Symbolic Logic

Def: *proposition* - statement either true (T) or false (F)

Ex: $1 + 1 = 2$

$2 + 2 = 3$

$3 < 7$

$x + 4 = 5$

"today is Monday"

Boolean Functions

- “and” $\wedge$
- “or” $\vee$
- “not” $\neg$
- “xor” $\oplus$
- “nand”
- “nor”
- “implication” $\Rightarrow$
- “equivalence” $\Leftrightarrow$

- “<u>not</u>” $\neg$

  “negation”

Truth table:

p	$\neg p$
T	F
F	T

Ex: let p=“today is Monday”

$\neg$p =“today is not Monday”

- “<u>and</u>” $\wedge$

  “conjunction”

Truth table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Ex: $x \geq 0 \wedge x \leq 10$

$(x \geq 0) \wedge (x \leq 10)$

- “<u>or</u>” $\vee$

  “disjunction”

Truth table:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Ex: $(x \geq 7) \vee (x=3)$

$(x=0) \vee (y=0)$

- “<u>xor</u>” $\oplus$

  “exclusive or”

Truth table:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Ex: $(x=0) \oplus (y=0)$

“it is midnight” $\oplus$ “it is sunny”

Logical Implication

- "implies" $\Rightarrow$

Truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Ex: $(x \le 0) \wedge (x \ge 0) \Rightarrow (x = 0)$

$1 < x < y \Rightarrow x^3 < y^3$

"today is Sunday" $\Rightarrow 1+1=3$

Other interpretations of $p \Rightarrow q$:

- “p implies q”
- “if p, then q”
- “p is sufficient for q”
- “q if p”
- “q whenever p”
- “q is necessary for p”

Logical Equivalence

- “biconditional” $\Leftrightarrow$

  or “if and only if” (“iff”)
  or “necessary and sufficient”
  or “logically equivalent” $\equiv$

Truth table:

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Ex: $p \Leftrightarrow p$

$$[(x=0) \vee (y=0)] \Leftrightarrow (xy=0)$$

$$\min(x,y)=\max(x,y) \Leftrightarrow x=y$$

logically equivalent ($\Leftrightarrow$) - means "has same truth table"

Ex: $p \Rightarrow q$ is equivalent to $(\neg p) \vee q$

i.e., $p \Rightarrow q \Leftrightarrow (\neg p) \vee q$

p	q	$p \Rightarrow q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Ex: $(p \Leftrightarrow q) \equiv [(p \Rightarrow q) \wedge (q \Rightarrow p)]$

$p \Leftrightarrow q \equiv p \Rightarrow q \wedge q \Rightarrow p$

$(p \Leftrightarrow q) \equiv [(\neg p \vee q) \wedge (\neg q \vee p)]$

Note: $p \Rightarrow q$ is <u>not</u> equivalent to $q \Rightarrow p$

Thm: $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$

Q: What is the negation of $p \Rightarrow q$?

A: $\neg(p \Rightarrow q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$

p	q	$\neg q$	$p \Rightarrow q$	$\neg(p \Rightarrow q)$	$p \wedge \neg q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

"Logic is in the eye of the logician."
- Gloria Steinem

Example

let p = “it is raining”
let q = “the ground is wet”

$p \Rightarrow q$: “if it is raining,
then the ground is wet”

$\neg q \Rightarrow \neg p$: “if the ground is not wet,
then it is not raining”

$q \Rightarrow p$: “if the ground is wet,
then it is raining”

$\neg(p \Rightarrow q)$: “it is raining, and
the ground is not wet”

Order of Operations

- negation first
- or/and next
- implications last
- parenthesis override others

(similar to arithmetic)

Def: *converse* of $p \Rightarrow q$ is $q \Rightarrow p$
contrapositive of $p \Rightarrow q$ is $\neg q \Rightarrow \neg p$

Prove: $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

Q: How many distinct 2-variable Boolean functions are there?

Bit Operations

$\neg$	
0	1
1	0

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Bit Strings

Def: *bit string* - sequence of bits

Boolean functions extend to bit strings (bitwise)

Ex: $\neg\, 0100 = 1011$

$0100 \wedge 1110 = 0100$

$0100 \vee 1110 = 1110$

$0100 \oplus 1110 = 1010$

$0100 \Rightarrow 1110 = 1111$

$0100 \Leftrightarrow 1110 = 0101$

Proposition types

Def: *tautology:* always true
contingency: sometimes true
contradiction: never true

Ex: $p \vee \neg p$ is a tautology

$p \wedge \neg p$ is a contradiction

$p \Rightarrow \neg p$ is a contingency

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$	$p \Rightarrow \neg p$
T	F	T	F	F
F	T	T	F	T

Logic Laws

Identity:

$$p \wedge T \Leftrightarrow p$$

$$p \vee F \Leftrightarrow p$$

Domination:

$$p \vee T \Leftrightarrow T$$

$$p \wedge F \Leftrightarrow F$$

Idempotent:

$$p \vee p \Leftrightarrow p$$

$$p \wedge p \Leftrightarrow p$$

Logic Laws (cont.)

Double Negation:

$$\neg(\neg p) \Leftrightarrow p$$

Commutative:

$$p \vee q \Leftrightarrow q \vee p$$

$$p \wedge q \Leftrightarrow q \wedge p$$

Associative:

$$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$$

$$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$$

Logic Laws (cont.)

Distributive:

$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$$

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$$

De Morgan's:

$$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$$

$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$$

Misc:

$$p \vee \neg p \Leftrightarrow T$$

$$p \wedge \neg p \Leftrightarrow F$$

$$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$$

Example

Simplify the following:

$$(p \wedge q) \Rightarrow (p \vee q)$$

Predicates

Def:*predicate* - a function or formula involving some variables

Ex: let P(x) = "x > 3"

x is the variable

"x>3" is the predicate

P(5)

P(1)

Ex: Q(x,y,z) = " $x^2+y^2=z^2$ "

Q(2,3,4)

Q(3,4,5)

Quantifiers

- Universal: "for all" $\forall$
  $\forall x\ P(x)$
  $\Leftrightarrow P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots$
  Ex: $\forall x \quad x < x + 1$
  $\forall x \quad x < x^3$

- Existential: "there exists" $\exists$
  $\exists x\ P(x)$
  $\Leftrightarrow P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots$
  Ex: $\exists x \quad x = x^2$
  $\exists x \quad x < x - 1$

Combinations:

$$\forall x\ \exists y \quad y > x$$

Examples

- $\forall x\ \exists y \quad x+y=0$

- $\exists y\ \forall x \quad x+y=0$

- "every dog has his day":

  $\forall d\ \exists y\ H(d,y)$

- $\lim_{x \to a} f(x) = L$

  $\forall \varepsilon \exists \delta \forall x\ (0<|x-a|<\delta \Rightarrow |f(x)-L|< \varepsilon)$

Examples (cont.)

- n is divisible by j (denoted n|j):

  $n|j \Leftrightarrow \exists k \in \mathsf{Z}\ n=kj$

- m is prime (denoted P(m)):

  $P(m) \Leftrightarrow [\forall i \in \mathsf{Z}\ (m|i) \Rightarrow (i=m) \vee (i=1)]$

- "there is no largest prime"

  $\forall p\ \exists q \in \mathsf{Z}\ (q>p) \wedge P(q)$

  $\forall p\ \exists q \in \mathsf{Z}\ (q>p) \wedge$
  $\quad [\forall i \in \mathsf{Z}\ (q|i) \Rightarrow (i=q) \vee (i=1)\ ]$

  $\forall p\ \exists q \in \mathsf{Z}\ (q>p) \wedge$
  $[\forall i \in \mathsf{Z}\ \{\exists k \in \mathsf{Z}\ q=ki\} \Rightarrow (i=q) \vee (i=1)]$

Negation of Quantifiers

Thm: $\neg(\forall x\ P(x)) \Leftrightarrow \exists x\ \neg P(x)$

Ex: $\neg$ "all men are mortal"

$\Leftrightarrow$ "there is a man who is not mortal"

Thm: $\neg(\exists x\ P(x)) \Leftrightarrow \forall x\ \neg P(x)$

Ex: $\neg$ "there is a planet with life on it"

$\Leftrightarrow$ "all planets do not contain life"

Thm: $\neg\exists x \forall y\ P(x,y) \Leftrightarrow \forall x \exists y\ \neg P(x,y)$

Ex: $\neg$ "there is a man that exercises every day"

$\Leftrightarrow$ "every man does not exercise some day"

Thm: $\neg\forall x \exists y\ P(x,y) \Leftrightarrow \exists x \forall y\ \neg P(x,y)$

Ex: $\neg$ "all things come to an end"

$\Leftrightarrow$ "some thing does not come to any end"

Quantification Laws

Thm: $\forall x\,(P(x) \wedge Q(x))$
$\Leftrightarrow (\forall x\, P(x)) \wedge (\forall x\, Q(x))$

Thm: $\exists x\,(P(x) \vee Q(x))$
$\Leftrightarrow (\exists x\, P(x)) \vee (\exists x\, Q(x))$

Q: Are the following true?

$\exists x\,(P(x) \wedge Q(x))$
$\Leftrightarrow (\exists x\, P(x)) \wedge (\exists x\, Q(x))$

$\forall x\,(P(x) \vee Q(x))$
$\Leftrightarrow (\forall x\, P(x)) \vee (\forall x\, Q(x))$

More Quantification Laws

- $(\forall x\ Q(x)) \wedge P \Leftrightarrow \forall x\ (Q(x) \wedge P)$
- $(\exists x\ Q(x)) \wedge P \Leftrightarrow \exists x\ (Q(x) \wedge P)$
- $(\forall x\ Q(x)) \vee P \Leftrightarrow \forall x\ (Q(x) \vee P)$
- $(\exists x\ Q(x)) \vee P \Leftrightarrow \exists x\ (Q(x) \vee P)$

Unique Existence

Def: $\exists!x\ P(x)$ means there exists a unique x such that P(x) holds

Q: Express $\exists!x\ P(x)$ in terms of the other logic operators

A:

Mathematical Statements

- Definition
- Lemma
- Theorem
- Corollary

Proof Types

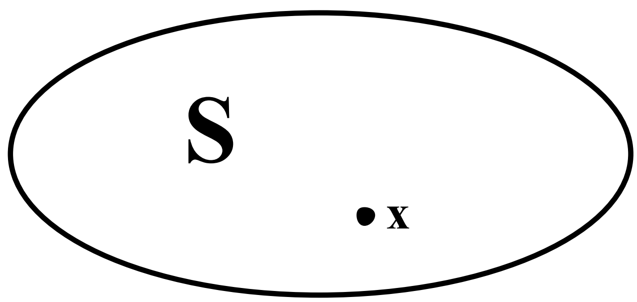
- Construction
- Contradiction
- Induction
- Counter-example
- Existence
- …

Sets

Def: *set* - an unordered collection of elements

Ex: {1, 2, 3} or {hi, there}

Venn Diagram:



Def: two sets are *equal* iff they contain the same elements

Ex: $\{1, 2, 3\} = \{2, 3, 1\}$

$\{0\} \neq \{1\}$

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

- Set <u>construction</u>:
  $|$ or $\ni$ means "such that"

  Ex: $\{k \mid 0<k<4\}$

  $\{k \mid k \text{ is a perfect square}\}$

- Set <u>membership:</u> $\in$ $\notin$

  Ex: $7 \in \{p \mid p \text{ prime}\}$

  $q \notin \{0, 2, 4, 6,\ldots\}$

- Sets can contain other sets

  Ex: $\{2, \{5\}\}$

  $\{\{\{0\}\}\} \neq \{0\} \neq 0$

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

Common Sets

Naturals: $N = \{1, 2, 3, 4, ...\}$

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

Rationals: $Q = \{ \frac{a}{b} \mid a,b \in Z,\ b \neq 0\}$

Reals: $\Re = \{x \mid x \text{ a real \#}\}$

Empty set: $\varnothing = \{\}$

Z^{+} = non-negative integers

$\Re^{-}$ = non-positive reals, etc.

Multisets

Def: a *set* w/repeated elements allowed

(i.e., each element has "multiplier")

Ex: $\{0, 1, 2, 2, 2, 5, 5\}$

For multisets: $\{3, 5\} \neq \{3, 5, 3, 3, 5\}$

Sequences

Def: ordered list of elements

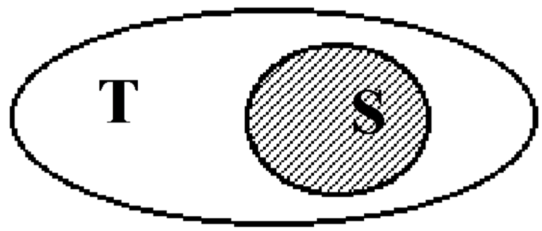
Ex: $(0, 1, 2, 5)$ "4-tuple"

$(1,2) \neq (2,1)$ "2-tuple"

Subsets

- Subset notation: $\subseteq$

$S \subseteq T \Leftrightarrow (x \in S \Rightarrow x \in T)$



- Proper subset: $\subset$

$S \subset T \Leftrightarrow ((S \subseteq T) \wedge (S \neq T))$

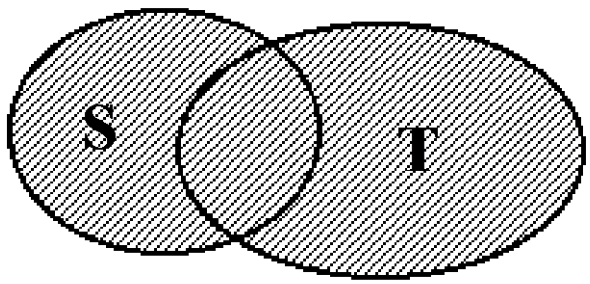
$S = T \Leftrightarrow ((T \subseteq S) \wedge (S \subseteq T))$

$\forall S \;\; \emptyset \subseteq S$

$\forall S \;\; S \subseteq S$

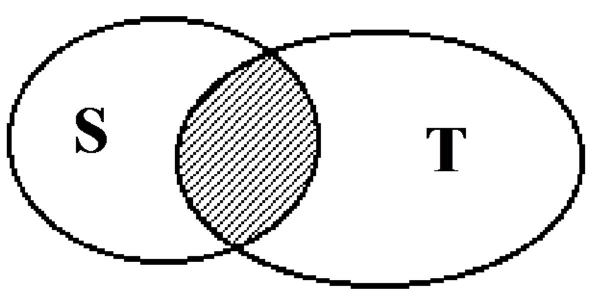
- <u>Union</u>: $\cup$

$S \cup T = \{x \mid x \in S \vee x \in T\}$



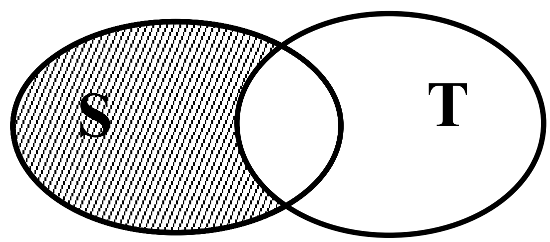
- <u>Intersection</u>: $\cap$

$S \cap T = \{x \mid x \in S \wedge x \in T\}$



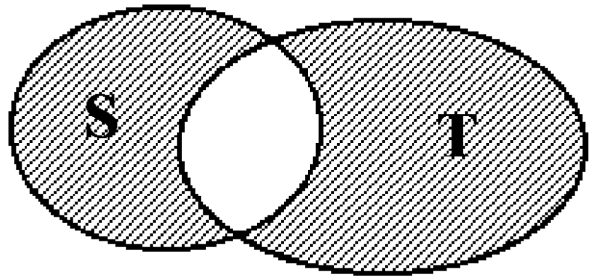
- Set <u>difference</u>: S - T

$$S - T = \{x \mid x \in S \wedge x \notin T\}$$



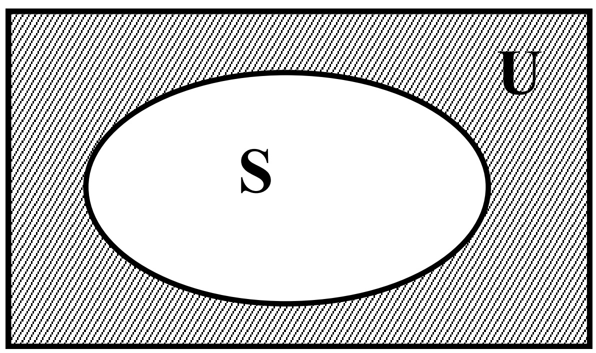
- <u>Symmetric difference</u>: $S \oplus T$

$$S \oplus T = \{x \mid x \in S \oplus x \in T\}$$
$$= S \cup T - S \cap T$$

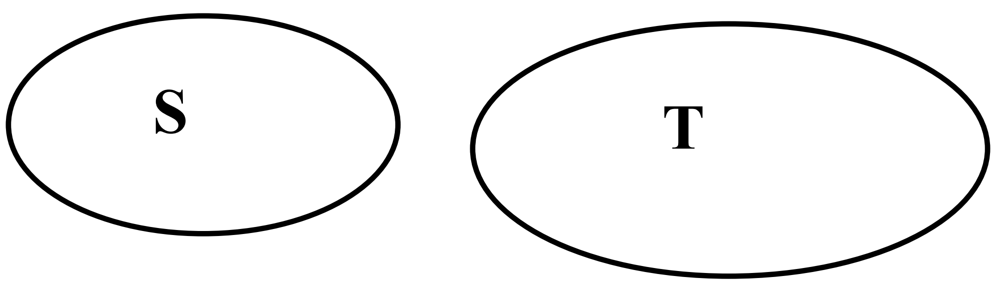


- Universal set: U (everything)
- Set <u>complement</u>: S' or $\overline{S}$

$$S' = \{x \mid x \notin S\} = U - S$$



- <u>Disjoint</u> sets: $S \cap T = \emptyset$



$S - T = S \cap T'$

$S - S = \emptyset$

Examples

$N \cup Z \cup Q \cup \Re = \Re$

$N \subset Z \subset Q \subset \Re$

$\forall x \in \Re \quad x \leq x^2+1$

$\forall x,y \in Q \ \min(x,y)=\max(x,y) \Leftrightarrow x=y$

$\Re^+ \cup \Re^- = \Re$

$\Re^+ \cap \Re^- = \{0\}$

Set Identities

- Identity:

  $S \cup \emptyset = S$

  $S \cap U = S$

- Domination:

  $S \cup U = U$

  $S \cap \emptyset = \emptyset$

- Idempotent:

  $S \cup S = S$

  $S \cap S = S$

- Complementation:

  $(S')' = S$

Set Identities (Cont.)

- Commutative Law:

$S \cup T = T \cup S$

$S \cap T = T \cap S$

- Associative Law:

$S \cup (T \cup V) = (S \cup T) \cup V$

$S \cap (T \cap V) = (S \cap T) \cap V$

Set Identities (Cont.)

- Distributive Law:

$$S\cup(T\cap V)=(S\cup T)\cap(S\cup V)$$

$$S\cap(T\cup V) = (S\cap T)\cup(S\cap V)$$

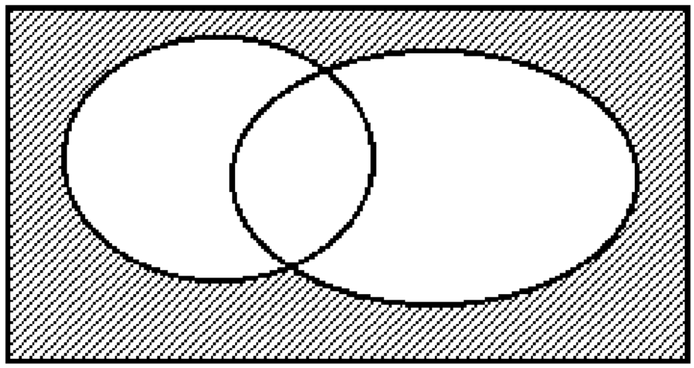
- Absorption:

$$S\cup(S\cap T)=S$$

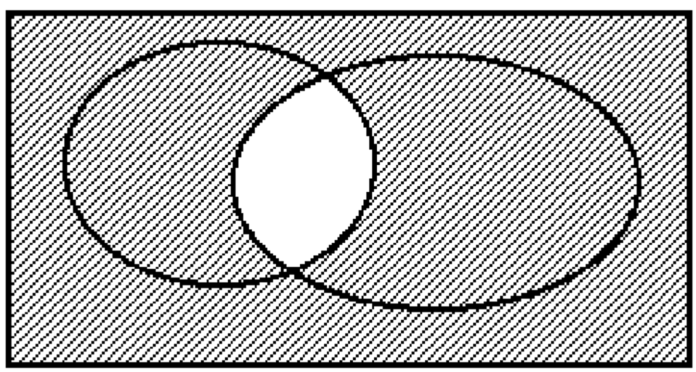
$$S\cap(S\cup T)=S$$

DeMorgan's Laws

$(S \cup T)' = S' \cap T'$



$(S \cap T)' = S' \cup T'$



Boolean logic version:

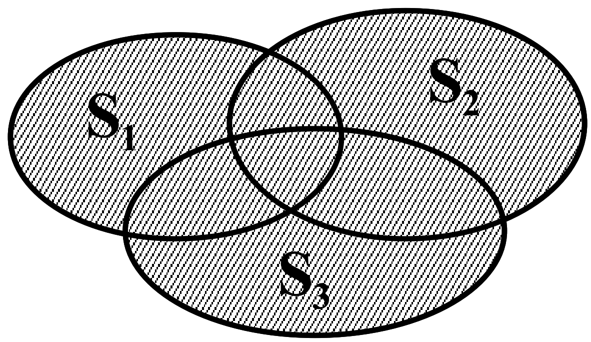
$(X \wedge Y)' = X' \vee Y'$

$(X \vee Y)' = X' \wedge Y'$

Generalized $\cup$ and $\cap$

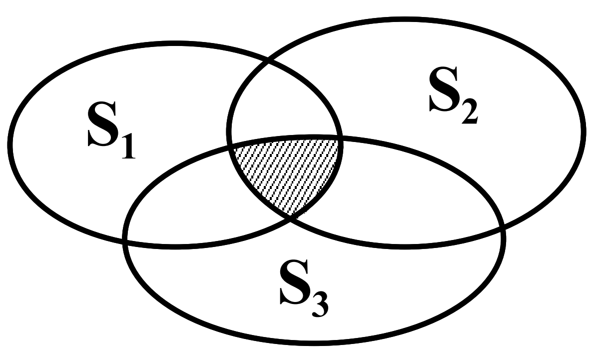
- $$\bigcup_{1 \le i \le n} S_i = S_1 \cup S_2 \cup S_3 \cup \ldots \cup S_n$$

$$= \{x \mid \exists i \; 1 \le i \le n \ni x \in S_i\}$$



- $$\bigcap_{1 \le i \le n} S_i = S_1 \cap S_2 \cap S_3 \cap \ldots \cap S_n$$

$$= \{x \mid \forall i \; 1 \le i \le n \Rightarrow x \in S_i\}$$



Set Representation

- $U = \{x_1, x_2, x_3, x_4, \ldots, x_{n-1}, x_n\}$

Ex: $S = \{x_1, \quad x_3, \quad\quad x_n\}$
bits: 1 0 1 0 ... 0 0 1

1010000...01 encodes $\{x_1, x_3, x_n\}$
0111000...00 encodes $\{x_2, x_3, x_4\}$

- "or" yields union:

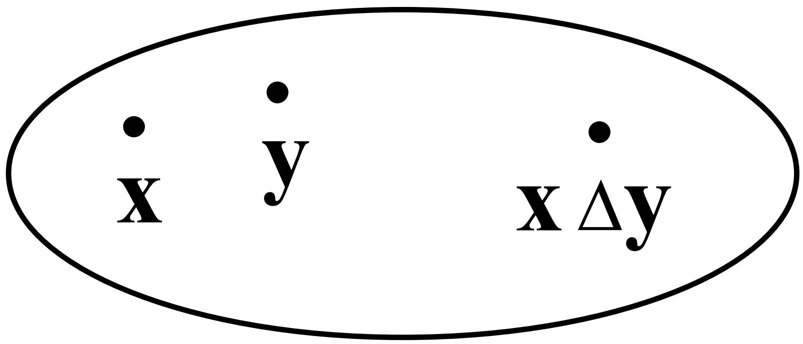
$$
\begin{array}{ll}
\ 1010000...01 & \{x_1, x_3, x_n\} \\
\vee\ \underline{0111000...00} & \{x_2, x_3, x_4\} \\
\ 1111000...01 & \{x_1, x_2, x_3, x_4, x_n\}
\end{array}
$$

- "and" yields intersection:

$$
\begin{array}{ll}
\ 1010000...01 & \{x_1, x_3, x_n\} \\
\wedge\ \underline{0111000...00} & \{x_2, x_3, x_4\} \\
\ 0010000...00 & \{x_3\}
\end{array}
$$

- Set closure: WRT operation Δ

  $$\forall x,y \in S \Rightarrow x \Delta y \in S$$



- Ex: $\Re$ is closed under addition since $x,y \in \Re \Rightarrow x+y \in \Re$

Abbreviations

- WRT "with respect to"
- WLOG "without loss of generality"

"When ideas fail, words come in very handy."
- Goethe (1749-1832)

Cartesian Product

- Ordered n-tuple: element sequence

  Ex: (2,3,5,7) is a 4-tuple

- Tuple equality:

  $(a,b)=(x,y) \Leftrightarrow (a=x) \wedge (b=y)$
  Generally: $(a_i)=(x_i) \Leftrightarrow \forall i \;\; a_i=x_i$

- Cross-product: ordered tuples

  $S \times T = \{(s,t) \mid s \in S,\ t \in T\}$

  Ex: $\{1, 2, 3\} \times \{a,b\} =$
  $\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$

  Generally, $S \times T \neq T \times S$

- Generalized cross-product:

$$S_1 \times S_2 \times \ldots \times S_n$$
$$= \{(x_1,\ldots,x_n) \mid x_i \in S_i,\ 1 \le i \le n\}$$

$$T^i = T \times T^{i-1}$$
$$T^1 = T$$

- Euclidean plane = $\Re \times \Re = \Re^2$

- Euclidean space = $\Re \times \Re \times \Re = \Re^3$

- Russel's paradox: set of all sets that do not contain themselves:

$$\{S \mid S \notin S\}$$

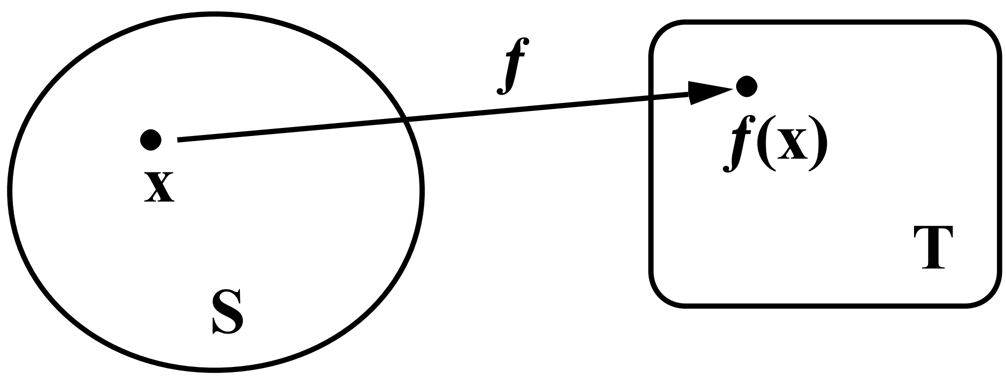
Q: Does S contain itself??

Functions

- Function: mapping f:S→T

  Domain S

  Range T



- k-ary: has k "arguments"
- Predicate: with range = {true, false}

Function Types

- One-to-one function: "1-1"

  a,b$\in$S ^ a$\neq$b $\Rightarrow$ f(a)$\neq$$f$(b)

  Ex: f: $\Re \rightarrow \Re$, f(x)=2x is 1-1

  g(x)=x^2 is not 1-1

- Onto function:

  $\forall$ t $\in$T $\exists$ s$\in$S $\ni$ f(s)=t

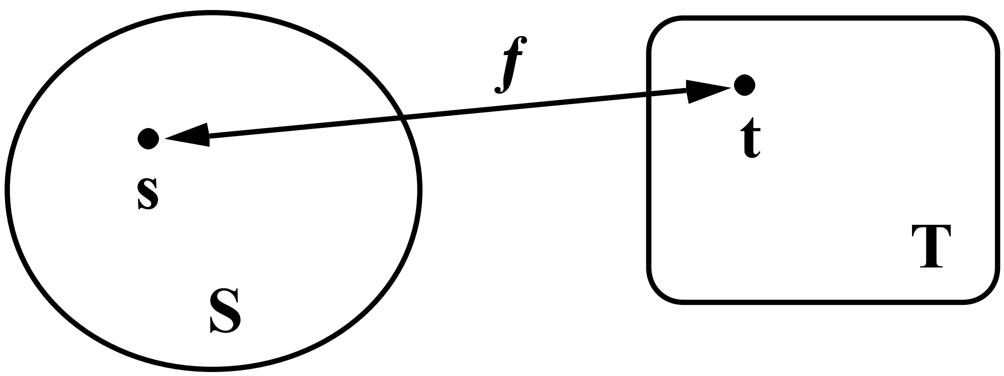
  Ex: f: Z$\rightarrow$Z, f(x)=13-x is onto

  g(x)=x^2 is not onto

1-to-1 Correspondence

- 1-to-1 correspondence: f:S↔T

  f is both 1-1 and onto



Ex: $f: \Re \leftrightarrow \Re \ni f(x)=x$ (identity)

$$h: \mathrm{N} \leftrightarrow \mathrm{Z} \ni h(x)= \begin{cases} \frac{x-1}{2}, & x \text{ odd}, \\ \frac{-x}{2}, & x \text{ even}. \end{cases}$$

- Inverse function:

f:S→T $\qquad$ f^{-1}:T→S

$f^{-1}(t)=s$ if $f(s)=t$

Ex: $f(x)=2x$ $\quad$ $f^{-1}(x)=x/2$

- Function composition:

β:S→T, α:T→V

$\Rightarrow \quad (\alpha \bullet \beta)(x)=\alpha(\beta(x))$

$(\alpha \bullet \beta)$:S→V

Ex: $\beta(x)=x+1 \quad \alpha(x)=x^2$

$(\alpha \bullet \beta)(x)= x^2 + 2x + 1$

Thm: $(f \bullet f^{-1})(x) = (f^{-1} \bullet f)(x) = x$

Set Cardinality

- Cardinality: $|S|$ = #elements in S

Ex: $|\{a,b,c\}|=3$

$|\{p \mid p \text{ prime} < 9\}| = 4$

$|\varnothing|=0$

$|\{\{1,2,3,4,5\}\}| = ?$

- Powerset: 2^S = set of all subsets

$2^S = \{T \mid T \subseteq S\}$

Ex: $2^{\{a,b\}} = \{\{\},\{a\},\{b\},\{a,b\}\}$

Q: What is $2^{\varnothing}$?

Theorem: $|2^S|=2^{|S|}$

Proof:

"Sometimes when reading Goethe, I have the paralyzing suspicion that he is trying to be funny."
- Guy Davenport

Generalized Cardinality

- S is <u>at least as large</u> as T:

  $|S| \geq |T| \Rightarrow \exists\, f: S \rightarrow T$, f onto

  i.e., "S covers T"

  Ex: $r: \Re \rightarrow Z$, $r(x) = \text{round}(x)$

  $\Rightarrow |\Re| \geq |Z|$

- S and T have <u>same cardinality</u>:

  $|S| = |T| \Rightarrow |S| \geq |T| \wedge |T| \geq |S|$

  or

  $\exists$ 1-1 correspondence $S \leftrightarrow T$

- Generalizes finite cardinality:

$\{1, 2, 3, 4, 5\} \geq \{a, b, c\}$

Infinite Sets

- Infinite set: $|S| > k \ \forall k \in Z$

  or

  $\exists$ 1-1 corres. $f: S \leftrightarrow T$, $S \subset T$

  Ex: $\{p \mid p \text{ prime}\}$, $\Re$

- Countable set: $|S| \leq |N|$

  Ex: $\emptyset$, $\{p \mid p \text{ prime}\}$, N, Z

- S is strictly smaller than T:

  $|S| < |T| \Rightarrow |S| \leq |T| \wedge |S| \neq |T|$

- Uncountable set: $|N| < |S|$

  Ex: $|N| < \Re$

  $|N| < [0,1] = \{x \mid x \in \Re, 0 \leq x \leq 1\}$

<u>Thm</u>: $\exists$ 1-1 correspondence Q$\leftrightarrow$N

<u>Pf</u> (<u>dove-tailing</u>):

	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
6	$\frac{1}{6}$	$\frac{2}{6}$	$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$	$\frac{6}{6}$	$\cdots$
5	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	$\frac{5}{5}$	$\frac{6}{5}$	$\cdots$
4	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	$\frac{5}{4}$	$\frac{6}{4}$	$\cdots$
3	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	$\frac{5}{3}$	$\frac{6}{3}$	$\cdots$
2	$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	$\frac{5}{2}$	$\frac{6}{2}$	$\cdots$
1	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{5}{1}$	$\frac{6}{1}$	$\cdots$
	1	2	3	4	5	6	

Thm: $|\Re|>|\mathsf{N}|$

Pf (diagonalization):

Assume $\exists$ 1-1 corres. f: $\Re \leftrightarrow \mathsf{N}$

Construct $x \in \Re$:

$$
\boxed{
\begin{array}{ll}
f(1)=2.\mathbf{7}18281828\ldots & \to \mathbf{8} \\
f(2)=1.4\mathbf{1}4213562\ldots & \to \mathbf{2} \\
f(3)=1.61\mathbf{8}033989\ldots & \to \mathbf{9}
\end{array}
}
$$

$\mathbf{X} = 0.\mathbf{829}\ldots \neq f(\mathrm{K}) \quad \forall \mathrm{K} \in \mathsf{N}$

$\Rightarrow$ f not a 1-1 correspondence

$\Rightarrow$ contradiction

$\Rightarrow$ $\Re$ is uncountable

Q: Is $|\Re| > |[0,1]|$?

Q: Is $|2^{\mathsf{N}}| = |\Re|$?

<u>Thm</u>: any set is "smaller" than its powerset.

$$|S| < |2^S|$$

Infinities

- $|N| = \aleph_0$
- $|\Re| = \aleph_1$
- $\aleph_0 < \aleph_1 = 2^{\aleph_0}$

- "Continuum Hypothesis"

  $\exists ?\ \omega \ni \aleph_0 < \omega < \aleph_1$

  Independent of the axioms!
  [Cohen, 1963]

- Axiom of choice [Godel 1940]

- Parallel postulate [Beltrami 1868]

Infinity Hierarchy

- $\aleph_i < \aleph_{i+1} = 2^{\aleph_i}$

$$0,\ 1,\ 2, \ldots,\ k,\ k+1, \ldots, \aleph_0,$$

$$\aleph_1,\ \aleph_2, \ldots,\ \aleph_k,\ \aleph_{k+1}, \ldots,$$

$$\aleph_{\aleph_0},\ \aleph_{\aleph_1}, \ldots,\ \aleph_{\aleph_k},\ \aleph_{\aleph_{k+1}}, \ldots$$

- First inaccessible infinity: ω...

For an informal account on infinities, see e.g.:
Rucker, <u>Infinity and the Mind</u>, Harvester Press, 1982.

Thm: # algorithms is countable.

Pf: sort programs by size:

"main(){}"

.
.

"main(){int k; k=7;}"

.
.

"<all of UNIX>"

.
.

“<Windows XP>"

.
.

"<intelligent program>"

.
.

⇒ # algorithms is countable!

Thm: # of functions is uncountable.

Pf: consider 0/1-valued functions (i.e., functions from N to {0,1}):

$\{(1,0), (2,1), (3,1), (4,0), (5,1), ...\}$

$\Rightarrow \{ \quad 2, \quad 3, \qquad\qquad 5, ...\} \in 2^N$

So, every subset of N corresponds to a different 0/1-valued function

$|2^N|$ is uncountable (why?)

$\Rightarrow$ # functions is uncountable!

Thm: most functions are uncomputable!

Pf: # algorithms is countable
functions is not countable

$\Rightarrow \exists$ more functions than
algorithms / programs!

$\Rightarrow$ some functions do not have algorithms!

Ex: The halting problem

Given a program P and input I, does P halt on I?

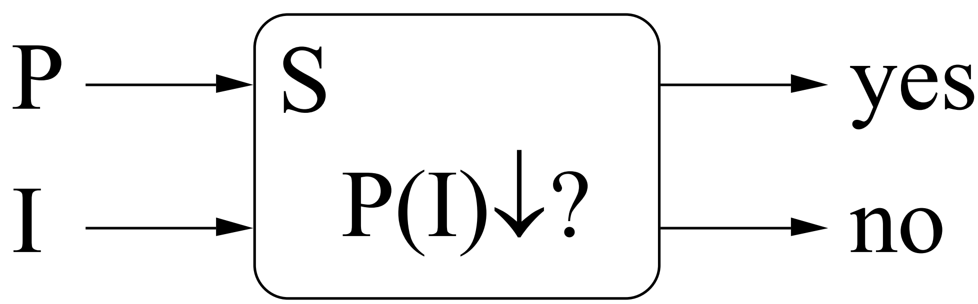
Def: $H(P,I) = \begin{cases} 1 & \text{if P halts on I} \\ 0 & \text{otherwise} \end{cases}$

The Halting Problem

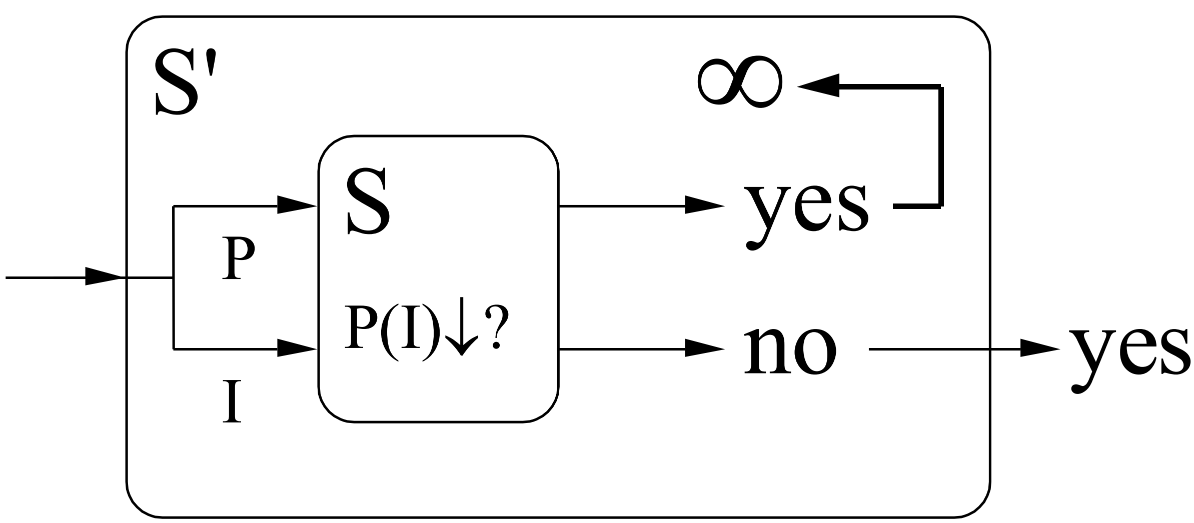
H: Given a program P and input I, does P halt on I? i.e., does P(I)↓ ?

Thm: H is uncomputable

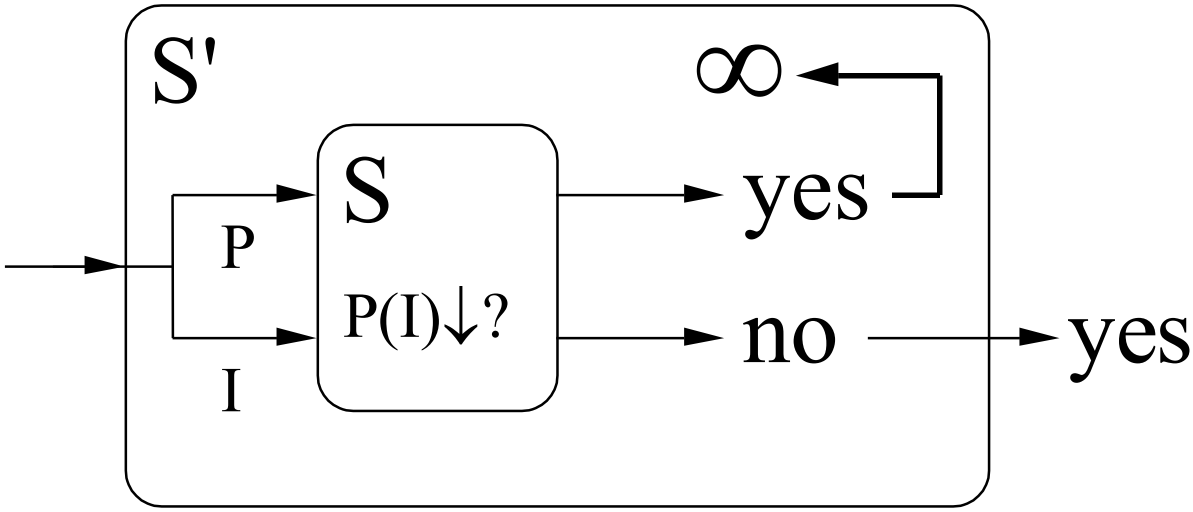
Pf: Assume subroutine S solves H.



Construct:



Analyze:



$$S'(S')\downarrow \Rightarrow S'(S')\uparrow$$
$$S'(S')\uparrow \Rightarrow S'(S')\downarrow$$

so, $S'(S')\uparrow \Leftrightarrow S'(S')\downarrow$

a contradiction!

$\Rightarrow$ S does not correctly compute H

But S was an arbitrary subroutine, so

$\Rightarrow$H is not computable!

Pigeon-Hole Principle

If N+1 objects are placed into N boxes
$\Rightarrow \exists$ a box with 2 objects.

If M objects are placed into N boxes &
M>N $\Rightarrow \exists$ box with $\left\lceil \frac{M}{N} \right\rceil$ objects.

- Useful in proofs & analyses

Relations

Relation: a set of “ordered tuples”

Ex: $\{(a,1),(b,2),(b,3)\}$

“$<$” $\{(x,y) \mid x,y \in \mathbb{Z},\ x<y\}$

Reflexive: $x \heartsuit x \ \forall x$

Symmetric: $x \heartsuit y \Rightarrow y \heartsuit x$

Transitive: $x \heartsuit y \wedge y \heartsuit z \Rightarrow x \heartsuit z$

Antisymmetric: $x \heartsuit y \Rightarrow \neg(y \heartsuit x)$

Ex: $\leq$ is reflexive
transitive
not symmetric

Equivalence Relations

Def: reflexive, symmetric, & transitive

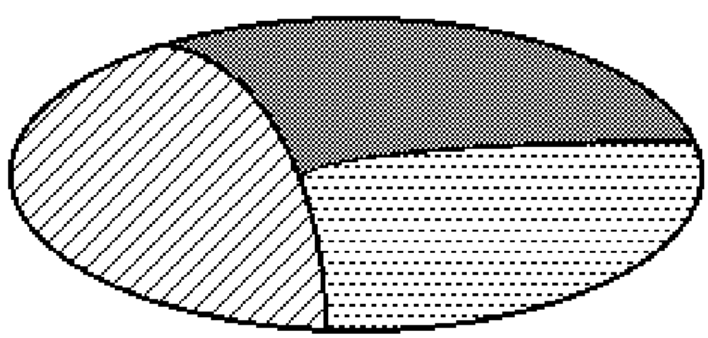
Ex: standard equality “=”

$$x=x$$

$$x=y \Rightarrow y=x$$

$$x=y \wedge y=z \Rightarrow x=z$$

Partition - disjoint equivalence classes:



Closures

- Transitive closure of ♥: TC
  smallest superset of ♥ satisfying
  $$x \heartsuit y \wedge y \heartsuit z \Rightarrow x \heartsuit z$$

  Ex: "predecessor"
  $$\{(x-1, x) \mid x \in \mathbb{Z}\}$$
  TC(predecessor) is "<" relation

- Symmetric closure of ♥:
  smallest superset of ♥ satisfying
  $$x \heartsuit y \Rightarrow y \heartsuit x$$

Graphs

- A special kind of relation

Graphs can model:

- Common relationships
- Communication networks
- Dependency constraints
- Reachability information

\+ many more practical applications!

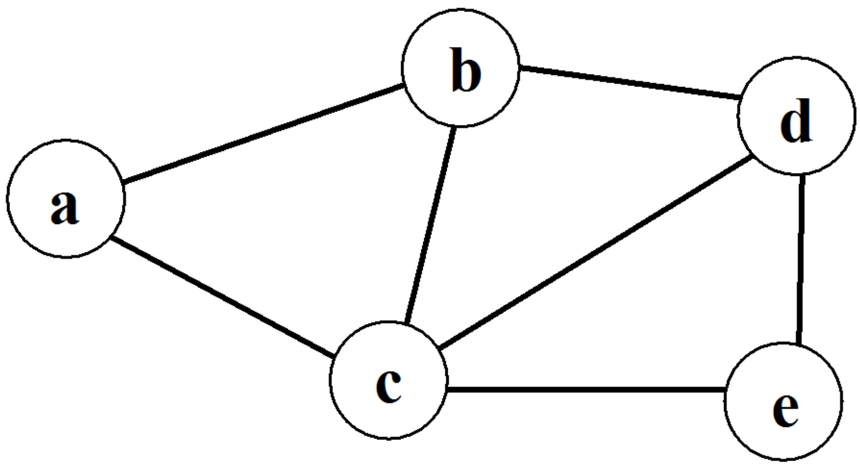
Graph $G=(V,E)$: set of vertices V, and a set of edges $E \subseteq V \times V$

Pictorially: nodes & lines

Undirected Graphs

Def: edges have <u>no</u> direction

- Example of undirected graph:

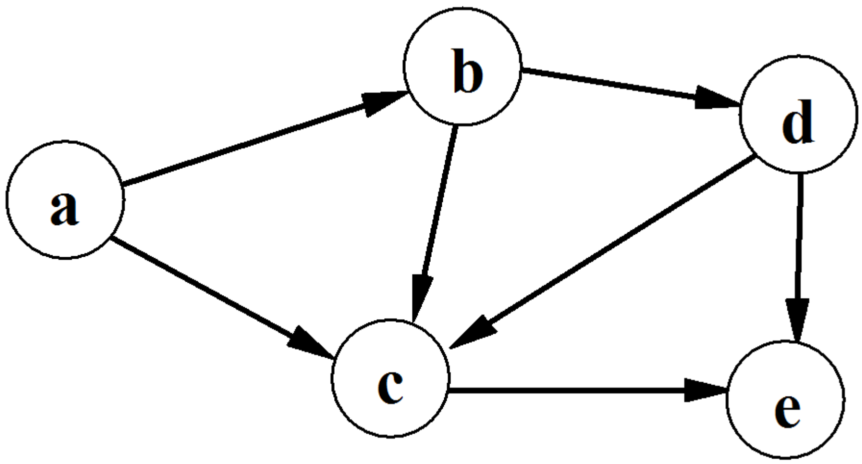


V={a,b,c,d,e}
E={(c,a),(c,b),(c,d),(c,e),
(a,b),(b,d),(d,e)}

Directed Graphs

Def: edges have direction

- Example of directed graph:

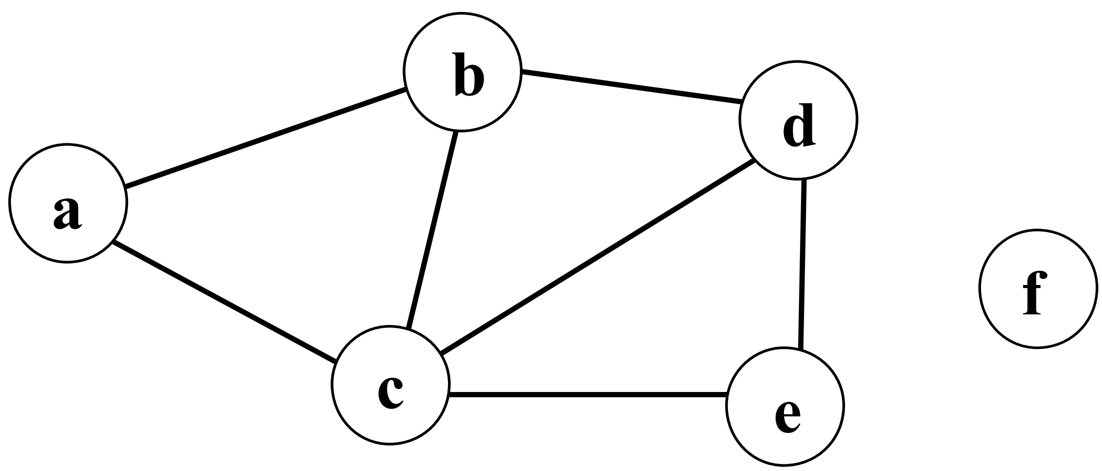


V={a,b,c,d,e}
E={(a,b),(a,c),(b,c),(b,d),
(d,c),(d,e),(c,e)}

Graph Terminology

Graph G=(V,E), E $\subseteq$ V$\times$V

- node $\equiv$ vertex
- edge $\equiv$ arc



Vertices u,v$\in$V are neighbors in G iff (u,v) or (v,u) is an edge of G

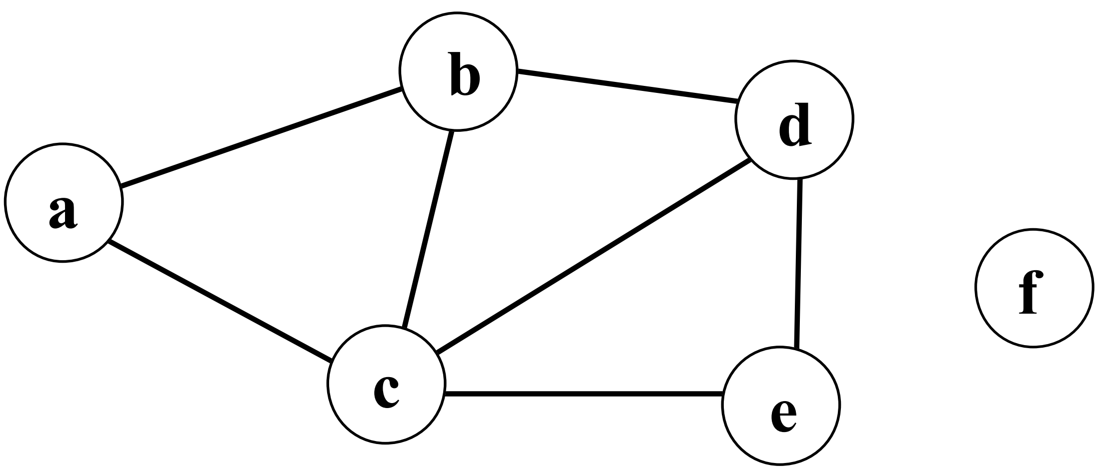
Ex: a & b are neighbors
a & e are not neighbors

Undirected Node Degree

Degree in undirected graphs:

Degree(v) = # of adjacent (incident) edges to vertex v in G

Ex: deg(c)=4 deg(f)=0

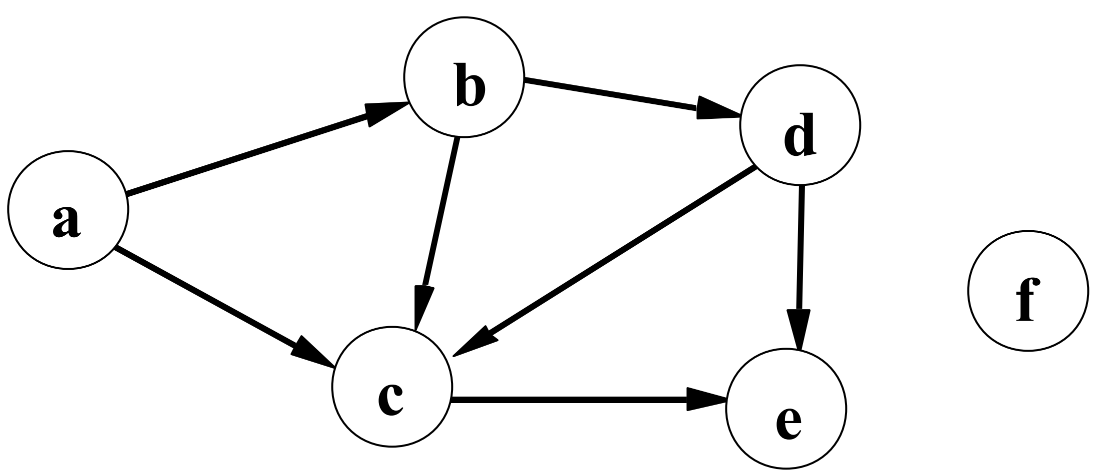


Directed Node Degree

Degree in directed graphs:

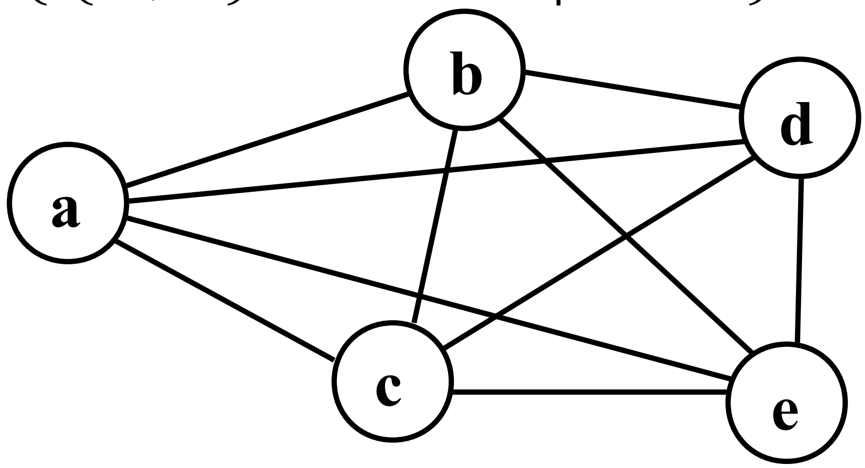
In-degree(v) = # of incoming edges
Out-degree(v) = # of outgoing edges

Ex: in-deg(c)=3 out-deg(c)=1
in-deg(f)=0 out-deg(f)=0



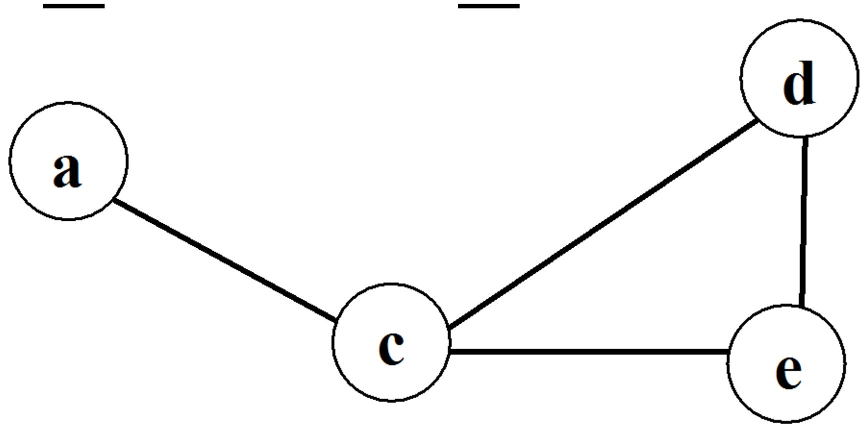
Q: Show that at any party there is an even number of people who shook hands an odd number of times.

Complete graph K_n contains all edges i.e., $E = \{\{u,v\} \in V \times V \mid u \neq v\}$



Q: How many edges are there in K_n?

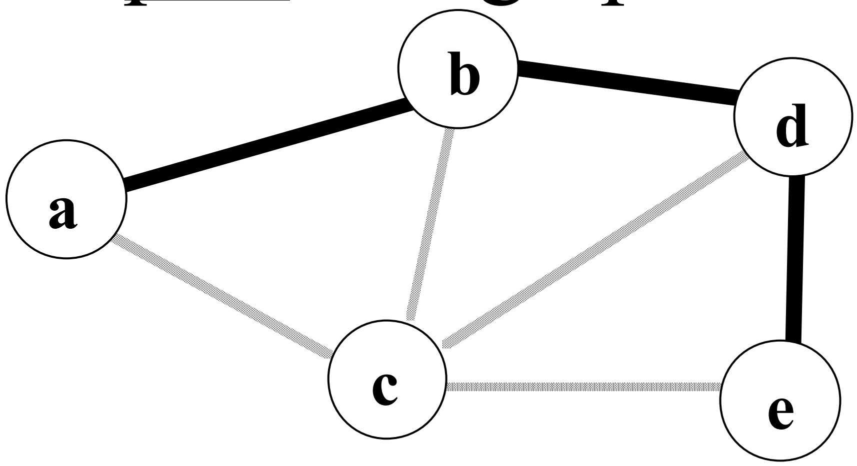
Subgraph of G is G'=(V',E') where $V' \subseteq V$ and $E' \subseteq E$



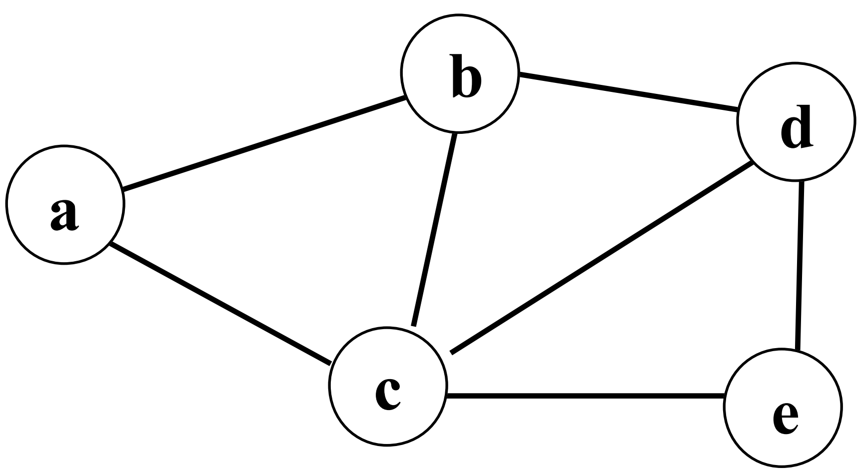
Q: Give a (non-trivial) lower bound on the number of graphs over n vertices.

Paths in Graphs

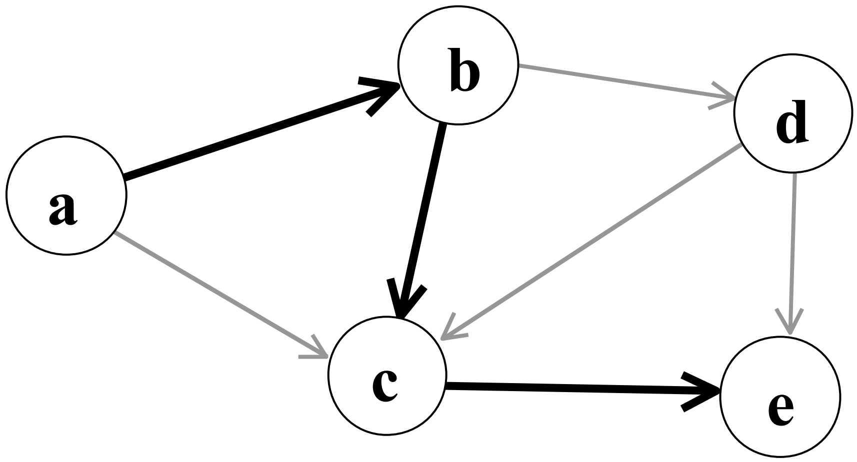
Undirected path in a graph:



A graph is connected iff there is a path between any pair of nodes:

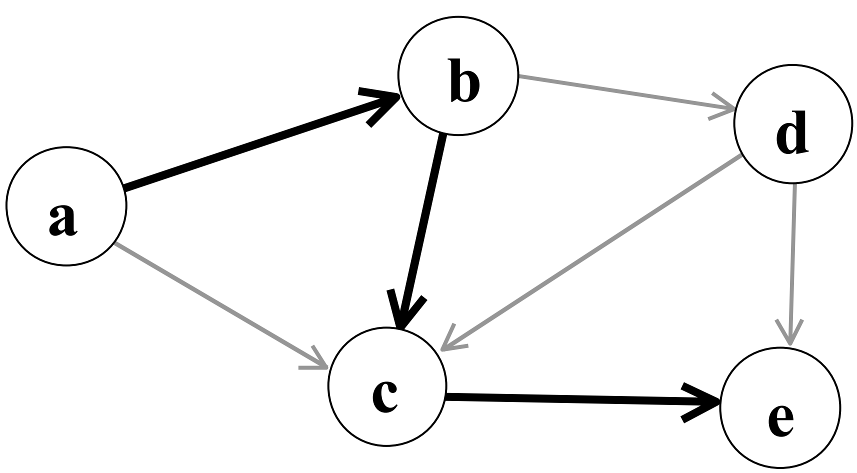


Directed path in a graph:

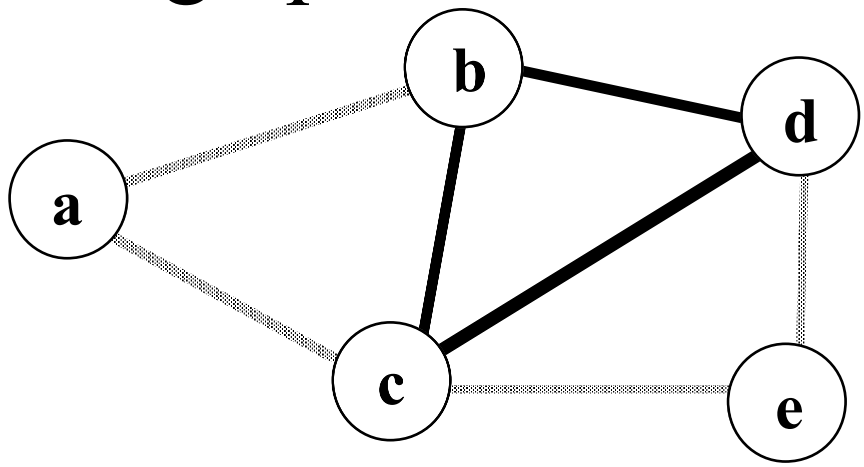


Graph is <u>strongly connected</u> iff there is a directed path between <u>any</u> node pair:

Ex: connected but not <u>strongly:</u>



A cycle in a graph:



A tree is an acyclic graph.

Tree T=(V’,E’) spans G=(V,E) if T is a connected subgraph with V’=V