Basic Structures: Sets, Functions, Sequences, and Sums

CSC-2259 Discrete Structures

Sets

A set is an unordered collection of objects

English alphabet vowels: $V = \{a, e, i, o, u\}$

$a \in V \qquad b \notin V$

Odd positive integers less than 10:

$$O = \{1,3,5,7,9\}$$

elements of set
members of set

Other set representations

Set of positive integers less than 100:

$$\{1,2,3,\ldots,99\}$$

omitted elements

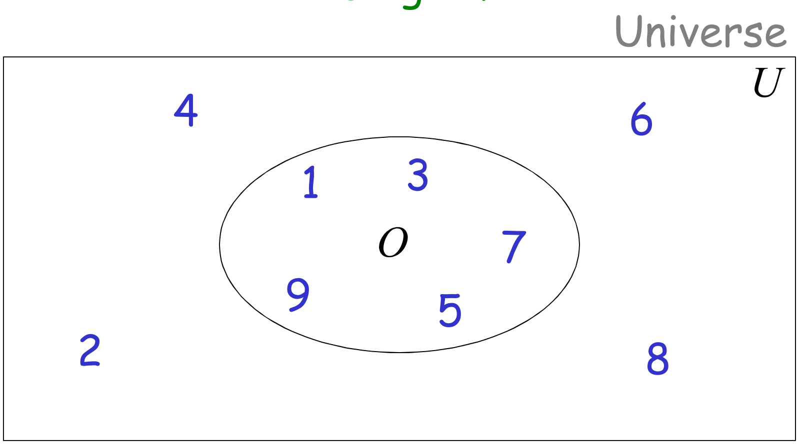
Odd positive integers less than 10:

$O = \{1,3,5,7,9\}$

$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$

$O = \{x \in Z^+ \mid x \text{ is odd and } x < 10\}$

Venn Diagram



$U = \{x \mid x \text{ is a positive integer less than } 10\}$

$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$

Useful sets

$N = \{0,1,2,3,\ldots\}$ Natural numbers

$Z = \{\ldots,-2,1,0,1,2,\ldots\}$ Integers

$Z^{+} = \{1,2,3,\ldots\}$ Positive integers

$Q = \{p/q \mid p \in Z, q \in Z, q \neq 0\}$ Rational numbers

$R = \{\text{set of Real numbers}\}$ Real numbers

Empty set

$$\varnothing = \{\}$$

$$\varnothing \neq \{\varnothing\}$$

Cardinality (size) of set

Finite sets	Number of elements
$S_1 = \{a, e, i, o, u\}$	$\vert S_1 \vert = 5$
$S_2 = \{a, b, c, \ldots, z\}$	$\vert S_2 \vert = 26$
$S_3 = \{1, 2, 3, \ldots, 99\}$	$\vert S_3 \vert = 99$

$|\varnothing| = |\{\}| = 0$ $\quad$ $|\{\varnothing\}| = 1$

Infinite set $\quad N = \{0, 1, 2, 3, \ldots\}$ $\quad$ infinite size

Equal sets

$$A = B$$

$$\forall x (x \in A \leftrightarrow x \in B)$$

Examples: $\{1,3,5\} = \{3,5,1\}$

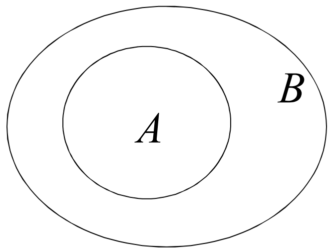
$$\{1,3,5\} = \{1,3,3,3,5,5,5,5\}$$

$$\{1,3,5,7,9\} = \{x \in Z^+ \mid x \text{ is odd and } x < 10\}$$

Subset

$$A \subseteq B$$

$$\forall x (x \in A \rightarrow x \in B)$$

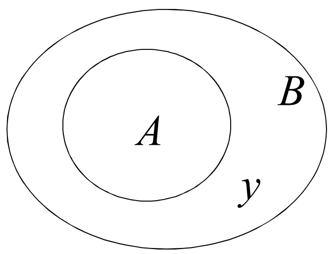


Examples: $\{1,3,5\} \subseteq \{0,1,3,5\}$ $N \subseteq Z$

For any set S**:** $S \subseteq S$ $\varnothing \subseteq S$

Proper Subset

$$A \subset B$$



$$A \subseteq B \wedge A \neq B$$

$$\forall x (x \in A \rightarrow x \in B \wedge \exists y (y \in B \wedge y \notin A))$$

Examples: $\{1,3,5\} \subset \{0,1,3,5\}$ $N \subset Z$

$$A = B$$

is equivalent to

$$A \subseteq B \quad \wedge \quad B \subseteq A$$

Power set

The power set of S contains all possible subsets of S (and the empty set)

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

Power set

$$P(S) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

$$\underbrace{|P(S)|}_{\text{Size of power set}} = 2^{|S|} = 2^3 = 8$$

Size of power set

Special cases

$$P(\varnothing) = \{\varnothing\}$$

$$P(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$$

Ordered tuples (relations)

Ordered n-tuple $(a_1, a_2, \ldots, a_n)$

ordered list of elements

$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ iff $\forall i(a_i = b_i)$

Example: $(1,2) \neq (2,1)$

Cartesian product

Cartesian product of two sets A, B

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

Example: $A = \{1,2\}$ $B = \{a,b,c\}$

$$A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$$

$$B \times A = \{(a,1),(b,1),(c,1),(a,2),(b,2),(c,2)\}$$

For this case: $A \times B \neq B \times A$

Size: $|A \times B| = |A| \times |B| = 2 \times 3 = 6$

Cartesian product of sets $A_1, A_2, \ldots, A_n$

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\}$$

Example: $A = \{1,2\}$ $B = \{a,b,c\}$ $C = \{x,y\}$

$$A \times B \times C = \{(1,a,x),(1,b,x),(1,c,x),(2,a,x),(2,b,x),(2,c,x),$$
$$(1,a,y),(1,b,y),(1,c,y),(2,a,y),(2,b,y),(2,c,y)\}$$

Size: $|A \times B \times C| = |A| \times |B| \times |C| = 2 \times 3 \times 2 = 12$

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \times |A_2| \times \cdots \times |A_n|$$

Sets and propositions

$\forall x \in S(P(x))$ shorthand for $\forall x(x \in S \rightarrow P(x))$

$\exists x \in S(P(x))$ shorthand for $\exists x(x \in S \land P(x))$

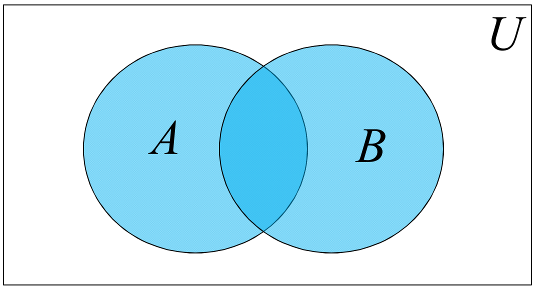
Truth set of proposition $P(x)$

$$\{x \in \text{Domain} \mid P(x)\}$$

all elements of the domain which satisfy $P(x)$

Set operations

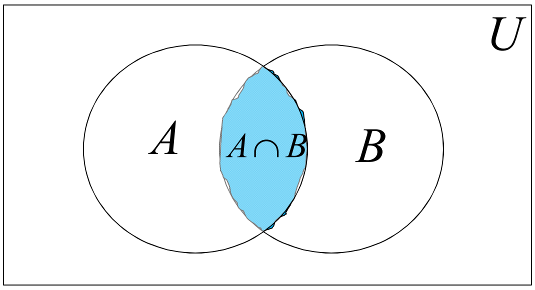
Union $A \cup B = \{x \mid x \in A \vee x \in B\}$



$A = \{1,3,5\}$ $B = \{1,2,3\}$ $A \cup B = \{1,2,3,5\}$

Intersection

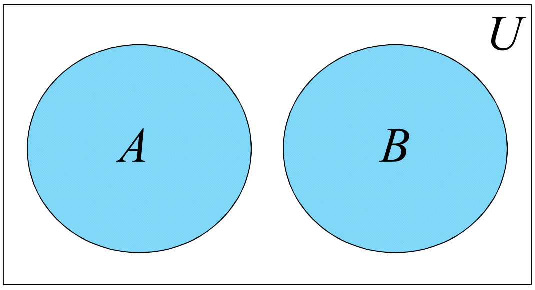
$A \cap B = \{x \mid x \in A \wedge x \in B\}$



$A = \{1,3,5\}$ $B = \{1,2,3\}$ $A \cap B = \{1,3\}$

Disjoint sets A, B

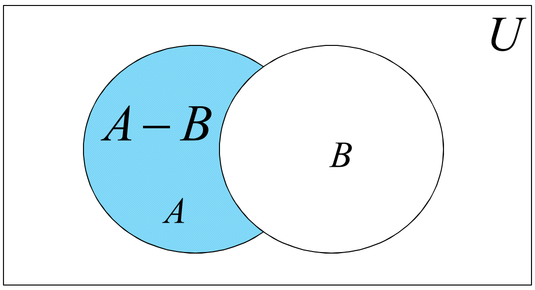
$$A \cap B = \varnothing$$



$A = \{1,3,5\}$ $B = \{2,9\}$ $A \cap B = \varnothing$

Set difference

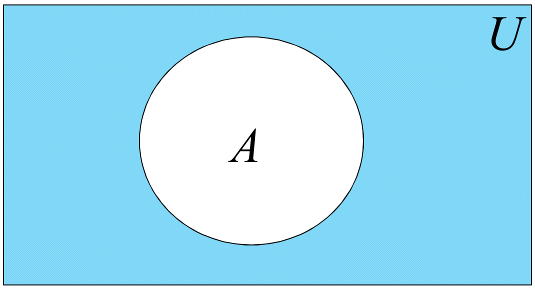
$$A - B = \{x \mid x \in A \wedge x \notin B\}$$



$A = \{1,3,5\}$ $B = \{1,2,3\}$ $A - B = \{5\}$

Complement

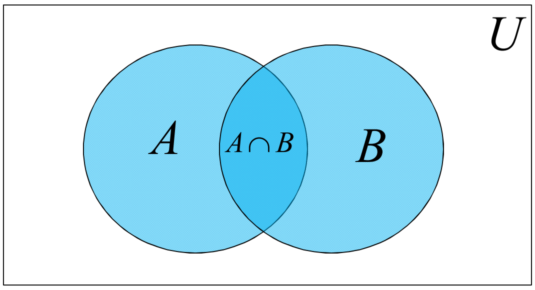
$$\overline{A} = \{x \mid x \notin A\}$$



$A = \{1,3,5\}$ $U = \{1,2,3,4,5\}$ $\overline{A} = \{2,4\}$

Size of union

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



$A = \{1,3,5\}$ $B = \{1,2,3\}$ $A \cup B = \{1,2,3,5\}$ $A \cap B = \{1,3\}$

$$|A \cup B| = |A| + |B| - |A \cap B| = 3 + 3 - 2 = 4$$

De Morgan's laws

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

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

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

Proof: Show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

Part 1: $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$

$x \in \overline{A \cap B}$

$\rightarrow x \notin A \cap B \rightarrow \neg(x \in A \cap B)$ De Morgan's law from logic

$\rightarrow \neg((x \in A) \wedge (x \in B)) \rightarrow \neg(x \in A) \vee \neg(x \in B)$

$\rightarrow (x \notin A) \vee (x \notin B) \rightarrow (x \in \overline{A}) \vee (x \in \overline{B})$

$\rightarrow x \in (\overline{A} \cup \overline{B})$

Part 2: $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

$$x \in (\overline{A} \cup \overline{B})$$
$$\rightarrow (x \in \overline{A}) \vee (x \in \overline{B}) \rightarrow (x \notin A) \vee (x \notin B)$$
$$\rightarrow \neg(x \in A) \vee \neg(x \in B) \rightarrow \neg((x \in A) \wedge (x \in B))$$
$$\rightarrow \neg(x \in A \cap B)$$

De Morgan's law from logic

$$\rightarrow x \in \overline{A \cap B}$$

End of Proof

Set identities

Identity laws

$A \cup \varnothing = A$

$A \cap U = A$

Domination laws

$A \cup U = U$

$A \cap \varnothing = \varnothing$

Idempotent laws

$A \cup A = A$

$A \cap A = A$

Complementation law

$\overline{\overline{A}} = A$

Complement laws

$A \cup \overline{A} = U$

$A \cap \overline{A} = \varnothing$

De Morgan's laws

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

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

Commutative laws

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

$$A \cap B = B \cap A$$

Associative laws

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

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

Absorption laws

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

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

Distributive laws

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

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

Generalized unions and intersections

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

Example: $A_i = \{i, i+1, i+2, \ldots\}$

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i+1, i+2, \ldots\} = A_1 = \{1,2,3,\ldots\}$$

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, i+2, \ldots\} = A_n = \{n, n+1, n+2, \ldots\}$$

Konstantin Busch - LSU 29

Computer representation of sets

Represent sets as binary strings

$$U = \{1,2,3,4,5,6,7,8,9,10\}$$

$A = \{1,3,5,7,9\}$ 1010101010

$B = \{2,4,6,8,10\}$ 0101010101

Konstantin Busch - LSU 30

Set operations become binary string operations

$A = \{1,2,3,4,5\}$	1111100000
$B = \{1,3,5,7,9\}$	1010101010
$A \cup B = \{1,2,3,4,5,7,9\}$	1111101010 Bitwise OR
$A \cap B = \{1,3,5\}$	1010100000 Bitwise AND

Powerset $P(S)$ of $S = \underbrace{\{a_1, a_2, a_3, \ldots, a_{n-1}, a_n\}}_{n \text{ elements}}$

$P(S)$ — n bits

$\emptyset$: 0000000000

$\{a_1\}$: 1000000000

$\{a_2\}$: 0100000000

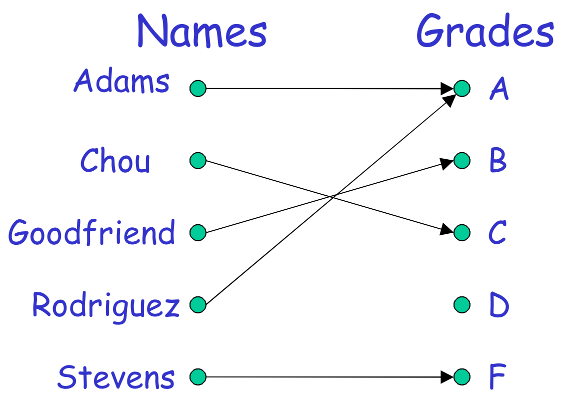
$\vdots$

S : 1111111111

2^n combinations

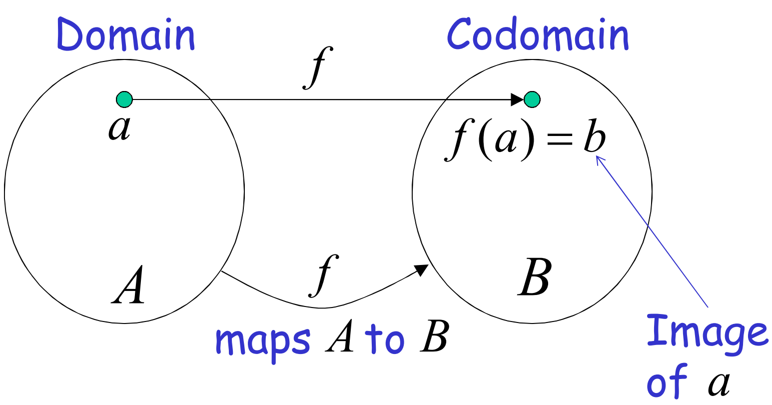
$$|P(S)| = 2^n = 2^{|S|}$$

Functions

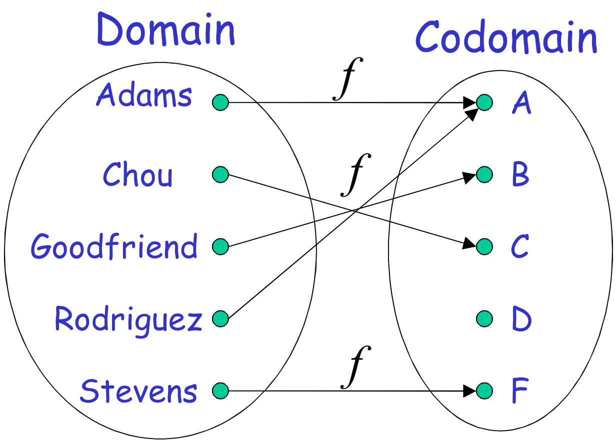


$f(\text{Chou}) = C$ $\qquad$ $f(\text{Rodriguez}) = A$

$f : A \rightarrow B$



Every element of domain
has exactly one image



$\text{Domain} = \{\text{Adams}, \text{Chou}, \text{Goodfriend}, \text{Rodriguez}, \text{Stevens}\}$

$\text{Codomain} = \{A, B, C, D, F\}$

$\text{Range} = \{A, B, C, F\}$ set of all images

$$f : Z \rightarrow Z$$

$$f(x) = x^2$$

$\text{Domain} = Z$

$\text{Codomain} = Z$

$\text{Range} = \{0, 1, 4, 9, \ldots\}$

Equal functions

$f : A \to B$ $g : C \to D$

$$f = g$$

$A = B$ same domain

$B = D$ same codomain

$\forall x \in A, f(x) = g(x)$ same mapping

In some programming languages,
domain and codomain are explicitly defined

```
int f(int a) {
    return a*a;
}
```

Add and multiply functions

Real numbers

$f_1 : A \to R$ $\quad (f_1 + f_2)(x) = f_1(x) + f_2(x)$

$f_2 : A \to R$ $\quad (f_1 f_2)(x) = f_1(x) f_2(x)$

Example: $f_1(x) = x^2$ $\quad f_2(x) = x - x^2$

$$(f_1 + f_2)(x) = f_1(x) + f_2(x) = x^2 + (x - x^2) = x$$

$$(f_1 f_2)(x) = f_1(x) f_2(x) = x^2 (x - x^2) = x^3 - x^4$$

Image of set

Set S

$$f(S) = \{t \mid \exists x \in S (t = f(x))\}$$
$$= \{f(x) \mid x \in S\}$$

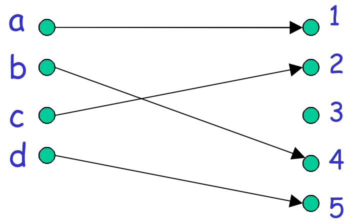
Example: $f(x) = x^2$

$$f(\{1,2,3\}) = \{1,4,9\}$$

One-to-one (injection) function

For every x, y in domain

$f(x) = f(y)$ implies $x = y$



Each element of range is image of one element of domain

Examples: $f(x) = x + 1$ is one-to-one

$g(x) = x^2$ is not one-to-one: $g(-1) = g(1) = 1$

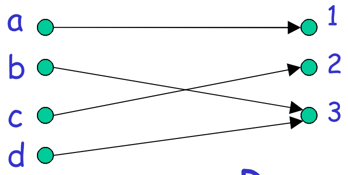
Increasing function: $x < y \rightarrow f(x) \leq f(y)$

Strictly increasing: $x < y \rightarrow f(x) < f(y)$

Strictly increasing functions are one-to-one

Onto (surjection) function $f : A \to B$

For every $y \in B$ there is $x \in B$ such that $f(x) = y$



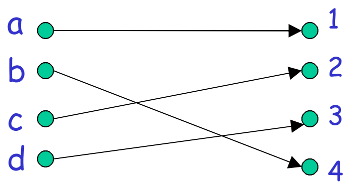
Range = Codomain

Examples: $f(x) = x + 1$ is onto

$g(x) = x^2$ is not onto: $\forall x \in Z, g(x) \neq -1$

One-to-one correspondence (bijection) function

a function which is one-to-one and onto

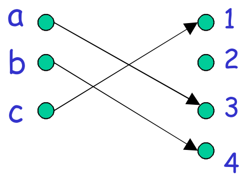


Examples: $f(x) = x + 1$ is bijection

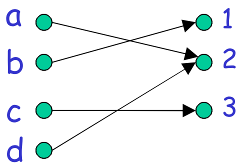
$g(x) = x^2$ is not bijection

Identity function $\iota_A(x) = x$ is bijection

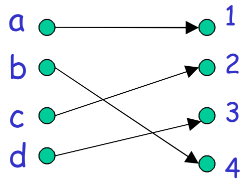
one-to-one
not onto



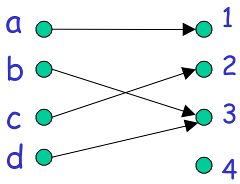
not one-to-one
onto



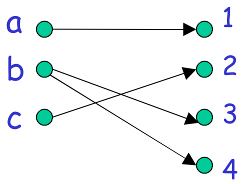
one-to-one
onto



not one-to-one
not onto

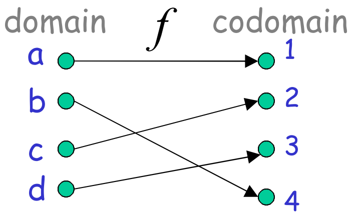


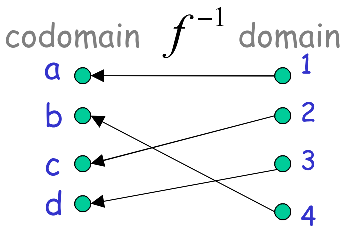
not a function



Inverse f^{-1} of a bijection function f

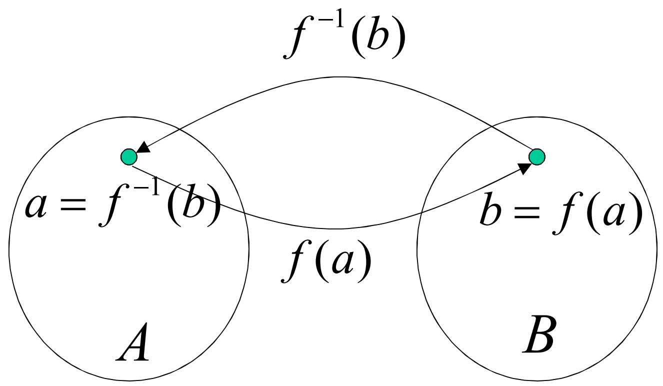
$f^{-1}(y) = x$ when $f(x) = y$





f is invertible function

Example: $f(x) = x + 1$ $\qquad f^{-1}(y) = y - 1$



Composition of functions

$f : B \to C$

$g : A \to B$

$$f \circ g : A \to C$$

$$(f \circ g)(x) = f(g(x))$$

Example: $f(x) = 2x \qquad g(x) = x^2$

$$(f \circ g)(x) = f(g(x)) = f(x^2) = 2x^2$$

$$(g \circ f)(x) = g(f(x)) = g(2x) = (2x)^2 = 4x^2$$

identity function

$$f \circ f^{-1} = f^{-1} \circ f = i$$

Suppose $f(x) = y$

$$(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y$$

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x$$

Floor and Ceiling

Let x be real

Floor function: $\lfloor x \rfloor$ largest integer less or equal to x

Ceiling function: $\lceil x \rceil$ smallest integer greater or equal to x

Examples: $\left\lfloor \frac{1}{2} \right\rfloor = 0$ $\left\lceil \frac{1}{2} \right\rceil = 1$ $\lfloor -3.1 \rfloor = -4$ $\lceil -3.1 \rceil = -3$

Factorial function

$f : N \to Z^+$ $\quad f(n) = n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$

$f(0) = 0! = 1$

$1! = 1 \qquad 2! = 1 \cdot 2 = 2 \qquad 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 760$

$20! = 1 \cdot 2 \cdot 3 \cdots 19 \cdot 20 = 2{,}432{,}902{,}008{,}176{,}640{,}000$

Stirling's formula: $n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$

Sequences

Sequence: function from a subset of integers to a set S

Finite sequence

2, 4, 6, 8, 10

a_1, a_2, a_3, a_4, a_5

$f(n) = a_n$

$f(1) = a_1 = 2$

$f(5) = a_5 = 10$

Infinite sequence

1,3,9,27,81,...

Alternate representation

$a_n = 3^k, \quad k \geq 0$

$\{a_n\} = a_1, a_2, a_3, a_4, a_5, \ldots$

$= 1,3,9,27,81, \ldots$

finite sequence: $a_1, a_2, \ldots, a_n$

String: $a_1 a_2 a_3 \cdots a_n$

all elements of sequence concatenated

Length of string: $|a_1 a_2 \cdots a_n| = n$

Empty string (null): λ $|\lambda| = 0$

Arithmetic progression

$$a, a+d, a+2d, \ldots, a+nd, \ldots$$

Initial term a

Common difference d

Example: $\{s_n\} = -1 + 4n$ start with $n = 0$

$$-1, 3, 7, 11, \ldots$$

Geometric progression

$$a, ar, ar^2, \ldots, ar^n, \ldots$$

Initial term a

Common ratio r

Example: $\{c_n\} = 2 \cdot 5^n$ start with $n = 0$

$$2, 10, 50, 250, 1250, \ldots$$

Summations

Sequence: $a_m, a_{m+1}, a_{m+2}, \ldots, a_n$

Sum: $a_m + a_{m+1} + a_{m+2} + \cdots + a_n = \sum_{i=m}^{n} a_i$

Example: $\sum_{i=1}^{5} i^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55$

Theorem: $$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Proof:

$$\begin{array}{lccccccc}
\{a_n\} = & 1 & 2 & 3 & 4 & \cdots & n-1 & n \\
\{b_n\} = & n & n-1 & n-2 & n-3 & \cdots & 2 & 1 \\
\{c_n\} = & n+1 & n+1 & n+1 & n+1 & \cdots & n+1 & n+1
\end{array}$$

$$S = \sum_{i=1}^{n} i = \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$$

$$n(n+1) = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = 2S$$

$$\Rightarrow \quad S = \frac{n(n+1)}{2}$$

End of Proof

Theorem: If a, r are real numbers and $r \notin \{0,1\}$, then

$$\sum_{i=0}^{n} ar^i = \frac{ar^{n+1} - a}{r-1}$$

Proof: Let $S = \sum_{i=0}^{n} ar^i$

$$rS = r\sum_{i=0}^{n} ar^i = \sum_{i=0}^{n} ar^{i+1} = \sum_{k=1}^{n+1} ar^k = \left(\sum_{k=0}^{n} ar^k\right) + (ar^{n+1} - a) = S + (ar^{n+1} - a)$$

$$\Rightarrow rS = S + (ar^{n+1} - a)$$

$$\Downarrow$$

$$S = \frac{ar^{n+1} - a}{r - 1}$$

End of Proof

Useful Summation Formulas

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=0}^{n} ar^i = \frac{ar^{n+1} - a}{r - 1}, \quad r \notin \{0,1\}$$

$$\sum_{i=0}^{\infty} x^i = \frac{1}{1 - x}, \quad |x| < 1$$

Countable Sets

Countable finite set:

Any finite set is countable by default

Countable infinite set:

An infinite set S is countable if there is a one-to-one correspondence from S to Z^+

Positive integers

Theorem: Even positive integers are countable

Proof:

Even positive integers: $2, 4, 6, 8, \ldots$

One-to-one Correspondence: $\updownarrow$

Positive integers: $1, 2, 3, 4, \ldots$

n corresponds to $2n$

End of Proof

Theorem: The set of rational numbers is countable

Proof:

We need to find a method to list

all rational numbers: $\frac{1}{2}, \frac{3}{4}, \frac{7}{8}, \ldots$

Naïve Approach Start with nominator=1

Rational numbers: $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots$

One-to-one correspondence: $\updownarrow \quad \updownarrow \quad \updownarrow$

Positive integers: $1, \; 2, \; 3, \; \ldots$

Doesn't work:

we will never list numbers with nominator 2: $\frac{2}{1}, \frac{2}{2}, \frac{2}{3}, \ldots$

Better Approach: scan diagonals

Nomin.=1 $\frac{1}{1}$ $\frac{1}{2}$ $\frac{1}{3}$ $\frac{1}{4}$ $\cdots$

Nomin.=2 $\frac{2}{1}$ $\frac{2}{2}$ $\frac{2}{3}$ $\cdots$

Nomin.=3 $\frac{3}{1}$ $\frac{3}{2}$ $\cdots$

Nomin.=4 $\frac{4}{1}$ $\cdots$

first diagonal

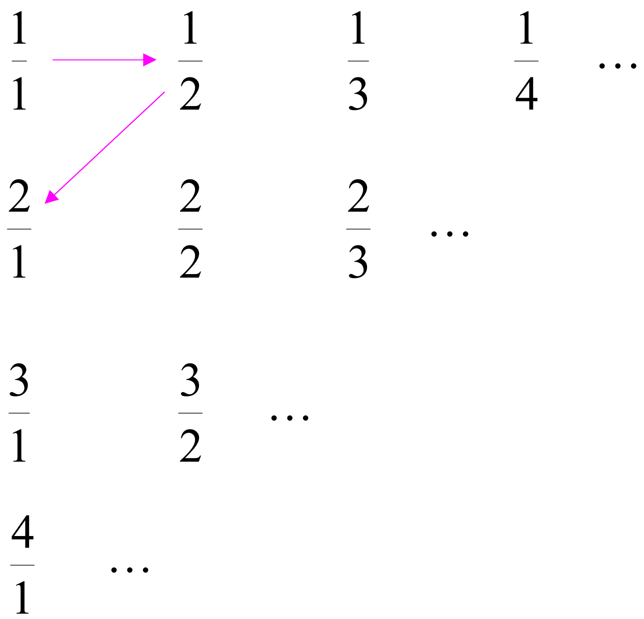
$\frac{1}{1}$ $\frac{1}{2}$ $\frac{1}{3}$ $\frac{1}{4}$ $\cdots$

$\frac{2}{1}$ $\frac{2}{2}$ $\frac{2}{3}$ $\cdots$

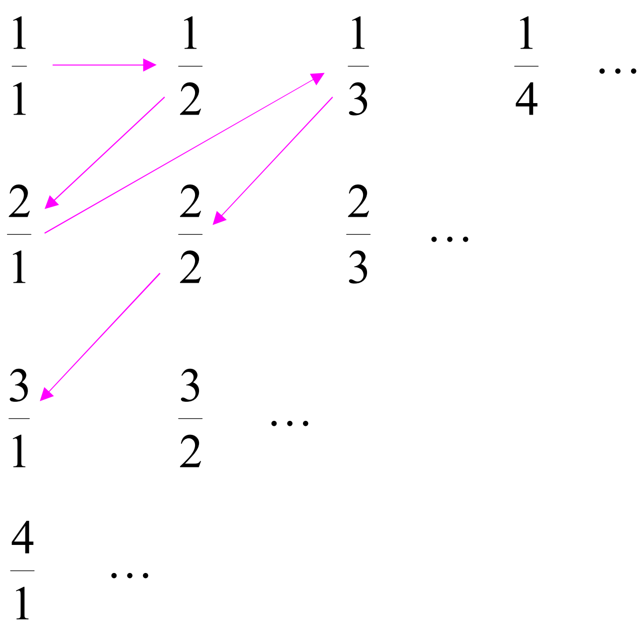
$\frac{3}{1}$ $\frac{3}{2}$ $\cdots$

$\frac{4}{1}$ $\cdots$

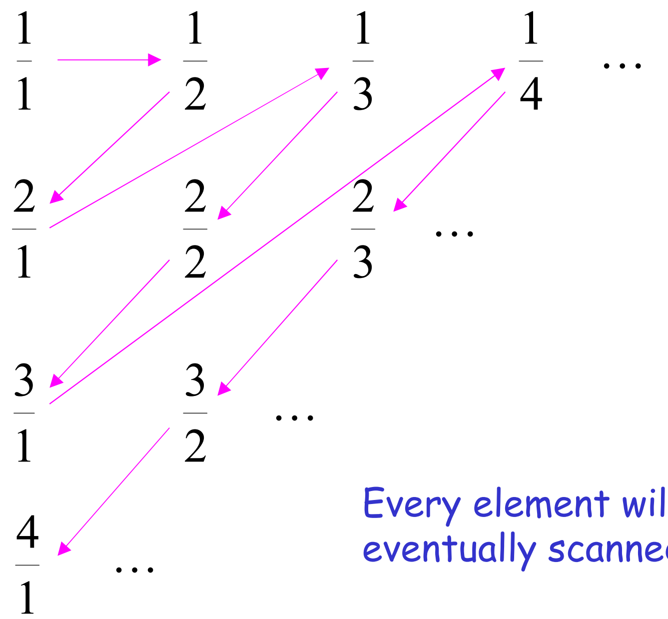
second diagonal



third diagonal



fourth diagonal...



Every element will be eventually scanned

Diagonal listing

Rational Numbers: $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{2}, \ldots$

One-to-one correspondence: $\updownarrow$

Positive Integers: $1, 2, 3, 4, 5, \ldots$

End of Proof

Theorem: Set $S = (0,1) \subseteq R$ is uncountable

Proof: Assume that S is countable,

then we can list its elements

$$S = \{s_1, s_2, s_3, \ldots\}$$

Elements of S

List the elements of $S = (0,1)$

s_1	=	0	.	0	1	4	5	2	9	4	2	1	6	$\cdots$
s_2	=	0	.	1	2	1	3	2	1	5	7	3	1	$\cdots$
s_3	=	0	.	1	3	0	2	0	5	3	1	8	4	$\cdots$
s_4	=	0	.	3	2	1	0	0	3	2	1	1	3	$\cdots$
s_5	=	0	.	4	6	1	8	4	2	1	5	2	1	$\cdots$
$\vdots$														

$$\begin{array}{lllllllllllllll} s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\ s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\ s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\ s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\ s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\ \vdots \end{array}$$

Create new element based on diagonal

$$t = 0 \,.\, x_1 \; x_2 \; x_3 \; x_4 \; x_5 \; x_6 \; x_7 \; x_8 \; x_9 \; x_{10} \; \cdots$$

$$\begin{array}{lllllllllllllll} s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\ s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\ s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\ s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\ s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\ \vdots \end{array}$$

If diagonal element is 0 then set digit to 1

$$t = 0 \,.\, 1 \; x_2 \; x_3 \; x_4 \; x_5 \; x_6 \; x_7 \; x_8 \; x_9 \; x_{10} \; \cdots$$

$$
\begin{array}{llllllllllllll}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

If diagonal element is not 0 then set digit to 0

$$t = 0 . 1 \; 0 \; x_3 \; x_4 \; x_5 \; x_6 \; x_7 \; x_8 \; x_9 \; x_{10} \cdots$$

$$
\begin{array}{llllllllllllll}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

If diagonal element is 0 then set digit to 1

$$t = 0 . 1 \; 0 \; 1 \; x_4 \; x_5 \; x_6 \; x_7 \; x_8 \; x_9 \; x_{10} \cdots$$

$$
\begin{array}{lcccccccccccccc}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & \textcircled{0} & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

If diagonal element is 0 then set digit to 1

$$t = 0 \,.\, 1 \; 0 \; 1 \; \textcircled{1} \; x_5 \; x_6 \; x_7 \; x_8 \; x_9 \; x_{10} \; \cdots$$

$$
\begin{array}{lcccccccccccccc}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & \textcircled{4} & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

If diagonal element is not 0 then set digit to 0

$$t = 0 \,.\, 1 \; 0 \; 1 \; 1 \; \textcircled{0} \; x_6 \; x_7 \; x_8 \; x_9 \; x_{10} \; \cdots$$

$$
\begin{array}{lllllllllllllll}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

By repeating process we obtain new number

$$t = 0 . 1\ 0\ 1\ 1\ 0\ 1 \cdots \in (0,1)$$

$$
\begin{array}{lllllllllllllll}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

Observation: $t \neq s_1$ (differ on first digit)

$$t = 0 . 1\ 0\ 1\ 1\ 0\ 1 \cdots$$

$$
\begin{array}{lllllllllllllll}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

Observation: $t \neq s_2$ (differ on second digit)

$$t = 0 \;.\; 1 \; 0 \; 1 \; 1 \; 0 \; 1 \; \cdots$$

$$
\begin{array}{lllllllllllllll}
s_1 & = & 0 & . & 0 & 1 & 4 & 5 & 2 & 9 & 4 & 2 & 1 & 6 & \cdots \\
s_2 & = & 0 & . & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 7 & 3 & 1 & \cdots \\
s_3 & = & 0 & . & 1 & 3 & 0 & 2 & 0 & 5 & 3 & 1 & 8 & 4 & \cdots \\
s_4 & = & 0 & . & 3 & 2 & 1 & 0 & 0 & 3 & 2 & 1 & 1 & 3 & \cdots \\
s_5 & = & 0 & . & 4 & 6 & 1 & 8 & 4 & 2 & 1 & 5 & 2 & 1 & \cdots \\
\vdots
\end{array}
$$

Observation: $t \neq s_3$ (differ on third digit)

$$t = 0 \;.\; 1 \; 0 \; 1 \; 1 \; 0 \; 1 \; \cdots$$

Observation: $t \neq s_i$ (differ on i digit)
for every i

↓

$$t \notin S = \{s_1, s_2, \ldots\} = (0,1)$$

Contradiction!

$$t = 0 \;.\; 1 \;\; 0 \;\; 1 \;\; 1 \;\; 0 \;\; 1 \;\; \cdots \in (0,1)$$

End of Proof

We have proven: $(0,1) \subseteq R$ is uncountable

It can be proven: Every subset of a countable set is countable

↓

It follows that the set of real numbers R is uncountable

The previous proof technique is known as:

Cantor diagonalization argument

The same technique can
be used in other proofs

Theorem: If S is an infinite countable set, then the power set $P(S)$ is uncountable

Proof:

Since S is countable, we can list its elements

$$S = \{s_1, s_2, s_3, \ldots\}$$

Elements of S

Elements of the power set $P(S)$ have the form:

$$\emptyset$$

$$\{s_1\}$$

$$\{s_1, s_3\}$$

$$\{s_1, s_3, s_4\}$$

$$\{s_5, s_7, s_9, s_{10}\}$$

$$\vdots$$

We encode each element of the powerset with a binary string of 0's and 1's

Powerset elements $P(S)$ (in arbitrary order)	Binary encoding s_1	s_2	s_3	s_4	$\cdots$
$\{s_1\}$	1	0	0	0	$\cdots$
$\{s_2, s_3\}$	0	1	1	0	$\cdots$
$\{s_1, s_3, s_4\}$	1	0	1	1	$\cdots$

Observation:
Every infinite binary string corresponds to an element of the power set

Example: $1 0 0 1 1 1 0 \cdots$

Corresponds to: $\{s_1, s_4, s_5, s_6, \ldots\} \in P(S)$

Let's assume (for contradiction) that the power set $P(S)$ is countable

Then: we can enumerate the elements of the powerset

$$P(S) = \{t_1, t_2, t_3, \ldots\}$$

Power set element $P(S)$	suppose that this is the respective **Binary encoding**					
t_1	1	0	0	0	0	$\cdots$
t_2	1	1	0	0	0	$\cdots$
t_3	1	1	0	1	0	$\cdots$
t_4	1	1	0	0	1	$\cdots$
$\vdots$	$\vdots$					

Take the binary string whose bits are the complement of the diagonal

t_1	(1)	0	0	0	0	$\cdots$
t_2	1	(1)	0	0	0	$\cdots$
t_3	1	1	(0)	1	0	$\cdots$
t_4	1	1	0	(0)	1	$\cdots$
Complement of diagonal	0	0	1	1		$\cdots$

Binary string: $t = 0011 \cdots$

The binary string $t = 0011 \cdots$

corresponds
to an element of
the power set $P(S)$: $t = \{s_3, s_4, \ldots\} \in P(S)$

Thus, t must be equal to some t_i: $t = t_i$

$$t \in P(S)$$

However,

the i-th bit in the binary string of t is different than the i-th bit of t_i, thus: $t \neq t_i$

$$t \notin P(S) = \{t_1, t_2, \ldots, t_n\}$$

Contradiction!!!

End of Proof