

Example 4: Integer n is even if and only if $3n + 6$ is even

1. (⇒, by Direct Proof) Assume that $n = 2a$ is even

2. Then $3n + 6 = 3(2a) + 6 = 2(3a + 3)$

3. Thus $3n + 6$ is even and we've proved the $p \rightarrow q$ direction

1. (⇐, by Contrapositive) Assume that $n = 2a + 1$ is odd

2. Then $3n + 6 = 3(2a + 1) + 6 = 2(3a + 4) + 1$

3. Thus $3n + 6$ is odd and we've proved $\neg p \rightarrow \neg q$ which is equivalent to the $q \rightarrow p$ direction