CSE 20
DISCRETE MATH

Fall 2020

http://cseweb.ucsd.edu/classes/fa20/cse20-a/

Today'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 and primes
- Define “arbitrary”

Recap

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.

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

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

Prime numbers

Definition (Rosen p. 257) An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

Which of the following gives a formal definition of the predicate Pr(x) over the set of integers which evaluates to T exactly when x is prime.

A. $\forall a \ (\ (x > 1 \wedge a > 0) \rightarrow F(a, x) \ )$

B. $\exists a \ (x > 1 \wedge (a = 1 \vee a = x) \wedge F(a, x) \ )$

C. $(x > 1) \wedge \forall a(\ (\ a > 0 \wedge F(a, x) \ ) \rightarrow (a = 1 \vee a = x) \ )$

D. $(x > 1) \wedge \forall a(\ (\ a > 1 \wedge \neg(a = x) \ ) \rightarrow \neg F(a, x) \ )$

E. None of the above

Prime numbers

Claim: 1 is not prime.

Proof:

Prime numbers

Claim: 4 is not prime.

Proof: