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.

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 .

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) =

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

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:

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

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

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

Definitions: Even and Odd

(zybook 4.1)

An integer x is even if _____

An integer x is odd if _____

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

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

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

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

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

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).
4. Since x-y is two times an integer, then x-y is even.

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

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

- 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

Proof by contrapositive: ex 1

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

Proof by contrapositive: ex 2

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

Proof by contrapositive: ex 3

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

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

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