

CSE 20—Discrete Math

Winter, 2006

January 24 (Day 5)
Number Theory

Instructor: Neil Rhodes

Proving Quantified Statements

Prove universal statement: $\forall x \in D, P(x) \rightarrow Q(x)$

- Exhaustive enumeration
- Generalizing from the generic particular
 - "Suppose x is in D and $P(x)$ "
 - ...
 - Therefore $Q(x)$
- Example: The difference of two odd numbers is even

2

Proving Quantified Statements

Prove existential statement: $\exists x \in D: P(x)$

- Constructive proof
 - Display an x
 - Give a set of directions for finding x
- Nonconstructive proof
 - Proof by contradiction (assume non-existence and show a contradiction)
 - Show x must exist
- Example:
 - In a group of 367 people, at least two share a birthday

3

Disproving Quantified Statements

Disprove universal statement: $\forall x \in D, P(x)$

- Counterexample
 - Show an x in D where $P(x)$, but not $Q(x)$
- Example: All numbers of the form $2^n - 1$ ($n > 1$) are prime

Disprove existential statement: $\exists x \in D: P(x)$

- Equivalent to:
 - Prove
 - Or, alternatively,
 - Therefore, best bet is generalizing from the generic particular.
- Example: There exists a prime which can be written as the square of an integer > 1

4

Number Theory

The study of the properties of integers

- Mathematics is the queen of the sciences and number theory is the queen of mathematics. —Gauss

Relationship to Computer Science

- Logical thinking
- Proof for important fundamental CS theorem very related to number-theory proof
- Cryptography

5

Important Sets

$\mathbb{Z}$ (*Zahl* = Number)

$\mathbb{Z}^+$

$\mathbb{N}$ (*Natural*)

- No general agreement on whether it includes 0

$\mathbb{Q}$ (*Quotient*)

$\mathbb{R}$ (*Real*)

$\mathbb{P}$ (*Prime*)

6

Prime Numbers

A prime, p , is a positive integer (greater than 1) whose only positive divisors are 1 and p

- Quantified statement:

A number greater than one that is not prime is called *composite*

- Quantified statement:

The set of primes is infinite

- $\forall x \in \mathbb{Z}^+, \exists y \in \mathbb{Z}^+: y > x \wedge P(y)$

7

Prime Numbers

Unique Prime Factorization (the fundamental theorem of arithmetic)

- Any integer ≥ 2 can be written as the multiple of a unique set of prime numbers.

m and n are *relatively prime* if they share no common factors

- We write $m \perp n$

Proving $\sqrt{2}$ is irrational

- Assume it can be written as m/n where $n \geq 2$ and $m \perp n$
- $2m^2 = n^2$
- n^2 is even
- n is even
- $2m^2 = (2k)^2$
- $m^2 = 2k^2$
- m^2 is even
- But since $m \perp n$, m^2 and n^2 can't share a common factor

8

Countably Infinite

A set is *countable* if:

- the number of elements is finite
- or, it has the same number of elements as $\mathbf{N}$, (countably infinite)

Equivalent cardinality

- Given two sets A and B
- If there exists a function $f: A \rightarrow B$, such that f is *bijective*:
 - $\forall a \in A, \forall a' \in A, f(a) = f(a') \rightarrow a = a'$ (injective, or one-to-one)
 - $\forall b \in B, \exists a \in A: f(a) = b$ (surjective, or onto)
- $|A| = |B|$

Examples

- $|\text{odd integers}| = |\mathbf{Z}|$
 - $f(x) = (x-1)/2$
- $|\mathbf{Z}^+| = |\mathbf{N}|$
 - $f(x) = x-1$
- $|\mathbf{P}| = |\mathbf{N}|$

9

Hilbert's Grand Hotel

The Grand Hotel has an infinite number of rooms and is all full

- One person wants to checkin
- A bus containing a countably infinite number of people want to checkin
- A countably infinite number of such buses arrive

10

Rationals are Countable

11

Reals are not Countable

Let's look at a subset of the reals: $\mathbf{R}^* = [0, 1)$

Assume the existence of an bijective function, $f: \mathbf{R}^* \rightarrow \mathbf{N}$

Diagonalization Argument

12

Infinite Hierarchy of Infinities

$|N| = \aleph_0$

Given a set S , the powerset of S , $P(S)$, is of higher cardinality

- Diagonalization argument

We say $\aleph_i$ is the next largest set size after $\aleph_{i-1}$

Continuum hypothesis:

- There is no set whose size is between that of the integers and that of the reals

13

Halting Problem

Assume there exists routine:

- `Boolean Halt(String program, String input)` (returns true if program executed on input halts, false otherwise)

- We can write:

```
Boolean trouble(String program) {  
    if not Halt(program, program)  
        return false;  
    else  
        while (true) ;  
}
```

- `Boolean trouble2(String program) {
 return not Halt(program, program);
}`

- Diagonalization (with trouble2):

14

Rationals and Irrationals

Rationals are closed under addition, subtraction, multiplication, and division

Irrationals are *not* closed under multiplication

- Irrational * irrational may equal rational
- What about irrational * (non-zero) rational?

15

Mersenne Primes

Primes of the form $2^n - 1$

- For example, 3, 7, 31, 63
- Any such prime must actually be of the form $2^p - 1$
 - Because $2^{km} - 1 = 2^m - 1(2^{m(k-1)} + 2^{m(k-2)} + \dots + 1)$
- 43rd known Mersenne prime: $2^{30,402,457} - 1$
 - Contains >9,000,000 digits

16

Sieve of Erataosthenes

Make a list of natural numbers

Circle the first number, 2, and mark all its multiples

Repeat

- Circle the first uncircled unmarked number
- Mark all its multiples

Circled numbers are prime

Distribution of Prime Numbers

There are approximately $x/\ln x$ primes $\leq x$

- (The size of the n th prime is approximately $n/\ln n$)