Sets

BIG IDEAS

Themes

1. There exist functions that cannot be computed in Java or any other computer language.

2. There exist subsets of the Natural Numbers that cannot be described in English or any other language.

Questions

1. What is a Function?

2. What is a Set?

3. What is a Subset?

<u>**Sets and Elements**</u>

Terms

- Sets = basic building blocks for mathematics

- Elements = members of sets

  -- virtually anything, even other sets

- Set = a collection of elements

  -- $x \in A$ means x is an element of the set A

  -- $x \notin A$ means x is NOT an element of the set A

<u>How to Build Sets</u>

1. *Enumerate all the elements*
   a. $\{red, blue, green\}$
   b. $\{1, 1, 2, 3, 5, 8, 13, \ldots\}$

2. *Specify a common property*
   a. $\{x \mid x \text{ is a fibonacci number}\}$
   b. $\{x \mid p(x) \text{ is true}\}$
   c. Observations
      i. any predicate can be used to specify a set
      ii. x is a dummy variable
      iii. usually there is a <u>universal set</u> or <u>domain</u> from which x is chosen
   d. Analogy -- sets $\approx$ predicates

3. *Sets are completely determined by their elements*
   a. order does not matter
   b. duplicates do not matter
   c. no additional information matters

<u>**Notation**</u>

Equals

- $A = B$ means $\forall x (x \in A \Leftrightarrow x \in B)$

Subset

- $B \supset A$ means $\forall x (x \in A \Rightarrow x \in B)$

Union

- $A \cup B = \left\{ x \mid (x \in A) \vee (x \in B) \right\}$

Intersection

- $A \cap B = \left\{ x \mid (x \in A) \wedge (x \in B) \right\}$

Complement

- $A^C = \{ x \mid \sim x \in A \} = \{ x \mid x \notin A \}$

Empty Set

- $\phi = \{ x \mid False \}$

Rules for Manipulating Sets	Rules of Propositional Calculus
1. *Commutativity*	
a. $A \cup B = B \cup A$	$p \vee q = q \vee p$
b. $A \cap B = B \cap A$	$p \wedge q = q \wedge p$
2. *Associativity*	
a. $(A \cup B) \cup C = A \cup (B \cup C)$	$(p \vee q) \vee r = p \vee (q \vee r)$
b. $(A \cap B) \cap C = A \cap (B \cap C)$	$(p \wedge q) \wedge r = p \wedge (q \wedge r)$
3. *Distributive Laws*	
a. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$
b. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$
4. *De Morgan's Laws (Generalize by Induction)*	
a. $(A \cup B)^c = A^c \cap B^c$	$\sim(p \vee q) = (\sim p) \wedge (\sim q)$
b. $(A \cap B)^c = A^c \cup B^c$	$\sim(p \wedge q) = (\sim p) \vee (\sim q)$
5. *Complements*	
a. $(A^c)^c = A$	$\sim\sim p = p$
b. $A \cup A^c = U$	$p \vee \sim p = T$
c. $A \cap A^c = \phi$	$p \wedge \sim p = F$

<u>Sets and Rules of the Propositional Calculus</u>

Analogies

a. $\cup \approx \vee$

b. $\cap \approx \wedge$

c. $c \approx \sim$

d. $U \approx T$

e. $\phi \approx F$

Proofs

a. Membership Tables $\Leftrightarrow$ Truth Tables

b. Reduce to rules for or, and, not

BIG IDEA

a. Equivalences in Propositional Calculus $\Rightarrow$ Identities in Set Theory

b. Mechanical: Logical Operators $\Rightarrow$ Boolean Operations

Set Membership Table

A	B	A^c	B^c	$A^c \cap B^c$	$A \cup B$	$(A \cup B)^c$
1	1	0	0	0	1	0
1	0	0	1	0	1	0
0	1	1	0	0	1	0
0	0	1	1	1	0	1

$$(A \cup B)^c = A^c \cap B^c$$

Theorem: $(A \cup B)^c = A^c \cap B^c$

$\Pr oof:$ $x \in (A \cup B)^c \Leftrightarrow x \notin A \cup B$

$$\Leftrightarrow \sim \big((x \in A) \vee (x \in B)\big)$$

$$\Leftrightarrow \sim (x \in A) \wedge \sim (x \in B) \qquad \textit{De Morgan's Law}$$

$$\Leftrightarrow (x \notin A) \wedge (x \notin B)$$

$$\Leftrightarrow (x \in A^c) \wedge (x \in B^c)$$

$$\Leftrightarrow x \in A^c \cap B^c$$

Definitions and Notation

1. *Disjoint*

    a. A and B have no common element

    b. $A \cap B = \phi$

2. *Difference*

    a. $A - B = \left\{ x \mid (x \in A) \wedge (x \notin B) \right\}$

    b. $A - B = A \cap B^c$

3. *Cross Product*

    a. $A \times B = \left\{ (a,b) \mid (a \in A) \wedge (b \in B) \right\}$

Definitions and Notation (continued)

4. *Cardinality*

   a. $|A| =$ cardinality of A = the number of elements in the set A

   b. $|A \cup B| = |A| + |B| - |A \cap B|$

   c. $|A \times B| = |A|\,|B|$

5. *Power Set*

   a. $P(A) = \{B \mid A \supset B\}$ = set of all subsets of A

   b. $|P(A)| = 2^{|A|}$ -- proof by binomial enumeration or induction

Theorem: A set with n elements has exactly 2^n subsets including itself and the empty set.

Proof:

Base Cases: $n = 0,1$.

- A Set with $n = 0$ elements has $2^0 = 1$ subset: the empty set.
- A Set with $n = 1$ elements has $2^1 = 2$ subsets: the empty set and the Set itself.

Inductive Step:

- Assume: Every set with n elements has exactly 2^n subsets including itself and the empty set.
- Must Show: Every set with $n+1$ elements has exactly 2^{n+1} subsets including itself and the empty set.

Inductive Proof: Let

- S = a set with $n+1$ elements.
- T = the set S with one element x removed from S.

Now observe that:

i. Since T has n elements, it follows by the inductive hypothesis that T has 2^n subsets.

ii. Every subset of S either contains x or does not contain x.

iii. There are exactly as many subsets of S that contain S as do not contain x -- Tricky Step!

iv. The number of subsets of S that do not contain x is the same as the number of subsets of T, which is 2^n.

v. Therefore the total number of subsets of S is $2(2^n) = 2^{n+1}$.

Example

- $S = \{1,2,3\}$
- $T = \{1,2\}$

Subsets of T = Subsets of S without 3	*Subsets of S with 3*
$\{\ \}$	$\{3\}$
$\{1\}$	$\{1, 3\}$
$\{2\}$	$\{2, 3\}$
$\{1, 2\}$	$\{1, 2, 3\}$

Proof

- $S = a\ \ finite\ \ set$
- $x \in S$
- $T = S - \{x\}$

Subsets of T = Subsets of S without x	*Subsets of S with x*
T_1	$\{T_1, x\}$
T_2	$\{T_2, x\}$
$\vdots$	$\vdots$
T_d	$\{T_d, x\}$

Infinite Union and Intersection

1. I = infinite indexing set -- can be uncountable

2. $$\bigcup_{i\in I} S_i = \left(x \mid \exists i \in I,\ x \in S_i\right)$$

3. $$\bigcap_{i\in I} S_i = \left(x \mid \forall\, i \in I,\ x \in S_i\right)$$

4. No limits, no convergence, just sets.

Russell's Paradox

1. Type 1 Sets = Sets that contain themselves as Elements
   - Example: Set consisting of all sets with 3 or more Elements

2. Type 2 Sets = Sets that do not contain themselves as Elements
   - **N**, **Z**, ...

3. Let S = All Sets of Type 2 = Set of all sets not containing themselves as Elements
   - $S \in S \;\rightarrow\; S$ is Type 1 $\;\rightarrow S \notin S$ CONTRADICTION
   - $S \notin S \;\rightarrow\; S$ is Type 2 $\;\rightarrow\; S \in S$ CONTRADICTION

   But every element must either be in S or not in S!

4. Naive Set Theory breaks down.
   - Axiomatic Set Theory introduced to control these paradoxes.

Functions

<u>Relations</u>

Ordered Pair -- (x,y)

- $(x, y) = (x^*, y^*)$ means that $x = x^*$ and $y = y^*$
- $(x, y) \neq (y, x)$ -- order matters

Cross Product

- $A \times B = \{(a,b) \mid (a \in A) \wedge (b \in B)\}$
- $|A \times B| = |A|\,|B|$

Binary Relation

- Any subset R of $A \times B$ is called a <u>binary relation</u> on A,B.
- $(a, b) \in R \Leftrightarrow aRb$

Functions

Definition

1. A *function* is any binary relation R where $(a, b), (a, c) \in R \Rightarrow b = c$

2. A *function* is a rule that assigns to each $a \in A$ a *unique* $b \in B$

   -- $b = f(a) \Leftrightarrow (a, b) \in R$

Applications

1. To measure relative size of Sets (finite and infinite)
   -- 1-1 Correspondence

2. To measure the relative speed of Algorithms
   -- $O(h)$ Notation

3. To store Subsets efficiently
   -- Bitstrings

Notation

Functions

- $B^A = \{f \mid f : A \to B\}$

Example

- $2 = \{0, 1\}$
- $2^A = \left\{f \mid f : A \to \{0,1\}\right\}$

Functions, Bitstrings, and Subsets

Main Observations

- Functions, Bitstrings, and Subsets are the same things

Functions, Bitstrings, and Subsets

- $2^A = \left\{ f \mid f : A \to \{0,1\} \right\} = \{S \mid S \subseteq A\}$ -- Functions and Bitstrings

  -- $\left\{ f \leftrightarrow S \right\} \Leftrightarrow \left\{ a \in S \Leftrightarrow f(a) = 1 \right\}$ -- Subsets

  -- $\left| 2^A \right| = 2^{|A|}$

Efficient Bitstring Representation of Subsets

- Fast Union (OR), Intersection (AND) and Complement

Bitstring Representation of Subsets

Example

- $A = \{a_1, \ldots, a_{10}\}$
- $S = \{a_2, a_4, a_5, a_9\}$
- $b_S = 0101100010$

Bitwise Boolean Operations

Union (OR)

- $1100010 \vee 1010100 = 1110110$

Intersection (AND)

- $1100010 \wedge 1010100 = 1000000$

Complement (Negation)

- $\sim 1100010 = 0011101$

Definitions

1. Domain
2. Range
3. Injective
4. Surjective
5. Bijective
6. Composite

Inverses

$f : A \to B$

- $f^{-1} = \{(b,a) \mid f(a) = b\}$ is a relation

  -- NOT necessarily a function

- f^{-1} is a function if and only if *f* is bijective.

- If *f* is injective, then f^{-1} is a function whose Domain is the Range of *f*.

Induced Functions

$f : A \to B$

- $f : P(A) \to P(B)$ where $f(S) = \{ f(a) \mid a \in S \}$
- $f^{-1} : P(B) \to P(A)$ where $f^{-1}(S) = \{ a \mid f(a) \in S \}$
- f^{-1} is a relation

  -- $B \times A \subset f^{-1}$

  -- f^{-1} is NOT a function on B

Functions and Set Operations

1. $f(S^c) \neq f(S)^c$

2. $f^{-1}(T^c) = \left(f^{-1}(T)\right)^c$

3. Union and Intersection -- Exercises

4. $f(x+y) = f(x) + f(y)$?

Theorem: $f^{-1}(T^c) = \left(f^{-1}(T)\right)^c$

Proof: $x \in f^{-1}(T^c) \Leftrightarrow f(x) \in T^c$

$$\Leftrightarrow f(x) \notin T$$

$$\Leftrightarrow x \notin f^{-1}(T)$$

$$\Leftrightarrow x \in \left(f^{-1}(T)\right)^c$$

Composite Functions

If $f: A \to B$ and $g: B \to C$, then $g \circ f: A \to C$

1. f, g 1-1 $\Rightarrow$ $g \circ f$ 1-1

2. f, g onto $\Rightarrow$ $g \circ f$ onto

3. f, g bijective $\Rightarrow$ $g \circ f$ bijective

Countable and Uncountable Sets

<u>**BIG IDEAS**</u>

There exist non-computatble functions.

There exist subsets of the Natural Numbers that we cannot describe.

Countable

Examples

1. Finite
   - -- Comes to an End

2. 1-1 correspondence with $\boldsymbol{N}$
   - -- Does not Come to an End
   - -- No Last Number
   - -- Infinite List

3. $f : \boldsymbol{N} \to S$ onto

4. $f : A \to S$ onto, A countable

Infinity

Infinity (∞) is NOT a natural number

-- $\infty + 1 = \infty$

-- $\infty + \infty = \infty$

-- $\infty \times \infty = \infty$

-- $\infty^n = \infty$

Size is measured by bijection NOT by subset!

Cardinality

Size

- There are many different notions of relative size:

  -- Subset

  -- Length

  -- 1-1 Correspondence

- These notions are NOT the same.

- Cardinality deals with 1-1 correspondence.

<u>Countable Sets</u>

1. $\mathbf{N}$
2. $\mathbf{N} \cup \{-1\}$
3. **Even numbers, Odd numbers**
4. $\mathbf{Z}$
5. $\mathbf{N} \mathrm{x} \mathbf{N}$
6. $\mathbf{Q}$
7. $A \times B$ **--** if A,B are both countable
8. $A_1 \times \cdots \times A_n$ -- if $A_1, \ldots, A_n$ are all countable
9. $B \supset A$, and B countable $\Rightarrow A$ countable

Tricks for Proving Countability

1. Shifts
   - $-1, 0, 1, 2, ...$
   - Even numbers
2. Interleave -- $\boldsymbol{Z}$
3. Doubly Infinite Patterns -- $\boldsymbol{N} \times \boldsymbol{N}$
4. Bijection from $\mathbf{N}$ or $A \times B$, where A, B are countable
5. Subset of a countable set
6. Intuition: Countable means there is a pattern

Theorem 0: $N \times N$ *is countable*.

Proof: List all the pairs in infinite horizontal rows:

$$\begin{array}{cccc}
 & (0,0) & (0,1) & (0,2)\ldots \\
\nearrow & & & \\
 & (1,0) & (1,1) & (1,2)\ldots \\
\nearrow & & & \\
 & (2,1) & (2,2) & (2,2)\ldots \\
\nearrow & & & \\
 & & \vdots &
\end{array}$$

List along the diagonals.

Every pair will eventually appear in the list.

Rational Numbers

Theorem 0: $N \times N$ *is countable.*

Corollary 0: The rational numbers $\boldsymbol{Q}$ *are countable.*

Proof: Every rational number can be represented by a pair of natural numbers.

Theorem 1: If Σ is a finite alphabet, then Σ^* is countable.

Proof #1: Order the elements of Σ by length of the string.

$$\Sigma^* = \{\varepsilon, a, \ldots, z, aa, \ldots, zz, \ldots\}$$

Clearly we list every element in Σ^* in a finite number of steps.

Proof #2: For the binary alphabet $\Sigma = \{0,1\}$, use the correspondence $\mathbf{N} \to \Sigma^*$ given by $1x \to x$.

Examples

-- Set of All English sentences

-- Set of All Scheme programs

-- All the sets of interest in Computer Science are countable.

Theorem 2: *P(**N**) is uncountable*.

Proof: Diagonalization argument.

Theorems 3: ***R*** *is uncountable*.

Proof: Diagonalization argument on [0,1].

Diagonalization argument based on power set representation.

Remark: Notice that $\mathbf{R} \neq \Sigma^*$ *where* $\Sigma = \{0,1,\ldots,9\}$.

Corollary: There exist irrational numbers.

Theorem 2: $P(\boldsymbol{N})$ *is uncountable*.

Proof: By Contradiction. Suppose that $P(\boldsymbol{N})$ is countable.

Let $S_1, S_2, \ldots$ be a list of ALL the subsets of $\boldsymbol{N}$.

Define: $S = \{n \in N \mid n \notin S_n\}$

If $S = S_n$, then

- $n \notin S_n \Rightarrow n \notin S$ (since $S = S_n$)
- $n \notin S_n \Rightarrow n \in S$ (by definition of S)

Impossible.

Therefore $S \subseteq \boldsymbol{N}$ is not in the list, so there is no list containing all the subsets of $\boldsymbol{N}$.

*Theorems 3: **R** is uncountable.*

Proof 1: By Contradiction. Suppose that $[0,1] \subset \boldsymbol{R}$ is countable.

$$1 \leftrightarrow .d_{11}d_{12}\cdots$$

$$2 \leftrightarrow .d_{21}d_{22}\cdots$$

$$\vdots$$

$$n \leftrightarrow .d_{n1}d_{n2}\cdots d_{nn}\cdots$$

$$\vdots$$

Define: $b = b_1 b_2 \cdots b_n \cdots$, where $b_n \neq d_{nn}$ for ALL n.

Then b is not in the list!

Hence there is no list containing all the numbers in $\boldsymbol{R}$.

Theorems 3: $\boldsymbol{R}$ *is uncountable*.

Proof 2: By Construction: $[0,1] = 2^N = P(N)$, since every real number in $[0,1]$ has a representation in binary.

$$b = .b_1 b_2 \cdots b_n \cdots \leftrightarrow \textit{subset of } N$$

But $P(N)$ is uncountable, so $\boldsymbol{R}$ is uncountable.

Corollary: $R = 2^N = P(N)$

<u>Uncountable Sets</u>

Examples

- $\mathbf{R}$
- $P(\mathbf{N})$
- $B \supset A$ and A uncountable $\Rightarrow$ B countable

Tricks for Proving Uncountability

- Diagonalize
- Superset of an uncountable set
- Bijection from an uncountable set

Intuition

- Uncountable means there is no pattern

Non-Computable Functions

Theorem 4: The functions $f:\mathbf{N}\rightarrow\{0,1\}$ *are uncountable*.

Proof: $2^N = P(N)$.

Corollary 1: There exist non-computable functions.

Corollary 2: There exist subsets of the Natural Numbers that cannot be described.

Non-Computable Functions -- Revisited

Theorem 4: The functions $f : \mathbf{N} \to \{0,1\}$ *are uncountable.*

Theorem 4a: The subsets $S \subseteq \mathbf{N}$ *are uncountable.*

Corollary 1: Almost all functions on* $\mathbf{N}$ *are non-computable.*

Corollary 2: Almost all subsets of the Natural Numbers cannot be described.*

Theorem 5: The countable union of countable sets is countable.

Proof: Consider the union of $A_1, A_2, \ldots, A_k, \ldots$.

Since each set is countable, we can list their elements.

- $A_k = a_{k,1}, a_{k,2}, \ldots$

Now proceed as in the proof that $\mathbf{N} \times \mathbf{N}$ is countable

by listing a_{ij} before a_{mn} if either

- $i + j < m + n$
- $i + j = m + n$ and $i < m$.

Eventually every element in the union appears in the list.

Equivalently map $f : \mathbf{N} \times \mathbf{N} \to$ Union by setting $f(i, j) = a_{ij}$.

Consequences

Observation

- The countable product of countable sets is NOT countable because ***R*** is not countable.

Corollaries

- The set of algebraic numbers -- solutions of polynomial equations -- is countable
- There exist transcendental numbers -- numbers that are not the solutions of polynomial equations.

Another Paradox

Theorem 5

- No set is 1-1 with its power set.

Paradox

- S = Set of all sets
- $P(S)$ is larger than S
- But S is everything!

Continuum Hypothesis

Observations

$\boldsymbol{N} = \aleph_0$

$\boldsymbol{R} = 2^{\aleph_0}$

Continuum Hypothesis

$2^{\aleph_0} = \aleph_1$