Logic in computer Science

Mathematical Logic

1

Mathematical Logic

As a continuation of symbolic logic in late 19th to mid 20th Century

Four important fields:

- Set theory,
- Model theory,
- Proof theory, and
- Computability theory.

2

Set Theory

- A *set* is a structure, representing an *unordered* collection of zero or more *distinct* objects.
- Set theory deals with operations between, relations among, and statements about sets
- *Set builder notation*: For any property $P(x)$ over any domain, $\{x \mid P(x)\}$ is *the set of all x such that P(x).*

  e.g., $\{ x \mid x$ is an integer where $x>0$ and $x<5 \}$

3

Basic Properties of Sets

- Sets are inherently *unordered*:
  - $\{a, b, c\} = \{a, c, b\} = \{b, a, c\} = \ldots = \{c, b, a\}$.
- All elements are *distinct* (unequal); multiple listings make no difference!
  - $\{a, b, c\} = \{a, a, b, a, b, c, c, c, c\}$.
- The empty set $\varnothing = \{\} = \{ x \mid$ **False**$\}$
- $1 \neq \{1\} \neq \{\{1\}\}$!!!
- **Cardinality**: $|S|$ is a measure of how many different elements S has. *E.g.*, $|\varnothing|=0$, $|\{1,2,3\}| = 3$, $|\{\{1,2,3\}\}| = 1$

4

4

The *Power Set* Operation

- The *power set* P(*S*) of a set *S* is the set of all subsets of *S*. P(*S*) = $\{x \mid x \subseteq S\}$.
- *E.g.* P({a,b}) = {∅, {a}, {b}, {a,b}}.
- Sometimes P(*S*) is written $\mathbf{2}^S$, because
- $|P(S)| = 2^{|S|}$ if S is finite
- |P(S)| > |S|, S is finite or not.
- *There are different sizes of infinite sets*!

5

5

Basic Set Relations

- ***Membership***: $x \in S$ *means* that object *x* is an ∈*lement* of set *S*.
  - $x \notin S :\equiv \neg(x \in S)$ "*x* is not in *S*"
- ***Equality***: $S=T$ *iff* $(\forall x: x \in S \leftrightarrow x \in T)$
- ***Subset***: $S \subseteq T$ *iff* $\forall x\, (x \in S \rightarrow x \in T)$
  - $\emptyset \subseteq S$, $S \subseteq S$.
- ***Proper subset***: $S \subset T$ *iff* $S \subseteq T$ *and* $S \neq T$.
- ***Union***: $A \cup B = \{ x \mid x \in A \vee x \in B \}$.
- ***Intersection***: $A \cap B = \{ x \mid x \in A \wedge x \in B \}$.
- ***Subtraction***: $A - B = \{ x \mid x \in A \wedge x \notin B \}$
- ***Complement***: $\overline{A} = U - A$, *where U is the universal set.*

6

6

Ordered *n*-tuples

- For $n \in \mathbf{N}$, the set of natural numbers, an *ordered n-tuple* or a *sequence of length n* is written $(a_1, a_2, \ldots, a_n)$. The *first* element is a_1, *etc.*
- These are like sets, except that duplicates matter, and the order makes a difference.
- Note $(1, 2) \neq (2, 1) \neq (2, 1, 1)$.
- Empty sequence, singlets, pairs, triples, quadruples, quintuples, …, *n*-tuples.

7

7

Cartesian Products of Sets

- For sets A, B, their *Cartesian product* $A \times B :\equiv \{ (a, b) \mid a \in A \text{ and } b \in B \}$.
- *E.g.* $\{a, b\} \times \{1, 2\} = \{ (a,1), (a,2), (b,1), (b,2) \}$
- For finite A, B, $|A \times B| = |A||B|$.
- The Cartesian product is ***not*** commutative: $A \times B \neq B \times A$ in general.
- Extends to $A_1 \times A_2 \times \ldots \times A_n$.
- $A^n = A \times A \times \ldots \times A$.

8

8

Set Identities

- Identity: $A \cup \varnothing = A \quad A \cap U = A$
- Domination: $A \cup U = U \quad A \cap \varnothing = \varnothing$
- Idempotent: $A \cup A = A = A \cap A$
- Double complement: $\overline{(\overline{A})} = A$
- Commutative: $A \cup B = B \cup A \quad A \cap B = B \cap A$
- Associative: $A \cup (B \cup C) = (A \cup B) \cup C$
  $A \cap (B \cap C) = (A \cap B) \cap C$
- DeMorgan's Law*:* $\overline{A \cup B} = \overline{A} \cap \overline{B}$
  $\overline{A \cap B} = \overline{A} \cup \overline{B}$

9

9

Generalized Union & Intersection

- *n*-ary union:
  $A \cup A_2 \cup \ldots \cup A_n = ((\ldots((A_1 \cup A_2) \cup \ldots) \cup A_n)$
- *n*-ary intersection:
  $A \cap A_2 \cap \ldots \cap A_n = ((\ldots((A_1 \cap A_2) \cap \ldots) \cap A_n)$
- "Big U" and "Big Arch" notation:
  $\bigcup_{i=1}^{n} A_i \qquad \bigcap_{i=1}^{n} A_i$
- For infinite sets of sets: $\bigcup_{A \in X} A \qquad \bigcap_{A \in X} A$

10

10

Relations and Functions

- A (binary) relation R is a subset of $A \times B$, where A, B are sets.
- For a $\in$ A and b $\in$ B, "a R b" is true iff (a, b) $\in$ R.
- Example: Let A be the students and B be the courses, relation $R \subseteq A \times B$ represents what students take what courses.
- A function f: A $\rightarrow$ B defines a relation $R \subseteq A \times B$: (a, b) $\in$ R iff f(a) = b. Thus, every function is a relation.
- Not all relations are functions: A relation $R \subseteq A \times B$ is a function if for any a $\in$ A and b, c $\in$ B, if (a, b) $\in$R and (a, c) $\in$R, then b = c.

11

11

Properties of Functions

- A function f: is a relation $R \subseteq A \times B$.
- A is the *domain* of f; B is the *range* of f.
- f is said to be *total* if $f(x)$ is defined for any $x \in A$; otherwise, f is said to be *partial.*
- f is *injective* if f is total and $f(x_1) \neq f(x_2)$ when $x_1 \neq x_2$.
- f is *surjective* (*a surjection*) if for every $y \in B$, there exists $x \in A$ such that $f(x) = y$.
- f is *bijective* (or *a bijection*, *one-to-one correspondence*) if f is both *injective* and *surjective.*
- f is *bijective* iff f has an inverse $f^{-1}: B \rightarrow A$

  $f(x) = y$ iff $f^{-1}(y) = x$.

12

Russell's Paradox

- Let T be the set that contains all sets which does **not** contain itself:

$$T = \{ S \mid S \notin S\}$$

Suppose T exists. Check to see $T \in T$, or $T \notin T$

1. If $T \in T$, by definition of T, $T \notin T$, a contradiction.
2. If $T \notin T$, by definition of T, $T \in T$, a contradiction.

- It caused a crisis in development of Set Theory.
- Cantor has found a solution: Sets should be hierarchical.
- The concept of "a set contains itself" is invalid.

13

How to Compare |S| and |T|?

It is easy when S is finite. How about infinite S?

$\mathbf{N} = \{0, 1, 2, 3, \ldots\}$ the set of natural numbers

$\mathbf{E} = \{0, 2, 4, 6, \ldots\}$ the set of even natural numbers

$|\mathbf{E}| < |\mathbf{N}|$? $\mathbf{E} \subset \mathbf{N}$, $\mathbf{E}$ is a proper subset of $\mathbf{N}$.

$f : \mathbf{E} \to \mathbf{N}$, $f(x) = x$, is injective, but not surjective.

$g : \mathbf{N} \to \mathbf{E}$, $g(x) = 2x$, is bijective (injective and surjective):

E: 0 2 4 6 8 10 12 14 16 …

N: 0 1 2 3 4 5 6 7 8 …

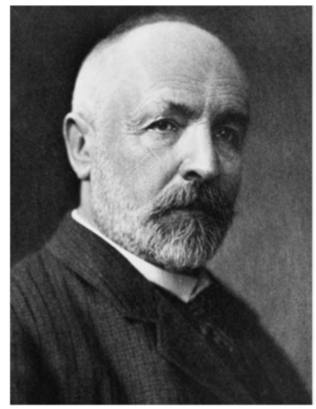
So $|\mathbf{E}| = |\mathbf{N}|$

14

Cantor's Solution

|S| = |T| if there is a bijection between S and T

Bronze monument to Cantor
in Halle-Neustadt, German



Georg Cantor
1845 – 1918

15

Countable Sets

A set S is *countable* if there exists an injective total function f: S → N.
S is *countably infinite* if S is both countable and infinite.

Claim: Every finite set is countable.
Proof: Let S = { $a_1, a_2, \ldots, a_n$ }.
Define $f(a_i) = i$, then f: S → N is injective.
So S is countable.

16

Countable Sets

Claim: Every subset S of **N** = {0, 1, 2, 3, …} is countable.

Proof: Define f(x) = x, then f: S → N is injective.

E = {0, 2, 4, 6, …}, the set of even natural numbers, is countable.

In fact, E is countably infinite.

17

Countable Sets

Claim: The set **Z** of integers is countably infinite.

Z = {… -3, -2, -1, 0, 1, 2, 3, …}

Proof: Define f(n) = **if** $0 \leq n$ **then** 2n **else** -1 – 2n.

Then f: **Z** → **N** is bijective: positive number to even numbers; negative numbers to odd numbers.

Z:	0	-1	1	-2	2	-3	3	-4	4	…
N:	0	1	2	3	4	5	6	7	8	…

18

Countable Sets

Claim: The set $\mathbf{N}^2$ of pairs of natural numbers is countably infinite.

$$\mathbf{N}^2 = \{(0,0), (0,1), (1,0), (1,1), (0,2), \ldots\}$$

Proof: Define $g(k) = k(k+1)/2$ (sum of first k positive integers), and $f(i, j) = g(i + j) + j$.

Then $f: \mathbf{N}^2 \to \mathbf{N}$ is bijective.

i\j	0	1	2	3	4	5
0	0	2	5	9	14	20
1	1	4	8	13	19	26
2	3	7	12	18	25	33
3	6	11	17	24	32	41
4	10	16	23	31	40	49

$k = 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$

$g(k) = 0 \quad 1 \quad 3 \quad 6 \quad 10 \quad 15 \quad 21$

$f(0,0) = 0$, $f(1,0) = 1$,

$f(0,1) = 2$, $f(2,0) = 3$, …

19

Countable Sets

Claim: S is countably infinite iff there is a bijection between S and **N**.

Proof: If there is a bijection between S and **N**, then S must be countable and infinite.

If S is countable, there is injective function $f: S \to \mathbf{N}$. Sort S by f, that is, let

$$S = \{ s_0, s_1, s_2, \ldots, s_k, \ldots \}$$

such that $i < j$ iff $f(s_i) < f(s_j)$.

Define $g: \mathbf{N} \to S$, $g(i) = s_i$, then g is a bijection between S and **N**.

20

Countable Sets

Claim: Any subset of a countable set is countable.

Proof is left as an exercise.

Claim: The set **R** of rational numbers is countable.

Proof: If we view each rational m/n as a pair (m, n), then **R** is a subset of $\mathbf{N}^2$. Since $\mathbf{N}^2$ is countable, so is **R**.

21

Countable Sets

Claim: The set $\{0, 1\}^*$ of all binary strings (of finite length) is countably infinite.

$$\{0, 1\}^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots \}$$

where shorter strings go first; then smaller values go first.

Proof: (easy) Define an injection $h: \{0, 1\}^* \to \mathbf{N}$: $h(\varepsilon) = 0$, $h(s)$ replaces every 0 by 2 and leaves 1 intact. Then $h: \{0, 1\}^* \to \mathbf{N}$ is injective:

$\{0, 1\}^*$: ε, 0, 1, 00, 01, 10, 11, 000, 001, …

N: 0, 2, 1, 22, 21, 12, 11, 222, 221, …

22

Countable Sets

Claim: The set $\{0, 1\}^*$ of all binary strings (of finite length) is countably infinite.

Proof: (harder) Define a bijection f: $\{0, 1\}^* \rightarrow \mathbf{N}$:

For s in $\{0, 1\}^*$, there are $1+2+2^2+...+2^{n-1} = 2^n - 1$ strings shorter than s, where $n = |s|$, the length of s.

Let v(s) be the decimal value of s, then there are v(s) strings of length n before s in the listing.

So the position of s in the list is $2^n + v(s)$.

Define $f(s) = 2^{|s|} + v(s) - 1$. Then f is a bijection:

$\{0, 1\}^*$: ε, 0, 1, 00, 01, 10, 11, 000, 001, …

N: 0 1 2 3 4 5 6 7 8 …

23

Countable Sets

A set S is *countably infinite* iff there is a bijection between S to $\mathcal{N}$, the natural numbers.

- $\mathcal{N}$ is countable.
- Subsets of countable sets are countable.
- The set of even natural numbers is countable.
- The set of all binary strings is countable.
- The union of two countable sets is countable.
- The Cartesian product of two countable sets is countable.

- Are there any uncountable sets?

24

Uncountable Sets

There are infinite many uncountable sets.

- ***R***: the set of real numbers.
- ***R*$_1$**: the set of real numbers between 0 and 1.
- $\mathscr{B}$: the set of infinite-length of binary strings
- $\mathscr{F}$: the Boolean functions over N.
- $\mathscr{P}$(N): the power set of natural numbers.
- $\mathscr{L}$: the set of all formal languages.
- The power set of any infinite set.

The proof is based on Cantor's Diagonalization Method.

25

Uncountable Sets

$\mathscr{B}$, the set of infinite-length of binary strings, is not countable.

- If $\mathscr{B}$ is countable, then there is a bijection between $\mathscr{B}$ and N.
- Let $\mathscr{B}$ = {s_1, s_2, …, s_i, … }, such that s_i maps to i.
- Construct the string s such that the j^{th} symbol of s is the complement of the j^{th} symbol of string s_j.
- Then s is a binary string not in $\mathscr{B}$, a contradiction.

$$
\begin{aligned}
s_1 &= 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\ldots\\
s_2 &= 1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\ldots\\
s_3 &= 0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\ldots\\
s_4 &= 1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\ldots\\
s_5 &= 1\,1\,0\,1\,0\,1\,1\,0\,1\,0\,1\ldots\\
s_6 &= 0\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\ldots\\
s_7 &= 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\ldots\\
s_8 &= 0\,0\,1\,1\,0\,0\,1\,1\,0\,0\,1\ldots\\
s_9 &= 1\,1\,0\,0\,1\,1\,0\,0\,1\,1\,0\ldots\\
s_{10} &= 1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\ldots\\
s_{11} &= 1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\ldots\\
\vdots &\quad \vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\vdots\,\ddots
\end{aligned}
$$

$$s = 1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\ldots$$

If s ∈ $\mathscr{B}$, then s = s_j for some j: s and s_j differ on the j^{th} symbol

26

Uncountable Sets

1. $\mathcal{B}$, the set of infinite-length of binary strings.
2. $\boldsymbol{R_1}$: the set of real numbers between 0 and 1.

- It suffices to show that there is a bijection between $\boldsymbol{R_1}$ and $\mathcal{B}$.
- Define f: $\mathcal{B} \rightarrow \boldsymbol{R_1}$, where f(s) = 0.s, a real in binary.
- E.g., s = 0001000110…, f(s) = 0.0001000110…
- It is easy to check that f is injective and surjective, or f has an inverse.

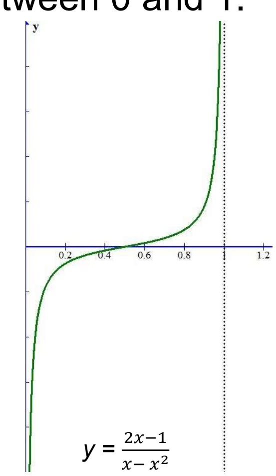
27

Uncountable Sets

1. $\mathcal{B}$, the set of infinite-length of binary strings.
2. $\boldsymbol{R_1}$: the set of real numbers between 0 and 1.
3. $\boldsymbol{R}$: the set of real numbers.

- It suffices to show that there is a bijection between $\boldsymbol{R_1}$ and $\boldsymbol{R}$.
- Define f: $\boldsymbol{R_1} \rightarrow \boldsymbol{R}$,

  $f(x) = (2x - 1)/(x - x^2)$.
- It is easy to check that f is injective and surjective.



28

Uncountable Sets

1. $\mathscr{B}$, the set of infinite-length of binary strings.
2. $\boldsymbol{R_1}$: the set of real numbers between 0 and 1.
3. $\boldsymbol{R}$: the set of real numbers.
4. $\mathscr{F}$: the Boolean functions over N.

- It suffices to show that there is a bijection between $\mathscr{F} = \{f \mid f: N \to \{0, 1\}\}$ and $\mathscr{B}$.
- Define g: $\mathscr{F} \to \mathscr{B}$, $g(f) = f(0)f(1)\ldots f(i)\ldots$, an infinite binary string.
- It is easy to check that g is injective and surjective.

29

Uncountable Sets

1. $\mathscr{B}$, the set of infinite-length of binary strings.
2. $\boldsymbol{R_1}$: the set of real numbers between 0 and 1.
3. $\boldsymbol{R}$: the set of real numbers.
4. $\mathscr{F}$: the Boolean functions over N.
5. $\mathscr{P}(N)$: the power set of natural numbers.

- It suffices to show that there is a bijection between $\mathscr{F} = \{f \mid f: N \to \{0, 1\}\}$ and $\mathscr{P}(N)$.
- Define g: $\mathscr{F} \to N$, $g(f) = \{\, i \mid f(i) = 1, i \in N\}$.
- It is easy to check that g is injective and surjective.
- So there is no bijection between N and $\mathscr{P}(N)$.

30

Uncountable Sets

Cantor's Theorem: $|A| < |\mathscr{P}(A)|$ for any set A.

- **Proof** by contradiction: If $|A| = |\mathscr{P}(A)|$, there is a bijection f between A and $\mathscr{P}(A)$.
- Define $S = \{ a \in A \mid a \notin f(a) \} \subseteq A$.
- Since $S \in \mathscr{P}(A)$, there exists $b \in A$ such that $f(x) = S$. Only two possibilities: $b \in S$ or $b \notin S$.

1. If $b \in S$, by definition of S, $b \notin f(b) = S$.
2. If $b \notin S$, by definition of S, $b \in f(b) = S$.

- Both cases have a contradiction, f can exist.
- It cannot be $|A| > |\mathscr{P}(A)|$ because $g(a) = \{a\}$ is an injection from A to $\mathscr{P}(A)$.

31

No Set of All Sets

Cantor's theorem implies that *there is no such thing as the "set of all sets".*

Proof:

- Suppose A were the set of all sets.
- Since every element of $\mathscr{P}(A)$ is a set, so $\mathscr{P}(A) \subseteq A$.
- Thus $|\mathscr{P}(A)| \leq |A|$, a contradiction to Cantor's theorem.

32

Cardinality Numbers

- Cantor chose the symbol $\aleph_0$ = |N|. $\aleph_0$ is read as aleph-null, after the first letter of the Hebrew alphabet.
- The cardinality of the reals is often denoted by $\aleph_1$, or *c* for the continuum of real numbers.

Set	Description	Cardinality
Natural numbers	1, 2, 3, 4, 5, …	$\aleph_0$
Integers	…, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, …	$\aleph_0$
Rational numbers	pair of natural numbers	$\aleph_0$
Real numbers	All decimals	*c*

33

Infinity of infinities

Cantor's theorem implies that there are infinitely many infinite cardinal numbers, and that there is no largest cardinal number.

$\aleph_0 = |N|$

$\aleph_1 = |\mathcal{P}(\mathrm{N})| = 2^{\aleph_0} > \aleph_0$

$\aleph_2 = |\mathcal{P}(\mathcal{P}(\mathrm{N}))| = 2^{\aleph_1} > \aleph_1$

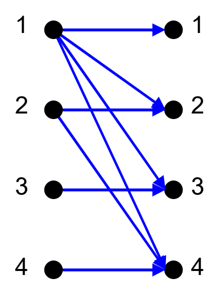
$\aleph_3 = |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathrm{N})))| = 2^{\aleph_2} > \aleph_2$

…

34

Relations on a set

- A relation *R* on the set *S* is a relation from *S* to *S.*
- Every relation *R* on *S* is equivalent to a digraph *G* = (*S, R*).
- Example: Let *S* be the set { 1, 2, 3, 4 }
  – Which pairs are in the relation *R* = { (*a*,*b*) | *a* divides *b* }
  – R = { (1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4) }



R	1	2	3	4
1	X	X	X	X
2		X		X
3			X	
4				X

More Examples

- Consider some relations on the set **Z** of integers.
- Are the following ordered pairs in the relation?

	(1,1)	(1,2)	(2,1)	(1,-1)	(2,2)
• R_1 = { (*a*, *b*) | $a \le b$ }	X	X			X
• R_2 = { (*a*, *b*) | $a > b$ }			X	X	
• R_3 = { (*a*, *b*) | $a = \|b\|$ }	X			X	X
• R_4 = { (*a*, *b*) | $a = b$ }	X				X
• R_5 = { (*a*, *b*) | $a = b+1$ }			X		
• R_6 = { (*a*, *b*) | $a+b \le 3$ }	X	X	X	X	

Relation Properties

Six properties of relations: for any $a, b, c \in A$

- Reflexive: $(a, a) \in R$
- Irreflexive: $(a, a) \notin R$
- Symmetric: If $(a, b) \in R$, then $(b, a) \in R$
- Asymmetric: If $(a, b) \in R$, then $(b, a) \notin R$
- Antisymmetric: If $(a, b) \in R$, $(b, a) \in R$, then a = b
- Transitive: If $(a, b) \in R$, $(b, c) \in R$, then $(a, c) \in R$

37

37

Notes on symmetric relations

- A relation can be neither symmetric or asymmetric
  - R = { (a,b) | a=|b| }
  - This is not symmetric
    - -4 is not related to itself
  - This is not asymmetric
    - 4 is related to itself
  - It is antisymmetric

38

38

Relations on numbers summary

	=	<	>	≤	≥
Reflexive	X			X	X
Irreflexive		X	X		
Symmetric	X				
Asymmetric		X	X		
Antisymmetric	X			X	X
Transitive	X	X	X	X	X

39

39

Composition of Relations

- Let R be a relation from A to B, and S be a relation from B to C
- The composite of R and S, denoted by $S \circ R$, consists of the ordered pairs (a, c), if $(a, b) \in R$, and $(b, c) \in S$, where $a \in A$, $b \in B$, and $c \in C$
- Note that S comes first when writing the composition!
- Example: Let M be the relation "is mother of" and F be the relation "is father of"
- What is $M \circ F$?
  - If $(a,b) \in F$, then a is the father of b
  - If $(b,c) \in M$, then b is the mother of c
  - Thus, $M \circ F$ denotes the relation "maternal grandfather"

40

40

Composition of Relations on a Set

Given relation R on S:

- $R^1 = R$
- $R^{n+1} = R^n \circ R$
  - Example: $R^2 = R \circ R$, $R^3 = R \circ R \circ R$, *etc.*
- The meaning of R^k in graph G = (S, R): (a, b) $\in R^k$ iff there is a path of length k from a to b.
- Let R^0 denote $\{ (x,x) \mid x \in S \}$.
- R^0 is the set of all loops in G = (S, R).
- The reflexive closure of R is $R \cup R^0$

41

41

Composition of Relations on a Set

- The transitive closure of R is

  $R^+ = R^1 \cup R^2 \cup \ldots \cup R^n \cup \ldots$
- The reflexive and transitive closure of R is

  $R^* = R^+ \cup R^0 = R^0 \cup R^1 \cup \ldots \cup R^n \cup \ldots$

- Example: S = { 1, 2, 3 } and R = {(1, 1), (1, 2), (2, 3)}
  - R^+ = {(1, 1), (1, 2), (2, 3), (1, 3)}
  - R^* = {(1, 1), (1, 2), (2, 3), (1, 3), (2, 2), (3, 3)}

42

42

Equivalence Relations

- **Equivalence relations** are used to relate objects that are similar in some way.
- A relation *R* on a set A is an equivalence relation if it is reflexive, symmetric, and transitive.
- Two elements that are related by an equivalence relation R are called **equivalent**.
- The best representation of an equivalence relation is Sets: equivalent items are in the same set.

43

Equivalence Relation: Example

- Suppose $f: A \rightarrow B$ is a function and A is non-empty.
- Let R be the relation on A: $R(x,y)$ is true iff $f(x) = f(y)$
- Show that R is an equivalence relation on A

- Reflexivity: $f(x) = f(x)$
  - True, as given the same input, a function always produces the same output
- Symmetry: if $f(x) = f(y)$ then $f(y) = f(x)$
  - True, by the definition of equality
- Transitivity: if $f(x) = f(y)$ and $f(y) = f(z)$ then $f(x) = f(z)$
  - True, by the definition of equality

44

44

Equivalence Classes

- Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the *equivalence class* of a.
- The equivalence class of a with respect to R is denoted by $[a]_R$
- When only one relation is under consideration, the subscript is often deleted, and $[a]$ is used to denote the equivalence class
- Note that these classes are disjoint!
  - As the equivalence relation is symmetric and transitive.

45

45

Example and Partition

- Consider $R = \{ (a,b) \mid a \bmod 2 = b \bmod 2 \}$
- The even numbers form an equivalence class
  - As do the odd numbers
- The equivalence class for the even numbers is denoted by [2] (or [4], or [784], etc.)
  - [0] = { …, -4, -2, 0, 2, 4, … }
  - 0 is a *representative* of its equivalence class
- There are only 2 equivalence classes formed by this equivalence relation, and they form a partition of the integers
- A partition of a set S is a collection of non-empty disjoint subsets of S whose union is S

46

46

Partitions

- Consider the relation R = { (a,b) | a mod 2 = b mod 2 }
- This splits the integers into two equivalence classes: even numbers and odd numbers
- Those two sets together form a partition of the integers
- Formally, a partition of a set S is a collection of non-empty disjoint subsets of S whose union is S
- In this example, the partition is { [0], [1] }
  - Or { {…, -3, -1, 1, 3, …}, {…, -4, -2, 0, 2, 4, …} }

47

47

Mathematical Logic

Four important fields:

- Set theory,
- Model theory,
- Proof theory, and
- Computability theory.

48

Model Theory

- Model theory is the study of mathematical structures (e.g. groups, fields, algebras, graphs, logics) in a formal language.
- Every formal language has its syntax and semantics.
- Models are a semantic structure associated with syntactic structures in a formal language.
- Theories are then introduced based on models.

49

Syntax and Semantics

- The syntax of a formal language specifies how various components of the language, such as symbols, words, and sentences, are defined.
- The semantics of a language specifies the meaning of various components of the language.
  - Meaning can be informal and formal.
  - Formal meanings can be checked by procedures or proofs using syntactic components.

50

Logic as a Language

- Syntax:
  - Symbols: What symbols are eligible
  - Grammars: how well-formed sentences (formulas) are formed
- Semantics:
  - Meaning of symbols
  - Truthiness of formulas
- Inference Systems
  - How to prove theorems (true formulas if the premises are true) from the given premises.

51

Models and Abstract Algebras

- In model theory, a theory is defined by a set of sentences and a model is an interpretation that satisfies the sentences of that theory.
- Abstract algebras are often used as models:

  model theory = abstract algebra + logic
- Abstract algebra (or universal algebra) is a broad field of mathematics, concerned with sets of abstract objects associated various operations and properties.

52

Boolean Algebra

- Most relevant to the logic of this course
- Almost a synonym of propositional logic (chapter 2)
- In Boolean algebra, 0 is used for false and 1 for true, + for disjunction, · for conjunction, It is thus a formalism for describing logical operations in the same way that elementary algebra describes numerical operations, such as addition and multiplication, like most other algebras.

53

Mathematical Logic

Four important fields:

- Set theory,
- Model theory,
- Proof theory, and
- Computability theory.

54

Proof Theory

- Proof Theory is a major branch of mathematical logic that represents proofs as formal mathematical objects, facilitating their analysis by mathematical techniques.
- In Proof Theory, a theory is defined by a set of formulas (sentences) called axioms.
- Assuming the axioms are true, the formula proved to be true by various proof methods are called theorems.

55

Axioms and Theorems: Example

- **Example**: Assume $\perp$ is false (0), T is true (1), $\neg$ is negation.
- The axioms are $\neg \perp = T$, $\neg T = \perp$.
- Prove $\neg \neg p = p$ is a theorem by case analysis:
- Case 1: $p = \perp$. $\neg \neg \perp = \neg T = \perp$
- Case 2: $p = T$. $\neg \neg T = \neg \perp = T$.

56

Properties of Axioms

- Consistency: A set of axioms is consistent if it allows all the axioms to be true at the same time.
  - For example, { p, $\neg$ p} is not consistent because p and $\neg$ p cannot be true at the same time.
- Independency: A set of axioms is indedendant if no axiom is a theorem of the other axioms. That is, no axioms can be deleted without changing the theorems that can be derived.

57

Proof Procedures

- A proof procedure P(A, B) takes a set A of axioms and a formula B as input, and returns true if it claims B is a theorem from A.

Two properties of P(A, B):

- Soundness: If P(A, B) returns true, then B is indeed a theorem of A.
- Completeness: If B is a theorem of A, then P(A, B) will return true in a finite number of steps.

58

Inference Systems

- A proof procedure is expressed as a set of rules (inference rules)
- Derive a formula (conclusion) is a theorem from the axioms (premises) by the rules
- Properties of an inference system:
  - Soundness: every proved formula must be a theorem.
  - Completeness: every theorem can be proved by the given inference system.

59

Premises, Conclusion and Proofs

- In logic, pieces of reasoning are analyzed using the notion of a proof.
- A proof consists of any number of *premises*, and any number of (intermediate and one final) *conclusions.*
- Premises are statements which are assumed to be true.
- We are merely interested in whether each conclusion follows logically from the premises: We are *not* interested in whether those premises are really true.

60

Deductive vs Inductive Validity

- A proof is said to be *deductively* valid if, assuming the premises to be true, the conclusion *must* be true as well.
- A proof is said to be *inductively* valid if, all the instances of the conclusion are shown to be true from the premises. The conclusion may be false if new premises are added.
- Example: We may show (x + y) = (y + x) for all natural numbers as an inductive theorem.
- If we add later an error value, err, to the natural numbers, then (x + y) = (y + x) may be false, because (1 + err) $\neq$ (err + 1).

61

Proof by Contradiction (Disproof)

- A statement is valid if it is impossible for the conclusion to be false while the premises are true.
- Thus, to demonstrate invalidity, all we have to do is to demonstrate that it is possible for the statement to be false while the premises are true.
- The easiest way to do this is to come up with a scenario (or possible world) in which all premises are true and the concluding statement false.

62

Decision Procedures

- A decision procedure is a sound proof procedure P(A, B) which stops on every input (A, B) with the answer "yes" or "no".
- **Claim**: A decision procedure is always complete.
- Proof: P(A, B) will always stop on every input (A, B). If B is a theorem, P(A, B) must return "yes" because P(A, B) is sound.
- Note: Some proof procedures may stop with "yes", "no", or "unknown", or loop forever.

63

Mathematical Logic

Four important fields:

- Set theory,
- Model theory,
- Proof theory, and
- Computability theory.

64

Computability Theory

- Computability theory, used to be called recursion theory, is a branch of mathematical logic and the theory of computation that studies computable functions.
- The field has since expanded to include the study of generalized computability and definability. In these areas, computability theory overlaps with proof theory and set theory.

65

Recursion Theory

- Recursion is used to construct objects and functions.
- **Example**: Given a constant symbol 0 of type T and a function symbol $s : T \rightarrow T$, the objects of type T can be recursively constructed as follows:

1. 0 is an object of type T;
2. If n is an object of type T, so is s(n);
3. Nothing else will be an object of T.

- $T = \{0, s(0), s^2(0), s^3(0), ..., s^i(0), ...\}$, which has bijection to the set of natural numbers.

66

Recursion Theory

- Functions can be recursively defined in a similar way. Let pre, add, sub, mul be the
- pre: T → T
- pre(0) = 0;
- pre(s(x)) = x.
- predecessor, addition, subtraction, and multiplication functions over the set of natural numbers:

67

Backus–Naur form (BNF)

- A notation technique for context-free grammars, often used to describe the syntax of programming languages
- Can be used to define the objects constructed by recursion.
- E.g., $\langle N \rangle ::= 0 \mid s(\langle N \rangle)$ defines

  $N = \{ 0, s(0), s^2(0), s^3(0), \ldots, s^i(0), \ldots\}$
- $\langle B \rangle ::= \varepsilon \mid 0\langle B \rangle \mid 1\langle B \rangle$ defines

  $B = \{ \varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$

68

Recursion Theory

Functions can be recursively defined, too.

- pre: T → T // predecessor
- pre(0) = 0;
- pre(s(x)) = x

- add: T, T → T // addition
- add(0, y) = y;
- add(s(x), y) = s(add(x, y)).

- sub: T, T → T // subtraction
- sub(x, 0) = x;
- sub(x, s(y)) = sub(pre(x), y).

- mul: T, T → T // multiplication
- mul(0, y) = 0;
- mul(s(x), y) = add(mul(x, y), y).

- <: T, T → {0, 1} // less than
- (x < 0) = 0;
- (0 < s(y)) = 1;
- s(x) < s(y) = x < y.

69

Computable Functions

- What does it mean "a function is computable" or "not computable"?
- **Church-Turing Thesis**: If a function can be computed, it must be computed by a Turing machine.
- Turing machine serves as a criterion to see if a function is computable or not: Do we have a Turing machine to compute it?
- Set of Turing machines is countable.
- Set of functions is uncountable. Thus, many, many functions are not computable.

70

Turing Completeness

- A computing model is **Turing complete** if the model can simulate a Turing machine, meaning it is theoretically capable of doing all tasks done by computers.
- Nearly all computers are Turing complete if the limitation of finite memory is ignored.
- Some logics are also Turing complete as they can also be used to simulate a Turing machine. As a result, some problems for such logics are not decidable.
- Computability theory helps us to decide if there exist decision procedures for some logics.