CS 40
FOUNDATIONS OF CS

Summer 2024
Session A
Week 3

Tuesday's learning goals

- Determine what evidence is required to establish that a quantified statement is true or false.
- Use logical equivalence to rewrite quantified statements (including negated quantified statements)
- Use universal generalization to prove that universal statements are true
- Define predicates associated with integer factoring
- Define "arbitrary"
- Write proofs in prose form
- New proof strategy: direct proof.

July 9

Axioms, Theorems, Proofs (zybook 4.1 and 4.3.1)

Proof: ⟶ Establish the truth of statement with clarity

Chess:

1) Chess picks
2) Initial arrangement
3) Rules
4) New arrangement

≡ numbers, sets, fns, propositions...
≡ Axioms (statements we believe to be true)
≡ Rules of logic
≡ Theorems

Proof:

Application: factoring

Rosen p. 301

Goal exchange information (e.g. key for cipher) with a stranger (Amazon, Venmo) without other observers accessing it

Mathematical tool It is much easier to multiply two large numbers than to factor a large number.

RSA

- Amazon picks two primes > 200 digits each, publishes their product
- Anyone can encrypt their credit card using this product.
- There are no known methods to decrypt without factoring into the original primes.
- Current algorithms for factoring products of large primes take billions of years.

Application: factoring

Consider the predicate F(a,b) with domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$ ɘn by "a is a factor of b"

Definition 1 (Rosen p. 238) When a and b are integers and a is nonzero, **a divides b** means there is an integer c such that b = ac . $\exists c \quad b = ac$

Terminology: a is a factor of b, a is a divisor of b, b is a multiple of a, a | b

Symbolically, F(a,b) = $\exists c \in \mathbb{Z} \; b = ac$

$S = \{x \in \mathbb{Z} \mid x$ is even$\}$

Application: factoring

Which of the following statements is true?

A. $\exists a \in \mathbb{Z}^{\neq 0}(F(a,a))$

B. $\exists a \in \mathbb{Z}^{\neq 0}(\neg F(a,a))$

C. $\forall a \in \mathbb{Z}^{\neq 0}(F(a,a))$ → How? Prove?

D. $\forall a \in \mathbb{Z}^{\neq 0}(\neg F(a,a))$

E. None of the above.

Universal generalization

Rosen p. 76

To prove that the **universal quantification**

$$\forall x P(x)$$

is **true**, we can take an **arbitrary element e** from the domain and show that P(e) is true, without making any assumptions about e other than that it comes from the domain.

Claim: Every nonzero integer is a factor of itself.

Proof:

Need to prove

$\forall x \in \mathbb{Z}^+$ $F(x,x)$

to show that ← T.S.T

should have been $\neq 0$

① Write what to prove

What does $F(x,x) = ?$ $\quad \exists c \in \mathbb{Z} \quad x = c \cdot x$

Statements to prove the claim

$\forall x \in \mathbb{Z}^+ \quad x = 1 \cdot x \quad$ (Axiom that $x = 1 \cdot x$)

$\equiv c$

implies $\Rightarrow \forall x \in \mathbb{Z}^+ \; \exists c \in \mathbb{Z} \; x = c \cdot x$

$\Rightarrow \forall x \in \mathbb{Z}^+ \; F(x,x)$

$\therefore \forall x \in \mathbb{Z}^+ \; F(x,x)$

Therefore

conclusion

Infering Logical statements

Alternate Proof: (2)

T.S.T $\quad \forall x \in \mathbb{Z}^+ \quad F(x,x)$

universal generalization

Let e be an arbitary, $+ve$ integer, i.e $e \in \mathbb{Z}^+$

We know from Axioms that

$$e = 1 \cdot e$$

$$\Rightarrow \quad \exists c \quad e = c \cdot e$$

$$\Rightarrow \quad F(e, e)$$

Therefore, since $F(e,e)$ is true for any arbitary $+^{ve}$ integer e,

We have $\forall x \in \mathbb{Z}^{+} \quad F(x, x)$

Universal generalization

Rosen p. 76

Claim: Every nonzero integer is a factor of itself.

Proof analysis: According to the definition, we want to show that

$\forall a \in \mathbb{Z}^{\neq 0}(F(a,a))$ $F(a,a) = \exists c \in \mathbb{Z}(a = ca)$

The proof by generalization gives a systematic method for finding the witness that proves each of the existential quantifications is true.

a	To show:	Witness	$F(a,a)$
1	$\exists c(1 = c1)$	1	T
2	$\exists c(2 = c2)$	1	T
3	$\exists c(3 = c3)$	1	T
4	$\exists c(4 = c4)$	1	T
⋮	⋮	⋮	⋮

Another proof

X: There is a nonzero integer that does not divide its square.

Claim: X is true / false

$\exists x \in \mathbb{Z}^{\neq 0} \sim F(x, x^2)$ → $x \mid x^2$

To prove that $\sim(\exists x \in \mathbb{Z}^{\neq 0} \sim F(x, x^2))$

$\Rightarrow \forall x \in \mathbb{Z}^{\neq 0} \; F(x, x^2)$ (using DeMorgan's)

To prove that $\forall x \in \mathbb{Z}^{\neq 0} \; F(x, x^2)$

Let e be an arbitrary non zero integer

$$e^2 = e \cdot e \quad \text{(by defn)}$$

$$\Rightarrow \exists c \in \mathbb{Z} \; e^2 = c \cdot e$$

$$\Rightarrow F(e, e^2)$$

Since $F(e, e^2)$ is true for any arbitrary non zero integer e

We have $\forall x \in \mathbb{Z}^{\neq 0} \; F(x, x^2)$

Therefore, $\sim \exists x \in \mathbb{Z}^{\neq 0} \; \sim F(x, x^2)$

So the claim is false

Definitions: Even and Odd

(zybook 4.1)

An integer x is even if $x = 2 \cdot c$ $\exists c \in \mathbb{Z}$ $x = 2 \cdot c$

An integer x is odd if $\exists c \in \mathbb{Z}$ $x = 2c + 1$

$F(2, x)$

$\sim F(2, x)$

Proof of conditionals: Direct Proof (zybook 4.2-4.2)

Theorem: If n is even, then n^2 is even

$E(n)$: n is Even

To prove: $\forall n \in \mathbb{Z}$ $E(n) \longrightarrow E(n^2)$ where $E(n)$ means n is Even

Let n be an arbitrary integer, ie $n \in \mathbb{Z}$

for some c, $n = 2 \cdot c$ because $E(n) \Rightarrow \exists c \; n = 2 \cdot c$

$$n^2 = (2 \cdot c)^2$$

$$= 4 \cdot c^2$$

$$= 2 \cdot \underbrace{(2c^2)}_{c'}$$ since c is an integer

$c' = 2c^2$ is an integer

$$= 2 \cdot c'$$

$\therefore \exists c \quad n^2 = 2 \cdot c$

Therefore, n^2 is Even so $E(n^2)$

$\therefore E(n) \longrightarrow E(n^2)$

Thus, since the claim is true for each n,

$\forall n \; E(n) \longrightarrow E(n^2)$

Proof of conditionals: Direct Proof

(zybook Ex:4.4.1e)

Theorem: If x is even integer and y is an odd integer, then $x^2 + y^2$ is an odd integer

To prove: $\forall x \forall y\ E(x) \wedge \sim E(y) \longrightarrow \sim E(x^2+y^2)$

Let x & y be arbitrary integers s.t x is even & y is odd

rewrite Theorems in terms of logic!

(using fact that an int is either even or odd)

Since x is even, for some const c $x = 2 \cdot c$
y is odd, for some const c $y = 2 \cdot c' + 1$

$$\text{So, } x^2 + y^2 = (2 \cdot c)^2 + (2 \cdot c' + 1)^2$$
$$= 4c^2 + 4 \cdot c'^2 + 4c' + 1$$
$$= 2\underbrace{(2c^2 + 2c'^2 + 2c')}_{c''} + 1$$

$\therefore x^2 + y^2$ is odd

Since for an arbitrary even integer x & odd integer y,

$x^2 + y^2$ is odd

$\Rightarrow \forall x \forall y \; xE(x) \wedge E(y) \rightarrow E(x^2 + y^2)$

Could have also written claim as:

x is odd $\wedge$ y is odd $\rightarrow$ $x^2 + y^2$ is odd

Best practices in writing proofs. (zybook 4.3.4)

Theorem: The product of an even integer and an odd integer is even.

Identify how each proof of the theorem is in error or is missing text that could make the proof more readable.

1) **Proof.**

Since x is even, x = 2k for some integer k. Since y is odd, y = 2j+1 for some integer j.

Plugging in the expression 2k for x and 2j+1 for y into xy gives:

$$xy = 2k(2j+1) = 2 \cdot k(2j+1) = 2(2jk+k).$$

Since j and k are integers, 2jk+k is also an integer. The expression xy is equal to two times an integer and is therefore even. ■

Find the mistake in the proof

Theorem: The difference between two odd numbers is even.

Identify which line has a mistake in the proof of the theorem above.

1)

1. Let x and y be two odd integers. We shall show that x-y is even.
2. Since x is odd, then x = 2k+1 for some integer k. Since y is odd, then y = 2j+1 for some integer j.
3. Since x and y are both odd, x-y must be even. !!!
4. Therefore the difference between two odd integers is even.

- ○ Line 1
- ○ Line 2
- ✓ ○ Line 3
- ○ Line 4

circular reasoning (using what you have to prove to prove it !!)

Find the mistake in the proof

Theorem: The difference between two odd numbers is even.

Identify which line has a mistake in the proof of the theorem above.

3)

1. Let x and y be two odd integers. We shall show that x-y is even.
2. Since x is odd, then x = 2k+1 for some integer k. Since y is odd, then y = 2k+1 for some integer k.
3. Plug in the expressions 2k+1 and 2k+1 for x and y into x-y to get x-y = (2k+1)-(2k+1) = 2k-2k = 2(k-k)
4. Since k is an integer, k-k is also an integer. Therefore x-y is two times an integer and x-y is even.

- ○ Line 1
- ✓ Line 2
- ○ Line 3
- ○ Line 4

→ uses the same integer k for x & y (this actually means x & y are the same!!!)

Find the mistake in the proof

Theorem: The difference between two odd numbers is even.

Identify which line has a mistake in the proof of the theorem above.

4)

1. Let x and y be two odd integers. We shall show that x-y is even.
2. Since x is odd, then x = 2k+1 for some integer k. Since y is odd, then y = 2j+1 for some integer j.
3. Then x-y = (2k+1) - (2j+1). = 2(k-j)
4. Since x-y is two times an integer, then x-y is even.

- ○ Line 1
- ○ Line 2
- ✓ Line 3
- ○ Line 4

incomplete but mostly right

Summary

To prove that the **universal quantification**

$$\forall x P(x)$$

is **true** when the predicate P has a finite domain, evaluate P(x) at each domain element to confirm it is T.

To prove that the **existential quantification**

$$\exists x P(x)$$

is **true**, we find a witness: an element in the domain for which P(x) is true.

To prove that the **universal quantification**

$$\forall x P(x)$$

is **false**, we find a counterexample: an element in the domain for which P(x) is false.

To prove that the **existential quantification**

$$\exists x P(x)$$

is **false** when the predicate P has a finite domain, evaluate P(x) at each domain element to confirm it is F.

Today's goal: devise more proof strategies for related statements.

~~Thursday's~~ learning goals contd...

Tuesday's

- Trace and/or construct a proof by contrapositive
- Work to prove/disprove in parallel
- Evaluate which proof technique(s) is appropriate for a given proposition

contrapositive of $A \to B$ is $\neg B \to \neg A$ & w.k.t $A \to B \equiv \neg B \to \neg A$

Proof by contrapositive: ex 1

Prove: If n^2 is odd, then n is odd

$\forall n \in \mathbb{Z}$ n^2 is odd $\to$ n is odd $\equiv$ $\forall n \in \mathbb{Z}$ $\neg n$ is odd $\to \neg n^2$ is odd

We prove the contrapositive of $\forall n \in \mathbb{Z}\ n^2$ is odd — contrapositive

$\to n$ is odel

which is $\forall n \in \mathbb{Z}$ $\neg n$ is odd $\to \neg n^2$ is odel

the statement is the same as,

$\forall n \in \mathbb{Z}$ n is even $\to n^2$ is even

the same proof as before (refer to previous slide)

Why is contrapositive actually useful here?

Suppose you are proving directly

$\forall n \in \mathbb{Z}$ n^2 is odd $\longrightarrow$ n is odd

Assume arbitrary $n \in \mathbb{Z}$ s.t n^2 is odd

$$n^2 = 2c + 1$$

$$\Rightarrow n = \sqrt{2c+1}$$ $\longrightarrow$ What to do after?

STUCK

Proof by contrapositive: ex 2

To prove that

Prove: For real numbers x and y, if (x+y)>=2, then x>=1 or y>=1

T.P.T $\forall x,y \in \mathbb{R} \quad (x+y) \geq 2 \longrightarrow x \geq 1 \vee y \geq 1$

Proof by contrapositive

T.P.T $\forall x,y \in \mathbb{R} \quad \sim(x \geq 1 \vee y \geq 1) \longrightarrow \sim(x+y) \geq 2$

$\Rightarrow \forall x,y \in \mathbb{R} \quad x < 1 \wedge y < 1 \longrightarrow (x+y) < 2$

Let x, y be arbitrary real numbers s.t $x < 1$ and such that $y < 1$

Then $x + y < 1 + 1$

< 2

Therefore, since the claim is true for arbitrary $x, y < 1$

$\Rightarrow \forall x, y \in \mathbb{R} \quad x < 1 \wedge y < 1 \longrightarrow (x + y) < 2$

By Proof of contrapositive

$\therefore \forall x, y \in \mathbb{R} \ (x + y) \geq 2 \longrightarrow x \geq 1 \text{ or } y \geq 1$

Proof by contrapositive: ex 3

Prove: For any integers, if $x|y$ and $x \nmid z$, then $x \nmid (y+z)$

T.P.T: $\forall x,y,z \in \mathbb{Z}$ $\quad x|y \wedge x \nmid z \longrightarrow x \nmid y+z$

aside: what does $x \nmid z$ mean?

x is not a factor of z

Division alg: $\forall\, x \nmid z \longrightarrow \exists c,r$ $x = c \cdot z + r$, $0 < r < z$, $c \in \mathbb{Z}^+$,

$2, 11 \quad 11 = 5 \cdot 2 + 1 \qquad 3, 11 \quad 11 = 3 \cdot 3 + 2$

We will prove the claim by using contrapositive,

P: $x \mid y+z \longrightarrow \sim(x \mid y \wedge x \nmid z)$

T.P.T : $x \mid y+z \longrightarrow x \nmid y \vee x \mid z$

To prove that

→ Two cases based on assuming one of A or B is F. T

A or B

Case (i): $x \mid y+z \wedge x \mid y \longrightarrow x \mid z$ ✓

$\sim x \nmid y$ (A is false)

Case (ii): $x \mid y+z \wedge x \nmid z \longrightarrow x \mid y$

B is false

P

Saw in class that just this sufficient by simplifying

T.P.T: $x \mid y+z \wedge x \mid y \longrightarrow x \mid z$

Simplifying P.

$P: Q \longrightarrow A \vee B$

$\equiv \sim Q \vee (A \vee B)$

$\equiv (\sim Q \vee A) \vee B$

$\equiv \sim(Q \wedge \sim A) \vee B$

$\equiv Q \wedge \sim A \longrightarrow B$ (Case (i))

T.P.T: $x \mid y+z \wedge x \mid y \longrightarrow x \mid z$

$x \mid y+z$

$\exists c$ s.t $\quad y+z = c \cdot x \quad -(1)$

$x \mid y$

$\exists c'$ s.t $\quad y = c' x \quad -(2)$

To show $x \mid z$

$$z = (y+z) - y$$

$$(1) - (2)$$

$$= c \cdot x - c' \cdot x$$

$$= (c - c') \cdot x$$

integer assuming c, c' are integers

Thus z is divisible by x

$\Rightarrow x \mid z$

$\therefore$ We have proved

$R: x \mid y+z \wedge x \mid y \longrightarrow x \mid z$

Thus, since we reduced P to R, we have proved P proving

$\forall x, y, z \in \mathbb{Z} \quad x \mid y \wedge x \nmid z \longrightarrow x \nmid y+z$

Prove or disprove

Understand the statement
- **Logical structure**
- **Relevant definitions**

Do you believe the statement?
- Try some small examples that illustrate relevant claims

Map out possible proof strategies
- For each strategy: what can we assume? What evidence do we need?
- Start with simplest strategies, move to more complicated if/when we get stuck

Work to prove / disprove statement (sometimes in parallel…)

Prove or disprove

If x and y are two distinct positive integers, such that xy is a perfect square, then x and y are perfect squares.

Prove or disprove

Claim: $\{4, 6\} \subseteq \{n \bmod 10 \mid \exists c \in \mathbb{Z}(n = 4c)\}$

$M =$

$\{4,6\} \subseteq \{0,2,4,6,8\}$

$8 = 12 \bmod 10$

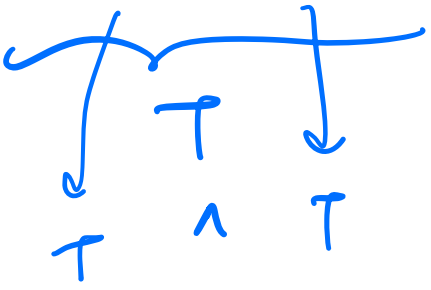
$6 = 6 \bmod 10$

Claim: $\forall x \in \mathbb{Z}\ \{x \in \{4,6\} \rightarrow x \in M\}$

Proof: Let e be an arbitrary element/integer in $\{4,6\}$

We know that $e=4$ or $e=6$,

$\forall e \in \mathbb{Z}$ $\quad e = 4 \wedge e = 6 \longrightarrow e \in M$



Case (i): $e = 4 \longrightarrow e \in M$

Case (ii): $e = 6 \longrightarrow e \in M$

Direct, for $n = 4 \cdot 1$

$n \bmod 10 = 4$ ← e

$\therefore e = 4 \in M$

Case (ii) $e = 6$

$6 = n \bmod 10$

choose n

Let $n = 16 = 4 \cdot 4$

$6 = n \bmod 10$

Now, since $n = 4 \cdot 4$

$\& \; 6 = n \bmod 10$

$\Rightarrow 6 \in M$

This proves case (ii)

Since case (i) & case (ii) are T

$\{4, 6\} \subseteq M$

Proof by cases

To prove that q holds when we know

$$p_1 \vee p_2$$

is true, we can show two conditional statements:

Goal 1: $(p_1 \rightarrow q)$

Goal 2: $(p_2 \rightarrow q)$

Then conclude q

Select a proof strategy

Prove or disprove: For every integer n, if n^2 is not divisible by 4, then n is odd.

A. Direct proof
B. Proof by contrapositive
C. Proof by universal exhaustion
D. Prove using a witness
E. Counterexample

Select a proof strategy

Prove or disprove: For every integer n, if n is even, then n^2 is divisible by 4.

A. Direct proof
B. Proof by contrapositive
C. Proof by universal exhaustion
D. Prove using a witness
E. Counterexample