W3203
Discrete Mathematics

Set Theory

Spring 2015
Instructor: Ilia Vovsha

http://www.cs.columbia.edu/~vovsha/w3203

Outline

- Sets
- Subsets, power set, Cartesian product
- Set operations, Venn diagrams
- Functions & sequences
- Binary relations
- Properties: one-to-one, onto
- Cardinality
- Infinite sets: countable, uncountable
- The Halting Problem
- Text: Rosen 2.1 – 2.5
- Text: Lehman 4, 7.1

Understanding Infinity

“All infinite sets are infinitely large, but some infinite sets are larger than others”

Sets (definition)

- Definition: a *set* is an unordered collection of objects
- Definition: the objects in a set are called *elements/members*
- Notation:
  - $\{\ \}$
  - $a \in A$
  - $a \notin A$

Sets (types)

- *Empty set:* set with no elements Ø or {}
- *Universal* set (U): set containing everything currently under consideration
- Important common sets:
  - **N** = *natural numbers* = {0,1,2,3….}
  - **Z** = *integers* = {…,-3,-2,-1,0,1,2,3,…}
  - $\mathbf{Z}^+$ = *positive integers* = {1,2,3,…..}
  - **R** = set of *real numbers*
  - $\mathbf{R}^+$ = set of *positive real numbers*
  - **C** = set of *complex numbers*.
  - **Q** = set of rational numbers

Sets (specification)

- Roster: $S = \{a,b,c,d\}$, $S = \{a,b,c,d, \ldots\ldots, z\}$
- Predicates (set builder notation):
  - $S = \{x \mid \mathrm{P}(x)\}$
  - $S = \{x \mid x \text{ is a positive integer less than } 100\}$
  - $\mathbf{Q}^{+} = \{x \in \mathbf{R} \mid x = p/q, \text{ for some positive integers } p,q\}$
- Intervals:
  - $[a,b] = \{x \mid a \leq x \leq b\}$
  - $(a,b) = \{x \mid a < x < b\}$
- Sets can be elements of other sets
- Operations on other sets
- Recursive construction

Relations on Sets

- *Subset*: set *A* is a *subset* of *B*, if and only if every element of *A* is also an element of *B*
  - $A \subseteq B$ $\qquad \forall x(x \in A \to x \in B)$
- *Equality*: two sets are *equal* if and only if they have the same elements
  - $A = B$ $\qquad \forall x(x \in A \leftrightarrow x \in B)$
- *Proper subset*: if A is a subset of B but A is not equal to B then A is a *proper subset* of B
  - $A \subset B$
    $\forall x(x \in A \to x \in B) \wedge \exists x(x \in B \wedge x \notin A)$

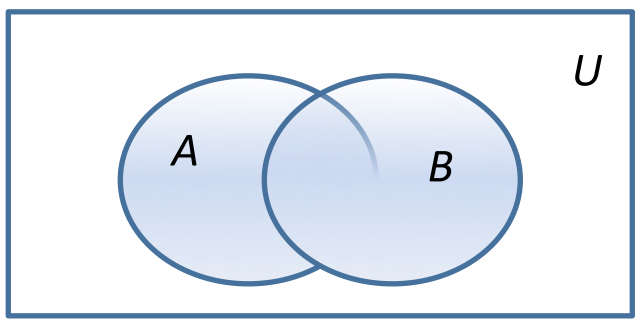
Set Operations

- *Union*: $A \cup B$ $\{x | x \in A \vee x \in B\}$
- *Intersection*: $A \cap B$ $\{x | x \in A \wedge x \in B\}$
- *Set difference*: $A - B$ $\{x \mid x \in A \wedge x \notin B\}$
- *Complement*: A^c or $\bar{A}$ $\{x \in U \mid x \notin A\}$

Union (Venn diagram)

- *Union*: $A \cup B$ $\{x | x \in A \lor x \in B\}$
- Example:

$\{1,2,3\} \cup \{3, 4, 5\} = \{1,2,3,4,5\}$

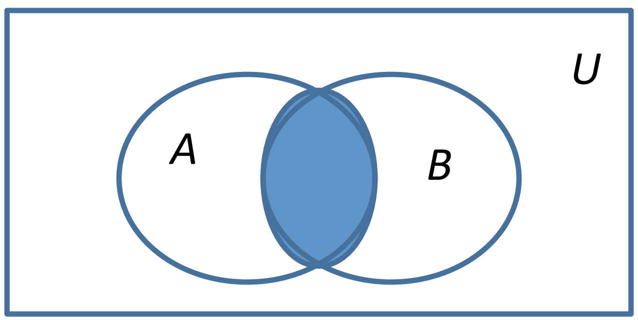


Intersection (diagram)

- *Intersection*: $A \cap B$ $\{x | x \in A \wedge x \in B\}$
- Example:

$\{1,2,3\} \cap \{3, 4, 5\} = \{3\}$

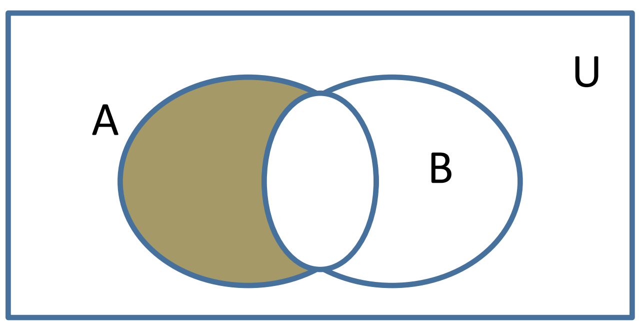
$\{1,2,3\} \cap \{4,5,6\} = \emptyset$



Set Difference (diagram)

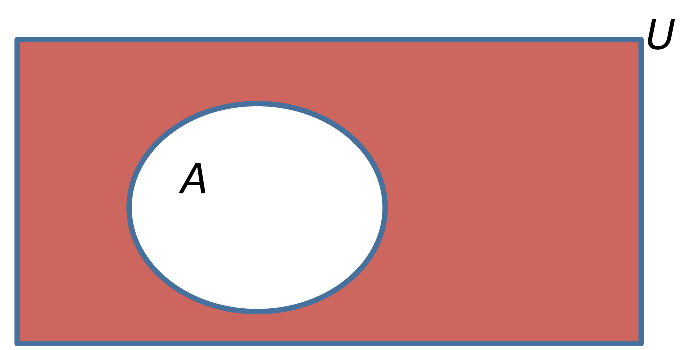
- *Set difference*: $A - B$ $\{x \mid x \in A \wedge x \notin B\}$
- $A - B$ is the set containing the elements of A that are not in B
- Example:

  $\{1,2,3\} - \{3, 4, 5\} = \{1,2\}$



Complement (diagram)

- *Complement*: A^c or $\bar{A}$ $\{x \in U \mid x \notin A\}$
- The complement of A (with respect to U) is the set $U - A$
- Example:
  - U is "positive integers less than 100"
  - A is $\{x \mid x > 70\}$
  - $\bar{A}$ is $\{x \mid x \leq 70\}$



Set Identities

- *Commutative, Associative, Distributive, De Morgan's laws*...

$$A \cup B = B \cup A$$

$$A \cup (B \cup C) = (A \cup B) \cup C$$

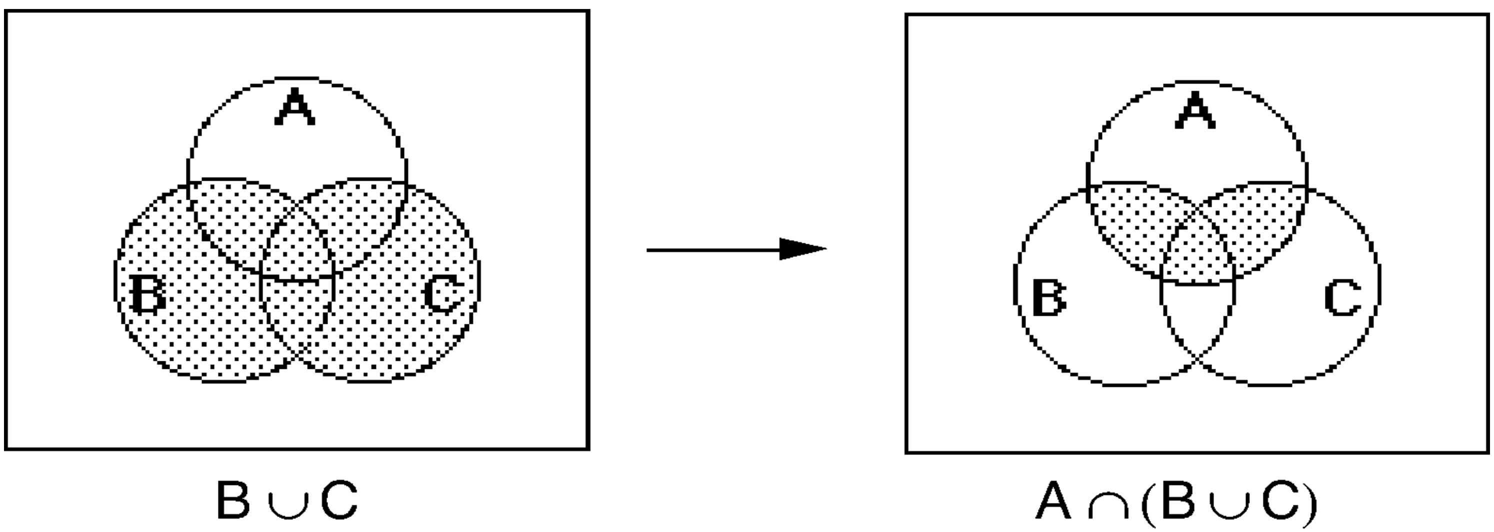
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

Set Identities (example 1)

Example 2.2.7: $\cap$ distributes over $\cup$.

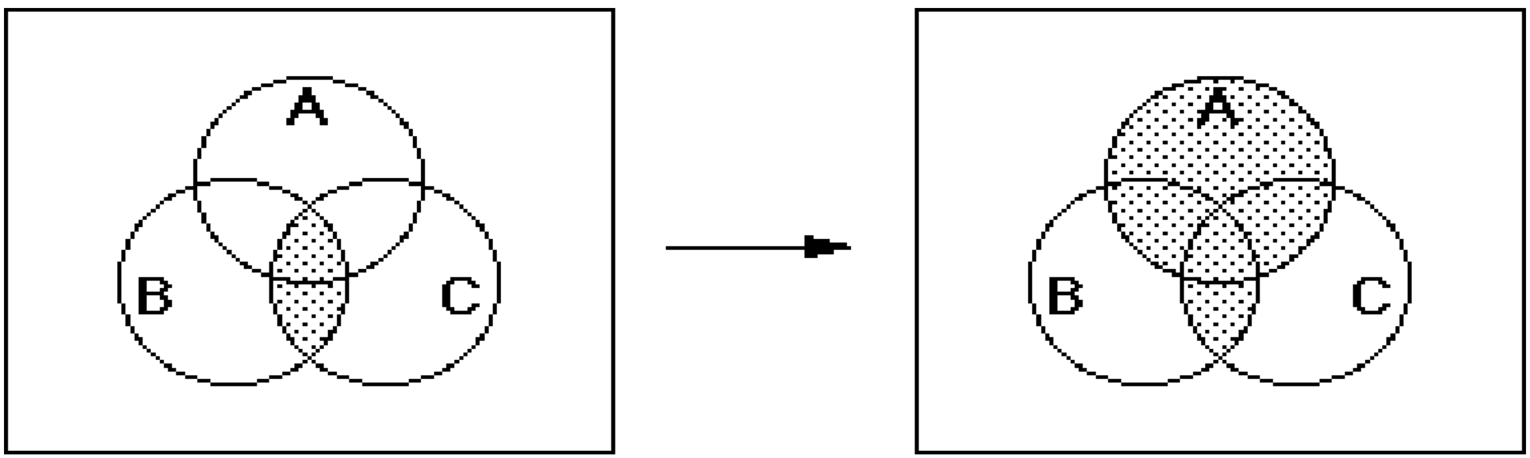
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$



Set Identities (example 2)

Example 2.2.8: $\cup$ distributes over $\cap$.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



$B \cap C$ $\quad\quad$ $A \cup (B \cap C)$

Power Set

- Recall: sets can be elements of other sets
  - $\{ \{1,2,3\}, a, \{b,c\} \}$
  - $\emptyset \neq \{ \emptyset \}$
- Power set*:* the set of all subsets of a set *A*, denoted *pow(A)* or $\mathcal{P}$(A)
  - *If A* = {a,b} then

    pow(A) = { ø, {a},{b},{a,b} }

Cardinality

- Definition: a *finite* set has exactly n (nonnegative integer) distinct elements. Otherwise it is *infinite*
- Definition: the *cardinality* of a finite set *A,* denoted by $|A|$, is the number of (distinct) elements of *A*
- Examples:
  - $|\varnothing| = 0$
  - $|\{1,2,3\}| = 3$
  - $|\{\varnothing\}| = 1$

Cartesian Product (two sets)

- Definition: the *Cartesian Product* of two sets (A × B) is the set of ordered pairs (a,b) where $a \in A$ and $b \in B$

$$A \times B = \{(a, b) | a \in A \land b \in B\}$$

- Example:
  - A = {a,b}   B = {1,2,3}
  - A × B = { (a,1),(a,2),(a,3),(b,1),(b,2),(b,3) }

Cartesian Product (n sets)

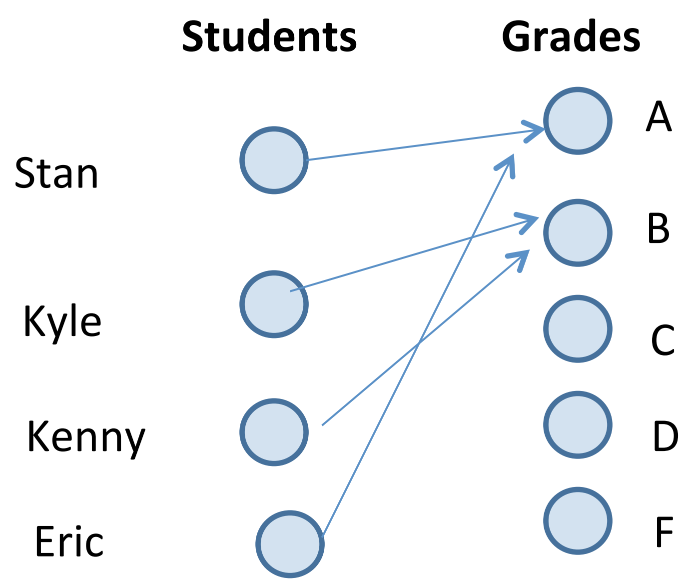
- Definition: the *Cartesian Product* of the sets ($A_1 \times A_2 \times \ldots\ldots \times A_n$) is the set of ordered n-tuples (a_1,a_2,.......,a_n) where ∀i, $a_i \in A_i$

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_i \in A_i \text{ for } i = 1, 2, \ldots n\}$$

- Example:
  - A = {0,1}   B = {0,1} C = {0,1}
  - A × B × C = { (0,0,0),(0,0,1),(0,1,0),(0,1,1),...}

Functions (definition)

- Definition: a *function* f from A to B ($f: A \rightarrow B$) is a mapping that assigns each element of set A to exactly one element of set B: $f(a) = b$



Functions (more definitions)

- We also say that $f : A \to B$ is a ***mapping*** from ***domain*** A to ***codomain*** B.
- $f(a)$ is called the ***image set of the element*** a, and the element a is called a ***preimage*** of $f(a)$.
- The set $\{a \mid f(a) = b\}$ is called the ***preimage set*** of b. NOTATION: $f^{-1}(b)$.

DEF: The set $\{b \in B \mid (\exists a \in A)[f(a) = b]\}$ is called the ***image of the function*** $f : A \to B$.

Functions (examples)

Example 2.3.1: Some functions from $\mathbb{R}$ to $\mathbb{Z}$.

(1) ***floor*** $\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}$ image $= \mathbb{Z}$

(2) ***ceiling*** $\lceil x \rceil = \min\{k \in \mathbb{Z} \mid k \geq x\}$ im $= \mathbb{Z}$

(3) ***sign*** $\sigma(x) = \begin{cases} -1 & \text{if } x < 0 \\ 0 & \text{if } x = 0 \\ +1 & x > 0 \end{cases}$

$\text{image}(\sigma) = \{-1, 0, +1\}$

The ***halting function*** maps the set of C programs to the boolean set, assigns TRUE iff this program will always halt eventually, no matter what input is supplied at run time.

Relations (definition)

- Definition: a *binary relation* R consists of two sets, A (*domain* of R), B, (*codomain* of R), and a subset of A $\times$ B called the *graph of* R
- We use "*a R b*", to mean that the pair (a,b) is in the graph of R
- Note: a function is a particular (special case) binary relation

Relations (properties)

- The relation $(\mathcal{R} : A \rightarrow B)$ is *one-to-one*, if and only if $R(a) = R(b)$ implies that $a = b$ for all a and b in the domain of f
  - There is at most one $a \in A$ such that $\mathcal{R}(a) = b$
  - **"Injection" (injective relation)**
- The relation is *onto*, IFF for every element $b \in B$, there is at least one element $a \in A$ with $R(a) = b$
  - **"Surjection" (surjective relation)**

Bijections

- Definition: a *bijection* is a *function* that is both one-to-one and onto (one-to-one correspondence)
  - **No unpaired elements**
  - **"bijective" (injective and surjective relation)**
- Definition: the *inverse* of a relation *R,* is the relation R^{-1} defined by the rule:
  - $b\ R^{-1}\ a$ *IFF* $a\ R\ b$

Showing Properties

Suppose that $f : A \to B$.

To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$ with $x \neq y$, then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

From Relations to Cardinality

- Cardinality of two sets (A & B) is equal IFF there is a bijection from A to B
  - $|A| = |B|$ IFF $\exists f : A \to B$ *(where f is a bijection)*
- Cardinality of set A is less than or equal to cardinality of set B IFF there is a one-to-one function (total, injective relation) from A to B
  - $|A| \leq |B|$ IFF $\exists f : A \to B$ *(where f is one-to-one)*

Cardinality of Power Sets

- Given a set A with n elements, what is the cardinality of the power set |P(*A)*|?
- Its a *finite* set, we can count the total number of subsets
- Another approach: establish a bijection from subsets of A to rows of a truth table with n variables (i.e. to a bit sequence)

Sequences

- Informal definition: a *sequence* is an ordered list of objects (terms)
- Definition: a *sequence* is a function from a subset of the integers {0, 1, 2,…} or {1, 2, 3…} to a set *S*
- Notation:
  - *(a,b,a)* -- *terms can repeat*
  - $(a,b,c) \neq (c,b,a)$ -- *order matters*
  - $a_n = f(n)$ -- image of integer n

Sequences (examples)

- Example: $a_n = \frac{1}{n}$ $\quad 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots$

TABLE 1 Some Useful Sequences.

nth Term	*First 10 Terms*
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, . . .
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, . . .
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, . . .
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, . . .
3^n	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, . . .
$n!$	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, . . .
f_n	1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, . . .

Infinite Sets

- How do you know that a set is infinite?
- Add an element to a set: if A is a finite set and b $\notin$ A, then $|A \cup \{b\}| = |A| + 1$.
- Not true for infinite sets! Need to find a bijection between A and A $\cup$ $\{b\}$
- Idea:
  - There is an infinite sequence $a_1, a_2, \ldots, a_n, \ldots$ of different elements of A
  - Define bijection f: A ∪ {b} → A
  - $f(b) = a_0$, $f(a_n) = a_{n+1}$

Countable Sets

- Definition: a set that is either finite or has the same cardinality as the set of positive integers ($\mathbf{Z}^+$) is called *countable*
- Definition: the cardinality of a countable, infinite set (*countably infinite*) is $\aleph_0$
  - ➢ $\aleph$ is aleph, the 1st letter of the Hebrew alphabet
  - ➢ We write $|S| = \aleph_0$
- It is possible to list the elements of a countable set in a sequence indexed by the positive integers

Integers vs. Integers

- Example: the set of positive even integers is countably infinite
- Approach: establish a bijection between $\mathbf{Z}^+$ and this set
- Solution: Let $f(x) = 2x$.

1	2	3	4	5	6	…..
↕	↕	↕	↕	↕	↕	
2	4	6	8	10	12	……

Integers vs. Rational Numbers

Theorem 2.5.2. *There are as many positive integers as rational fractions.*

$$\begin{array}{ccccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \frac{2}{6} & \cdots \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \frac{3}{6} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \frac{4}{6} & \cdots \\
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \frac{5}{6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

Pf: $$f\left(\frac{p}{q}\right) = \frac{(p+q-1)(p+q-2)}{2} + p \qquad \diamond$$

Integers vs. Real Numbers

- Example: the set of real numbers (**R**) is uncountable
- Approach: Cantor's diagonal argument (obtain a contradiction)
- Solution:

1. Suppose **R** is countable. Then the real numbers between 0 and 1 are also countable
   - Any subset of a countable set is countable
2. The real numbers between 0 and 1 can be listed in order r_1, r_2, r_3,…
3. Denote the (infinite) decimal representation of this listing

Integers vs. Real Numbers (proof)

- Solution:

1. Suppose **R** is countable. Then the real numbers between 0 and 1 are also countable
2. The real numbers between 0 and 1 can be listed in order $x_1, x_2, x_3, \ldots$
3. Let the (infinite) decimal representation be:
4. Form a new real number
5. Show it can't be on list

$$
\begin{aligned}
x_1 &= .\underline{8}841752032669031\ldots \mapsto 1\\
x_2 &= .1\underline{4}15926531424450\ldots \mapsto 2\\
x_3 &= .32\underline{0}2313932614203\ldots \mapsto 3\\
x_4 &= .167\underline{9}888138381728\ldots \mapsto 4\\
x_5 &= .0452\underline{9}98136712310\ldots \mapsto 5\\
&\vdots
\end{aligned}
$$

Cantor's Diagonal Argument

1. Suppose **R** is countable. Then the real numbers between 0 and 1 are also countable
2. The real numbers on [0,1] can be listed in order x_1 , x_2 , x_3 ,…
3. Let the (infinite) decimal representation be:
4. Form a new real number X: $0.d_1d_2d_3$...
   - $d_j = 4$ if jth digit of x_j is not 4
   - $d_j = 5$ if jth digit of x_j is 4
5. Show it can't be on list:
   - X is not equal to any of the x_1 , x_2 , x_3 ,…
   - Differs from x_j in its jth position
   - Every real number has a unique decimal expansion

$$
\begin{aligned}
x_1 &= .\underline{8}841752032669031\ldots \mapsto 1\\
x_2 &= .1\underline{4}15926531424450\ldots \mapsto 2\\
x_3 &= .32\underline{0}2313932614203\ldots \mapsto 3\\
x_4 &= .167\underline{9}888138381728\ldots \mapsto 4\\
x_5 &= .0452\underline{9}98136712310\ldots \mapsto 5\\
&\vdots
\end{aligned}
$$

Sets vs. Power Sets

- Theorem: for any set A, the cardinality of the power set $\mathcal{P}$(A) is larger
- Approach: show that you cannot construct a bijection g: A → $\mathcal{P}$(A)
- Solution:

1. Suppose a bijection 'g' has been established between elements of A ($a_1, a_2, \ldots$) and $\mathcal{P}$(A) ($B_1, B_2, \ldots$) .
2. Let X be the set of elements of A which do not belong to their "associated subsets"
   - If $a_1 \notin B_1$ then $a_1 \in X$
   - $X \in \mathcal{P}$(A)
3. Suppose that X corresponds to some element $a_i \in$ A, and derive a contradiction

The Halting Problem

- The problem is to determine, given a program and an input to the program, whether the program will eventually halt when run with that input
- Turing proved no algorithm can exist which always correctly decides whether, for a given arbitrary program and its input, the program halts when run with that input

The Halting Problem (terminology)

- *Compilation:* generating a program of low-level instructions from a program text written in some high level programming language
- Routine features of compilers involve *type-checking* to eliminate run-time errors, and optimizing the generated programs
- Call a programming procedure (compiled program)—written in your favorite programming language—a *string procedure*
- Focusing just on string procedures, the general *halting problem* is to decide, given strings s (program) and t (input), whether or not the procedure P_s halts when applied to t.
- A program that type-checks is guaranteed not to cause a run-time type-error. But since its impossible to always recognize when programs won't cause type-errors, no type-checker can be perfect