CSE 240
Logic and Discrete Math
Lecture notes
Number Theory and
Proof Techniques

Weixiong Zhang
Washington University in St. Louis
http://www.cse.wustl.edu/~zhang/teaching/cse240/Spring10/index.html
Coverage

- Chapter 3.1
- Chapter 3.2
- Chapter 3.3
- Types of proofs
Test Driving

- Acquired the first-order predicate calculus mechanism over the last N lectures
- Time to try them out
- Chapter 3 is an interesting test
Sneak-preview: Sets

What is a set?
A collection of elements:
  - Order is irrelevant
  - No repetitions
  - Can be infinite
  - Can be empty

Examples:
  - \{Angela, Belinda, Jean\}
  - \{0,1,2,3,\ldots\}
Operations on sets

- **S** is a set

**Membership:**
  - \( x \in S \)
  - \( x \) is an element of \( S \)
  - \( \text{Angela} \in \{\text{Angela, Belinda, Jean}\} \)

**Subset:**
  - \( S_1 \subseteq S \)
  - Set \( S_1 \) is a subset of set \( S \)
  - All elements of \( S_1 \) are elements of \( S \)
  - \( \{\text{Angela, Belinda}\} \subseteq \{\text{Angela, Belinda, Jean}\} \)
Operations on sets

- $S, S_1$ are sets
- Equality:
  - $S = S_1$
  - iff they have the same elements
- Difference:
  - $S \setminus S_1$
  - is a set of all elements that belong to $S$ but NOT to $S_1$
  - $\{\text{Angela, Belinda, Jean}\} \setminus \{\text{Angela, Dana}\} = \{\text{Belinda, Jean}\}$
Operations on sets

- **S, S₁ are sets**

- **Intersection:**
  - \( S \cap S₁ \)
  - is a set of all elements that belong to both
  - \( \{\text{Angela, Belinda, Jean}\} \cap \{\text{Angela, Dana}\} = \{\text{Angela}\} \)

- **Union:**
  - \( S \cup S₁ \)
  - is a set of all elements that belong to either
  - \( \{\text{Angela, Belinda, Jean}\} \cup \{\text{Angela, Dana}\} = \{\text{Angela, Belinda, Jean, Dana}\} \)
We will work with numbers for the next little while

\( \mathbb{R} \) is the set of all real numbers
- 0, 1, -5.27, \( \pi \), ...

\( \mathbb{Q} \) is the set of rational numbers
- 0, 1, -5.27, ...

\( \mathbb{Z} \) is the set of integer numbers
- 0, 1, -1, 2, ...

\( \mathbb{N} \) is the set of natural numbers
- 0, 1, 2, ...

Numbers
Notes

The following inclusions hold
- \( \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \)

Note that the inclusions are actually proper:
- \( \mathbb{N} \neq \mathbb{Z} \neq \mathbb{Q} \neq \mathbb{R} \)

Algebraic operations (+, -, *, /, etc.) are defined on all of these sets

Order relations are also defined:
- Any two numbers are comparable (\(<, >, =\))
Numbers in Predicate Logic

Our interpretations will set the domain set to \( \mathbb{R} \) (or sometimes \( \mathbb{N}, \mathbb{Z}, \mathbb{Q} \)).

We will use functional symbols:

- \( +, *, -, /, \) etc.
- \( \forall n \in \mathbb{N} \ [n+1 \in \mathbb{N}] \)
- Domain set is \( \mathbb{R} \)
- For every natural number \( n \), \( n+1 \) is a natural number as well

We will also use operator notation for predicates \(<, >, =, \) :

- \( \forall n \in \mathbb{N} \ [n < n+1] \)
- Domain set is \( \mathbb{R} \)
- For every natural number \( n \), \( n < n+1 \)
Premises

One can define a system of predicate logic statements that describe all foundational properties of numbers

- Axioms

Axiomatic introduction of real numbers, integers, etc.

We won’t do it at this moment

- Non-trivial

Nevertheless we will use these “imaginary” premises to prove other statements
Proving Statements

From now we will be proving statements
- Theorems
- Propositions
- Corollaries
- Lemmas

They are statements in predicate logic

We will be showing that they are logically implied by the system of premises (axioms)
Odd / Even

Define predicate even(n):
- \( n \) is an even integer iff
- Exists an integer \( k \) such that \( n=2k \)
- \( \forall n \in \mathbb{Z} \ [\text{even}(n) \iff \exists k \in \mathbb{Z} \ [n=2k]] \)

Define predicate odd(n):
- \( n \) is an even integer iff
- Exists an integer \( k \) such that \( n=2k+1 \)
- \( \forall n \in \mathbb{Z} \ [\text{odd}(n) \iff \exists k \in \mathbb{Z} \ [n=2k+1]] \)
Odd / even ?

-95*2

(a+b)² if a, b are even

n*(n+1) if n is even

56⁰

n+1 if n is odd

n*(n-1) + 3

sqrt(7⁴)

3.14
Prime / Composite

Define predicate \( \text{prime}(n) \):
- \( n \) is a prime number iff
- \( n>1 \) and
- for any its positive integer factors \( r \) and \( s \) one of them is \( 1 \)
- \( \forall n \in \mathbb{Z} \ [\text{prime}(n) \Leftrightarrow n>1 \land \forall r,s \in \mathbb{N} \ [n=rs \rightarrow r=1 \lor s=1]] \)

Define predicate \( \text{composite}(n) \):
- \( n \) is a composite integer iff
- \( n \) is not prime and is greater than \( 1 \)
- \( \forall n \in \mathbb{Z} \ [\text{composite}(n) \Leftrightarrow n>1 \land \neg \text{prime}(n)] \)
Prime / composite?

- 34
- 1
- -50
- 3.14
- $7^{25}$
- $(2a+8k)^3$
- $p-1$ where $p$ is a prime
- $p+1$ where $p$ is a prime
- 1881988129206079638386972394616504398071635633794173827007633564229888597152346654853190606065047430453173880113033967161996923212057340318795506569962213051687593076502570590
Who wants to pocket **US$15K** today?

- Excellent!
- Then just find non-trivial natural factors of:

  31074182404900437213507500358885679300
  37346022842727545720161948823206440518
  08150455634682967172328678243791627283
  80334154710731085019195485290073377248
  22783525742386454014691736602477652346
  609
Suppose someone gives you a number $n$ and asks to find factors of it.

Integers $r$ and $s$ such that $rs=n$.

How would you do it?
- Can try all integers from 1 to $n$.
- Can try all integers from 1 to $\sqrt{n}$.
- Can try all primes from 1 to $\sqrt{n}$.

Running time: exponential in the number of digits of $n$. 

On August 22, 1999, a group of researchers completed the factorization of the 155 digit RSA Challenge Number.

Sieving: 35.7 CPU-years in total on...
- 160 175-400 MHz SGI and Sun workstations
- 8 250 MHz SGI Origin 2000 processors
- 120 300-450 MHz Pentium II PCs
- 4 500 MHz Digital/Compaq boxes

This CPU-effort is estimated to be equivalent to approximately 8,000 MIPS years

Calendar time for the sieving was 3.7 months.
Applications

- Long prime numbers are very difficult to factor (i.e., find $r$ and $s$ such that $rs=n$)

- However, once you know one factor it is easy to find the other (just divide)

- Security codes, encryption, etc. are based on some of these properties:
  - Banks
  - Web (credit cards, passwords, etc.)
  - Military
  - Etc.
Quantum Computing

In the early 90s Peter Shor of ATT Labs devised a factoring algorithm:
- Factors numbers in polynomial time
- Much faster than conventional algorithms

So how come he hasn’t collected the $15K himself?

The algorithm is fast on quantum computers only

Where can I buy a quantum computer?

State-of-the-art: IBM quantumly factored 15 into 5 and 3 in Dec 2001
We will work with numbers for the next little while.

\textbf{R} is the set of all real numbers
- \(0, 1, -5.27, \pi, \ldots\)

\textbf{Q} is the set of rational numbers
- \(0, 1, -5.27, \ldots\)

\textbf{Z} is the set of integer numbers
- \(0, 1, -1, 2, \ldots\)

\textbf{N} is the set of natural numbers
- \(0, 1, 2, \ldots\)
Odd / Even

Define predicate even(n):
- n is an even integer iff
- Exists an integer k such that n=2k
- \( \forall n \in \mathbb{Z} \ [\text{even}(n) \iff \exists k \in \mathbb{Z} \ [n=2k]] \)

Define predicate odd(n):
- n is an even integer iff
- Exists an integer k such that n=2k+1
- \( \forall n \in \mathbb{Z} \ [\text{odd}(n) \iff \exists k \in \mathbb{Z} \ [n=2k+1]] \)
A theorem

“Every integer is even or odd. But not both”

∀n∈Z [(odd(n) v even(n)) & ¬(odd(n) & even(n))]

Need some premises:

- Integer numbers are closed under +, -, *
- Trichotomy law: any number >0, =0, <0
- Well ordering principle: Every non-empty set of naturals contains its smallest element

Proof – recall how we introduced integers
Lemma 1

Let’s prove an auxiliary statement first:

For any $r, x \in \mathbb{R}$ if $r > 0, x < 1$ then $rx < r$

\[ \forall r, x \in \mathbb{R} \ [r > 0, x < 1 \rightarrow rx < r] \]

Proof:

- $x < 1$
- $r > 0 \rightarrow rx < r$
Lemma 2

Let’s prove another auxiliary statement:

There are no integers between 0 and 1

\(~ ( \exists n \in \mathbb{N} \ [0 < n < 1] )\)

Proof:

Suppose not

Then \( \exists n \in \mathbb{N} \ [0 < n < 1] \)

Consider set \( S = \{ n, n^2, n^3, \ldots \} \)

Every \( s \in S \) is integer and non-negative (i.e., natural)

Therefore \( \min(S) = s_m \in S \)

Consider \( s_m \cdot n \) then: \( s_m \cdot n \in S \) and \( s_m \cdot n < s_m \) (by Lemma 1)

Thus, \( s_m \neq \min(S) \ \Rightarrow \ \text{Contradiction} \)
Theorem (part 1)

“Every integer is even or odd”

\[ \forall n \in \mathbb{Z} \ [ \text{odd}(n) \lor \text{even}(n) ] \]

Proof:

- Suppose not
- Then \( \exists n \in \mathbb{Z} \ [ \neg(\text{odd}(n) \lor \text{even}(n)) ] \)
- Then let’s find the minimum \( m = 2k \) such that \( n < m \)
- Clearly, \( 2k-1 < n < 2k \)
- Subtract \( 2k-1 \) from all: \( 0 < n-2k+1 < 1 \)
- Then \( n-2k+1 \) is an integer and between \( 0, 1 \)
  - Contradiction with Lemma 2
Theorem (part 2)

“No integer is even and odd”

\[ \neg \exists n \in \mathbb{Z} \left[ \text{odd}(n) \land \text{even}(n) \right] \]

Proof:

Suppose not

Then \( \exists n \in \mathbb{Z} \left[ \text{odd}(n) \land \text{even}(n) \right] \)

By the definitions: \( n = 2k \) and \( n = 2m + 1 \)

Thus, \( 2k = 2m + 1 \)

Subtract \( 2m \) from both sides: \( 2(k - m) = 1 \)

Thus, \( k - m = \frac{1}{2} \) \( \rightarrow \) not an integer
Types of Proofs

Many interesting statements are of the type:

\[ \forall n \ S(n) \]

Two primary proof methods:

- Direct
  - Take an arbitrary \( n \), prove \( S(n) \), generalize
  - If \( S(n) \equiv P(n) \rightarrow Q(n) \)
    - Then can prove \( \sim Q(n) \rightarrow \sim P(n) \) instead

- Indirect
  - Show that \( \exists n \sim S(n) \) would lead to a contradiction
Contraposition & Contradiction

Suppose the statement to prove is:

\[ \forall n \ [ P(n) \rightarrow Q(n) ] \]

Direct proof by contraposition:

- Take an arbitrary \( n \)
- Show that if \( \sim Q(n) \) holds for that \( n \) then \( \sim P(n) \) holds

Indirect proof (by contradiction):

- Assume \( P(n) \) and \( \sim Q(n) \) hold for some \( n \)
- Show \( \sim P(n) \)
  - Contradiction: cannot have \( P(n) \) and \( \sim P(n) \)
Illustration

If \( n^2 \) is even then \( n \) is even

\[ \forall n \ [ \ P(n) \rightarrow Q(n) \ ] \]

Direct proof by contraposition:

Assume \( \sim Q(n) \) : \( n \) is not even

\( n \) is odd

Then \( n = 2k+1 \)

\( n^2 = 4k^2 + 4k + 1 \)

\( n^2 \) is odd : \( n^2 \) is not even : \( \sim P(n) \)
Illustration

If \( n^2 \) is even then \( n \) is even

\[ \forall n \ [ \ P(n) \rightarrow Q(n) \ ] \]

Indirect proof (by contradiction):

Assume \( P(n) \) and \( \sim Q(n) \)

\( n^2 \) is even

\( n \) is not even : \( n \) is odd

Then \( n = 2k+1 \)

\( n^2 = 4k^2 + 4k + 1 \)

\( n^2 \) is odd : \( n^2 \) is even : contradiction
The third proof

Theorem: \( n^2 \) is even \( \rightarrow \) \( n \) is even

How about a direct proof without contraposition?

Proof

- Assume \( n^2 \) is even
- \( 2 \mid n^2 \)
- \( p \mid ab \rightarrow p \mid a \lor p \mid b \) (Euclid’s 1st theorem)
- \( 2 \mid n \lor 2 \mid n \)
- Then \( n \) is even
Define predicate $\text{prime}(n)$:

- $n$ is a prime number iff
- $n > 1$ and
- for any its positive integer factors $r$ and $s$ one of them is 1

$$\forall n \in \mathbb{Z} [\text{prime}(n) \iff n > 1 \land \forall r, s \in \mathbb{N} [n = rs \rightarrow r = 1 \lor s = 1]]$$

Define predicate $\text{composite}(n)$:

- $n$ is a composite integer iff
- $n$ is not prime and is greater than 1

$$\forall n \in \mathbb{Z} [\text{composite}(n) \iff n > 1 \land \neg \text{prime}(n)]$$
Existential Statements

\( \exists x \; P(x) \)

Proofs:

- **Constructive**
  - Construct an example of such \( x \)

- **Non-constructive**
  - By contradiction
    - Show that if such \( x \) does NOT exist than a contradiction can be derived
Example

Prove that

\[ \exists n \in \mathbb{N} \ \exists a, b \text{ prime}(a) \ & \text{prime}(b) \ & (a+b=n) \]

Proof:

- \[ n=210 \]
- \[ a=113 \]
- \[ b=97 \]

// Piece of cake…
Universal Statements

\[ \forall x \ P(x) \]
\[ \forall x \ [Q(x) \rightarrow R(x)] \]

Proof techniques:

- Exhaustion
- By contradiction
  - Assume the statement is not true
  - Arrive at a contradiction
- Direct
  - Generalizing from an arbitrary particular member
- Mathematical induction (chapter 4)
Example 1

Exhaustion:

Any even number between 4 and 30 can be written as a sum of two primes:

- 4 = 2 + 2
- 6 = 3 + 3
- 8 = 3 + 5
- ...
- 30 = 11 + 19
Problems?

- Works for finite domains only

- What if I want to prove that for any integer $n$ the product of $n$ and $n+1$ is even?

- Can I exhaust all integer values of $n$?
Example 2

Theorem: \( \forall n \in \mathbb{Z} \ [ \text{even}(n*(n+1)) \] \)

Proof:

- Consider a particular but arbitrarily chosen integer \( n \)

- \( n \) is odd or even

- Case 1: \( n \) is odd
  - Then \( n=2k+1, \ n+1=2k+2 \)
  - \( n(n+1) = (2k+1)(2k+2) = 2(2k+1)(k+1) = 2p \) for some integer \( p \)
  - So \( n(n+1) \) is even
Example 2 (cont’d)

Case 2: \( n \) is even

Then \( n = 2k, \ n + 1 = 2k + 1 \)

\[ n(n+1) = 2k(2k+1) = 2p \]

for some integer \( p \)

So \( n(n+1) \) is even

Done!
Example 3

Theorem: the square of any odd integer has the form $8m+1$ for some integer $m$

Proof?
Which strategy?

Corollary: the square of any odd integer is odd
Fallacy

- Generalizing from a particular but **NOT arbitrarily chosen** example
- I.e., using some **additional** properties of \( n \)
- Example:
  - “all odd numbers are prime”
  - “Proof”:
    - Consider odd number 3
    - It is prime
    - Thus for any odd \( n \) \( prime(n) \) holds
- Such “proofs” can be given for correct statements as well!
Prevention

- Try to stay away from specific instances (e.g., 3)

- Make sure that you are not using any additional properties of $n$ considered

- Challenge your proof
  - Try to play the devil’s advocate and find holes in it…
Other Common Mistakes

- Pages 135-136 in the book

- Using the same letter to mean different things

- Jumping to a conclusion
  - Insufficient justification

- Begging the question
  - assuming the claim first

- Misuse of the word if
Rational Numbers

A real number is rational iff it can be represented as a ratio/quotient/fraction of integers $a$ and $b$ ($b \neq 0$)

- $\forall r \in \mathbb{R} \ [r \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z} \ [r = a/b \ & \ b \neq 0]]$

Notes:
- $a$ is numerator
- $b$ is denominator
- Any rational number can be represented in infinitely many ways
- The fractional part of any rational number written in any natural radix has a period in it
Rational or not?

-12
  -12/1

3.1459
  3+1459/10000

0.5555555555555555...
  ?

0.56895689568956895689...
  5689/9999

1+1/2+1/4+1/8+...
  2

0
  0/1
Theorem 1

Any number with a periodic fractional part in a natural radix representation is rational

Proof:

Constructive, $\text{radix}=10$, no whole part:

- $x=0.n_1\ldots n_m n_1\ldots n_m\ldots=0.(n_1\ldots n_m)$
- $x\times10^m-x=n_1\ldots n_m$
- $x=n_1\ldots n_m/(10^m-1)$
Theorem 2

Any geometric series:

\[ S = q^0 + q^1 + q^2 + q^3 + \ldots \]

where \(-1 < q < 1, \ q \neq 0\)

evaluates to \( S = \frac{1}{1-q} \)

Proof

Proof idea (informally)

More formal proof
Every integer is a rational number

Proof: set the denominator to 1

Book: page 143
The set of rational numbers is closed with respect to arithmetic operations $+$, $-$, $\times$, $/$.

Partial proofs: textbook pages 144-145

Formal proof
Irrational Numbers

So far all the examples were of rational numbers

How about some irrationals?

- π
- e
- sqrt(2)
Summary for chapter 3

Proof techniques

Direct

- Existential – find one
- Universal
  - Contraposition
  - Arbitrarily chosen k, shown it’s true
  - Induction

Indirect

- contradiction