Discrete Mathematics
CS 2610

Propositional Logic: Precedence

- By convention…

Logical Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Examples:

$\neg p \wedge q \rightarrow r$ is equivalent to $((\neg p) \wedge q) \rightarrow r$

$p \leftrightarrow q \rightarrow r \wedge s$ is equivalent to $p \leftrightarrow (q \rightarrow (r \wedge s))$

Logic and Bit Operations

- *A bit* is a binary digit: 0 or 1.
- Bits are usually used to represent truth values.
  - By convention:
    0 represents "false"; 1 represents "true".
- Bit operations correspond to logical operators, replacing false by 0 and true by 1

x	y	$\neg x$	$x \wedge y$	$x \vee y$	$x \oplus y$
0	0	1	0	0	0
0	1	1	0	1	1
1	0	0	0	1	1
1	1	0	1	1	0

Propositional Equivalences

- A ***tautology*** is a proposition that is always true.
  - Ex.: $p \vee \neg p$

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

- A ***contradiction*** is a proposition that is always false.
  - Ex.: $p \wedge \neg p$

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

- A ***contingency*** is a proposition that is neither a tautology nor a contradiction.
  - Ex.: $p \rightarrow \neg p$

p	$\neg p$	$p \rightarrow \neg p$
T	F	F
F	T	T

Propositional Logic: Logical Equivalence

- If p and q are propositions, then **p is logically equivalent to** q if their truth tables are the same.
  - "p is equivalent to q." is denoted by $p \equiv q$
- p, q are ***logically equivalent*** if their biconditional $p \leftrightarrow q$ is a tautology.

Propositional Logic: Logical Equivalences

- ***Identity***

$$p \wedge \mathbf{T} \equiv p$$

$$p \vee \mathbf{F} \equiv p$$

- ***Domination***

$$p \vee \mathbf{T} \equiv \mathbf{T}$$

$$p \wedge \mathbf{F} \equiv \mathbf{F}$$

- ***Idempotence***

$$p \vee p \equiv p$$

$$p \wedge p \equiv p$$

- ***Double negation***

$$\neg\neg p \equiv p$$

Propositional Logic: Logical Equivalences

- ***Commutativity:***

$$p \vee q \equiv q \vee p$$

$$p \wedge q \equiv q \wedge p$$

- ***Associativity:***

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

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

Propositional Logic: Logical Equivalences

- ***Distributive***:

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

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

- ***De Morgan's***:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q \qquad \textit{(De Morgan's I)}$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q \qquad \textit{(De Morgan's II)}$$

Propositional Logic: Logical Equivalences

- ***Excluded Middle:***

$$p \vee \neg p \equiv \mathbf{T}$$

- ***Uniqueness:***

$$p \wedge \neg p \equiv \mathbf{F}$$

- **A useful LE involving $\rightarrow$:**

$$p \rightarrow q \equiv \neg p \vee q$$

Propositional Logic

- Use known logical equivalences to prove that two propositions are logically equivalent

Example:

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

We will use the LE,

$\neg\neg p \equiv p$ ***Double negation***

$\neg(p \wedge q) \equiv \neg p \vee \neg q$ ***(De Morgan's II)***

Predicate Logic

Define:

UGA(x) = "x is a UGA student."

Universe of Discourse – *all people*

x is a variable that represents an arbitrary individual in the Universe of Discourse

A **predicate *P***, or propositional function, is a function that maps objects of the universe of discourse to propositions

- **UGA**(Daniel Boone*)* is a **proposition**.
- **UGA***(x)* is **not a proposition.**

UGA(x) is like an English predicate template

- ____________ is a UGA student

Predicate Logic: Universal Quantifier

Suppose that P(x) is a predicate on some universe of discourse.

The universal quantification of P(x) ($\forall$**x P(x)**) is the **proposition**:

"P(x) is true for all x in the universe of discourse."

$\forall$x P(x) reads "for all x, P(x) is True"

- $\forall$x P(x) is TRUE means P(x) is true for all x in UD(x).
- $\forall$x P(x) is FALSE means there is an x in UD(x) for which P(x) is false.

Predicate Logic: Existential Quantifier

Suppose P(x) is a predicate on some universe of discourse.

The existential quantification of P(x) is the proposition:

"There exists at least one x in the universe of discourse such that P(x) is true."

$\exists$ x P(x) reads "for some x, P(x)" or "There exists x, P(x) is True"

$\exists$x P(x) is **TRUE** means

there is an x in UD(x) for which P(x) is true.

$\exists$x P(x) is **FALSE** means :

for all x in UD(x) is P(x) false

Predicates - Quantifier negation

$\forall x\, P(x)$ means "P(x) is true for every x."

What about $\neg\forall x\, P(x)$?

It is not the case that ["P(x) is true for every x."]

"There exists an x for which P(x) is not true."

$$\exists x\, \neg P(x)$$

Universal negation:

$$\neg\forall x\, P(x) \equiv \exists x\, \neg P(x).$$

Proofs

A *theorem* is a statement that can be proved to be true.

A *proof* is a sequence of statements that form an argument.

Proofs: Modus Ponens

I have a total score over 96.

If I have a total score over 96, then I get an A for the class.

$\therefore$ I get an A for this class

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$$

Tautology:

$$(p \wedge (p \to q)) \to q$$

Proofs: Modus Tollens

If the power supply fails then the lights go out.

The lights are on.

$\therefore$ The power supply has not failed.

$$\begin{array}{l} \neg q \\ p \rightarrow q \\ \hline \therefore \neg p \end{array}$$

Tautology:

$$(\neg q \land (p \rightarrow q)) \rightarrow \neg p$$

Proofs: Addition

I am a student.

$\therefore$ I am a student or I am a visitor.

$$\frac{p}{\therefore\ p \vee q}$$

Tautology:

$p \rightarrow (p \vee q)$

Proofs: Simplification

I am a student and I am a soccer player.

∴ I am a student.

$$\frac{p \wedge q}{\therefore\ p}$$

Tautology:

$(p \wedge q) \rightarrow p$

Proofs: Conjunction

I am a student.
I am a soccer player.

∴ I am a student and I am a soccer player.

$$\begin{array}{c} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$$

Tautology:

$((p) \wedge (q)) \rightarrow p \wedge q$

Proofs: Disjunctive Syllogism

I am a student or I am a soccer player.
I am a not soccer player.

$\therefore$ I am a student.

$$\begin{array}{l} p \vee q \\ \neg q \\ \hline \therefore p \end{array}$$

$$\boxed{\begin{array}{c} \text{Tautology:} \\ ((p \vee q) \wedge \neg q) \rightarrow p \end{array}}$$

Proofs: Hypothetical Syllogism

If I get a total score over 96, I will get an A in the course.
If I get an A in the course, I will have a 4.0 semester average.

$\therefore$ If I get a total score over 96 then
I will have a 4.0 semester average.

$$\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore\ p \rightarrow r \end{array}$$

Tautology:

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

Proofs: Resolution

I am taking CS1301 or I am taking CS2610.

I am not taking CS1301 or I am taking CS 1302.

$\therefore$ I am taking CS2610 or I am taking CS 1302.

$$\begin{array}{c} p \vee q \\ \neg p \vee r \\ \hline \therefore\ q \vee r \end{array}$$

Tautology:

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

Proofs: Proof by Cases

I have taken CS2610 or I have taken CS1301.
If I have taken CS2610 then I can register for CS2720
If I have taken CS1301 then I can register for CS2720

$\therefore$ I can register for CS2720

$$\begin{array}{l} p \vee q \\ p \rightarrow r \\ q \rightarrow r \\ \hline \therefore \quad r \end{array}$$

Tautology:

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

Fallacy of Affirming the Conclusion

If you have the flu then you'll have a sore throat.

You have a sore throat.

$\therefore$ You must have the flu.

$$\begin{array}{l} q \\ p \to q \\ \hline \therefore p \end{array}$$

Fallacy:

$$(q \wedge (p \to q)) \to p$$

Fallacy of Denying the Hypothesis

If you have the flu then you'll have a sore throat.

You do not have the flu.

$\therefore$ You do not have a sore throat.

$$\begin{array}{l} \neg p \\ p \rightarrow q \\ \hline \therefore \neg q \end{array}$$

Fallacy:

$(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$

Inference Rules for Quantified Statements

$$\frac{\forall x\, P(x)}{\therefore\ P(c)}$$

Universal Instantiation

(for an arbitrary object c from UoD)

$$\frac{P(c)}{\therefore\ \forall x\, P(x)}$$

Universal Generalization

(for any arbitrary element c from UoD)

$$\frac{\exists x\, P(x)}{\therefore\ P(c)}$$

Existential Instantiation

(for some specific object c from UoD)

$$\frac{P(c)}{\therefore\ \exists x\, P(x)}$$

Existential Generalization

(for some object c from UoD)

Proof: Valid argument

- An argument is **valid** if whenever all the premises are **true** then the conclusion is **true**.

$p_1,\ldots,p_n$: premises or hypotheses of the problem

q: conclusion

An argument is valid if

$$p_1 \wedge p_2 \wedge \ldots \wedge p_n \rightarrow q$$

is true when $p_1,\ldots,p_n$ are true.

What happens if a premise is false?

Proofs

- Step 1: Translate the sentences into logical expressions

- Step 2: Use rules of inferences to build a proof

Direct proofs

- Start with premises and deduce the conclusion:
  - Assume that the premises are true
  - Apply rules of inferences and theorems

Vacuous Proofs

$p \rightarrow q$ is ***vacuously true*** if ***p*** is false

In this case, $p \rightarrow q$ is a **vacuous proof**

Ex. p: $0 > 1$
q: Mars is an asteroid

What can we say about $p \rightarrow q$?

Trivial Proofs

$p \rightarrow q$ is *trivially true* if ***q*** is true,

In this case, we have a **trivial proof**

Example:

$$x>1 \rightarrow 1=1$$

Indirect Proofs

To prove $p \rightarrow q$, we prove its contrapositive,

$$\neg q \rightarrow \neg p$$

Example:

if n^2 is even then n is even

is equivalent to …

if n is odd then n^2 is odd

We can prove "If n^2 is even then n is even" by proving "If n is odd then n^2 is odd"

Proof By Contradiction: Reductio ad Absurdum

- To prove ***p***, we assume $\neg$ p and derive a contradiction.

  Based on the tautology

$$(\neg p \rightarrow F) \rightarrow p$$

  "if the negation of p implies a contradiction then p must be true"

Example:

"If I win $1,000,000, I will buy a sailboat."
"If I buy a sailboat, I will go sailing every summer."
"This summer, I will take one vacation.
"I plan to go biking this summer."

Prove that I have not yet won $1,000,000.

Overview of last class

A **predicate *P***, or propositional function, is a function that maps objects in the universe of discourse to propositions

- Predicates can be quantified using the universal quantifier ("for all") $\forall$ or the existential quantifier ("there exists") $\exists$
- Quantified predicates can be negated as follows
  - $\neg\forall x\ P(x) \equiv \exists x\ \neg P(x)$
  - $\neg\exists x\ P(x) \equiv \forall x\ \neg P(x)$
- Quantified variables are called "bound"
- Variables that are not quantified are called "free"

Proof Techniques-Quantifiers: For all Proofs

- $\forall$ x P(x) : provide a proof, not just examples.

Ex. "The product of any two odd integers is odd"

Proof:

Proof Techniques

Disproving $\forall x\, P(x)$

- Find an counterexample for $\forall x\, P(x)$
  - a value k in the **Universe of Discourse** such that $\neg P(k)$

Example: For every n positive number, $2^{n^2} + 1$ is prime.

Find a counterexample:

Proof Techniques-Quantifiers: Existence Proofs

Two ways of proving $\exists x\ P(x)$.

Existence Constructive Proof:

Find a k in the UoD such that P(k) holds.

Existence Non-Constructive Proof

Prove that $\exists x\ P(x)$ is true without finding a k in the UoD such that P(k) holds

Proof Techniques-Quantifiers: Existence Proofs

$\exists x\ P(x)$:Existence Constructive Proof:

Find a k in the UoD such that P(k) holds.

Example:

There is a rational number that lies strictly between $19^{100} - 1$ and 19^{100}

Proof:

Existential Proof: Non-Constructive

Prove that $\forall n \in N$, $\exists p$ such that p is prime, and $p > n$.

Proof: (BWOC)
Assume the opposite is true.
Then $\exists n$, $\forall p$ such that p is prime, $p \leq n$.
Let $p_1, p_2, \ldots, p_k$ be all the prime numbers
between 2 and n.
Consider the value $r = p_1 \times p_2 \times \ldots \times p_n + 1$.
Then r is not divisible by any prime number $p \leq n$.
Thus, either r is prime or r has prime factors greater than n!

Sets

A *set* is an unordered collection of objects.

Examples:

- $\{ 1, 6, 7, 2, 9 \}$ $= \{6, 7, 1, 2, 9\}$
- $\{ a, d, e, 1, 2, 3\}$ $= \{a, a, d, d, e, e, 1, 2, 3\}$

Order and repetition don't matter

The empty set, or the set containing no elements.

$\varnothing = \{\}$ Note: $\varnothing \neq \{\varnothing\}$

Singleton is a set S that contains exactly one element

Universal Set

- Universal Set is the set containing all the objects under consideration.
- It is denoted by **U**

Set Builder Notation

- Set Builder – characterize the elements in a set by stating the properties that the elements must have to belong to the set.

$$\{ x \mid P(x) \}$$

  - reads x that satisfy P(x), x such that P(x)
  - x belongs to a **universal set U**.

- concise definition of a set

Examples:

P = { x | x is prime number} **U** : $\mathbf{Z^+}$

M = { x | x is a mammal} **U:** All animals

$\mathbf{Q^+} = \{ x \in \mathbf{R} \mid x = p/q$, for some positive integers p, q $\}$

Elements of sets

$x \in S$ means "x is an element of set S"
$x \notin S$ means "x is not an element of set S

Example:

$3 \in S$ reads:

"3 is an element of the set S".

Which of the following is true:

1. $3 \in \mathbf{R}$
2. $-3 \in \mathbf{N}$

Subsets

$A \subseteq B$ means "A is a subset of B" or, "B contains A"

"every element of A is also in B"
or, $\forall x\ ((x \in A) \rightarrow (x \in B))$

$A \subseteq B$ means "A is a subset of B"
$B \supseteq A$ means "B is a superset of A"

Subsets

$A \subseteq B$ means "A is a subset of B"

For Every Set S,

i) $\emptyset \subseteq S$, the empty set is a subset of every set

ii) $S \subseteq S$, every set is a subset of itself

Power Sets

The ***power set*** of S is the set of all subsets of S.

$$\mathbf{P}(S) = \{ x \mid x \subseteq S \}$$

If $S = \{a\}$, $\mathbf{P}(S) = ?$ $\{\varnothing, \{a\}\}$

If $S = \{a,b\}$, $\mathbf{P}(S) = ?$ $\{\varnothing, \{a\}, \{b\}, \{a, b\}\}$

If $S = \varnothing$, $\mathbf{P}(S) = ?$ $\{\varnothing\}$

Fact: if S is finite, $|\mathbf{P}(S)| = 2^{|S|}$.

n-Tuples

- An ***ordered n-tuple***, $n \in \mathbf{Z}^+$, is an ordered list

$$(a_1, a_2, \ldots, a_n).$$

  - Its *first* element is a_1.
  - Its second element is a_2, *etc.*
  - *Enclosed between parentheses (list not set).*

- *Order and length matters:*

$$(1, 2) \neq (2, 1) \neq (2, 1, 1).$$

Cartesian Product

The ***Cartesian Product*** of two sets A and B is:

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

Example:

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

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

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

Not commutative!

In general,

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

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

Union Operator

The ***union*** of two sets A and B is:

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

Example:

$A = \{1,2,3\}$, $B = \{1,6\}$

$A \cup B = \{1,2,3,6\}$

Intersection Operator

The ***intersection*** of two sets A and B is:

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

Example:

$A = \{1,2,3\}$, $B = \{1,6\}$

$A \cap B = \{1\}$

Two sets A, B are called ***disjoint*** iff their intersection is empty.

$$A \cap B = \varnothing$$

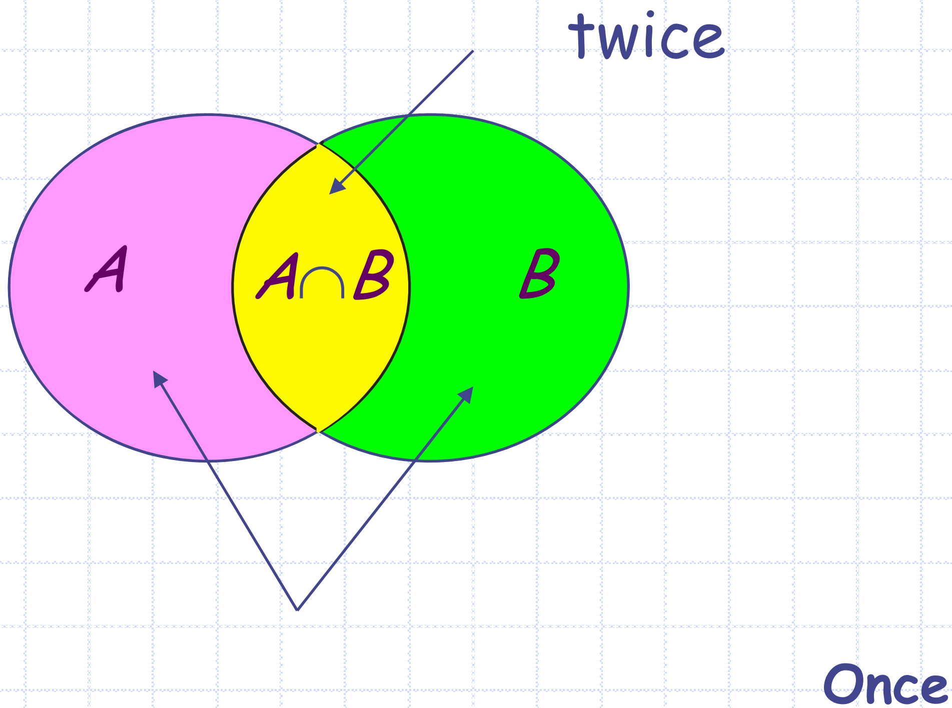
Example:

$A = \{1,2,3\}$, $B = \{9,10\}$, $C = \{2, 9\}$

A and B are disjoint sets, but A and C are not

Set Theory : Inclusion/Exclusion

- What is the cardinality of $A \cup B$?



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

Set Complement

The ***complement*** of a set A is:

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

$$x \in \overline{A} \leftrightarrow x \notin A$$

Example:

$\mathbf{U} = N$
$\underline{A} = \{x \in N \mid x \text{ is odd } \}$
$A = \{x \in N \mid x \text{ is even } \}$

$$\overline{\varnothing} = \mathbf{U}$$

$$\overline{\mathbf{U}} = \varnothing$$

Set Difference

- The ***set difference***, A - B, is:

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

Example:

$A = \{2,3,4,5\}$, $B = \{3,4,7,9\}$

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

$B - A = \{7,9\}$

It is not commutative!!

Symmetric Difference

The *symmetric difference*, $A \oplus B$, is:

$$A \oplus B = \{ x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

(i.e., x is in one or the other, but not in both)

Is it commutative ?

Set Identities

- Identity:
  - $A \cup \emptyset = A, \quad A \cap \boldsymbol{U} = A$
- Domination:
  - $A \cup \boldsymbol{U} = \boldsymbol{U}, \quad A \cap \emptyset = \emptyset$
- 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:
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cap (B \cap C) = (A \cap B) \cap C$

Set Identities

- Absorption:
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Complement:
  - $A \cup \overline{A} = \boldsymbol{U}$
  - $A \cap \overline{A} = \varnothing$
- Distributive:
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

De Morgan’s Rules

- De Morgan’s I $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$
- DeMorgan’s II $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

Proving Set Identities

How would we prove set identities of the form

$$S_1 = S_2$$

Where S_1 and S_2 are sets?

1. Prove $S_1 \subseteq S_2$ and $S_2 \subseteq S_1$ separately.
   - Use previously proven set identities.
   - Use logical equivalences to prove equivalent set definitions.
2. Use a *membership table*.

Functions (Section 2.3)

Let A and B be nonempty sets.

A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a in A. If f is a function from A to B, we write $f : A \rightarrow B$.

Functions are sometimes called *mappings*.

Proof Using Logical Equivalences

Prove that $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$

Proof: First show $\overline{(A \cup B)} \subseteq \overline{A} \cap \overline{B}$, then the reverse.

$$
\begin{array}{ll}
\text{Let } c \in \overline{(A \cup B)} & \\
c \in \overline{\{x \mid x \in A \vee x \in B\}} & \text{(Def. of union)} \\
\neg\,(c \in A \vee c \in B) & \text{(Def. of complement)} \\
\neg\,(c \in A) \wedge \neg(c \in B) & \text{(De Morgan's rule)} \\
(c \notin A) \wedge (c \notin B) & \text{(Def. of } \notin\text{)} \\
(c \in \overline{A}) \wedge (c \in \overline{B}) & \text{(Def. of complement)} \\
c \in \{x \mid x \in \overline{A} \wedge x \in \overline{B}\} & \text{(Set builder notation)} \\
c \in \overline{A} \cap \overline{B} & \text{(Def. of intersection)}
\end{array}
$$

By U.G., $\overline{(A \cup B)} \subseteq \overline{A} \cap \overline{B}$. Each step above is reversible, therefore $\overline{A} \cap \overline{B} \subseteq \overline{(A \cup B)}$.

Functions (Section 2.3)

Let A and B be nonempty sets.

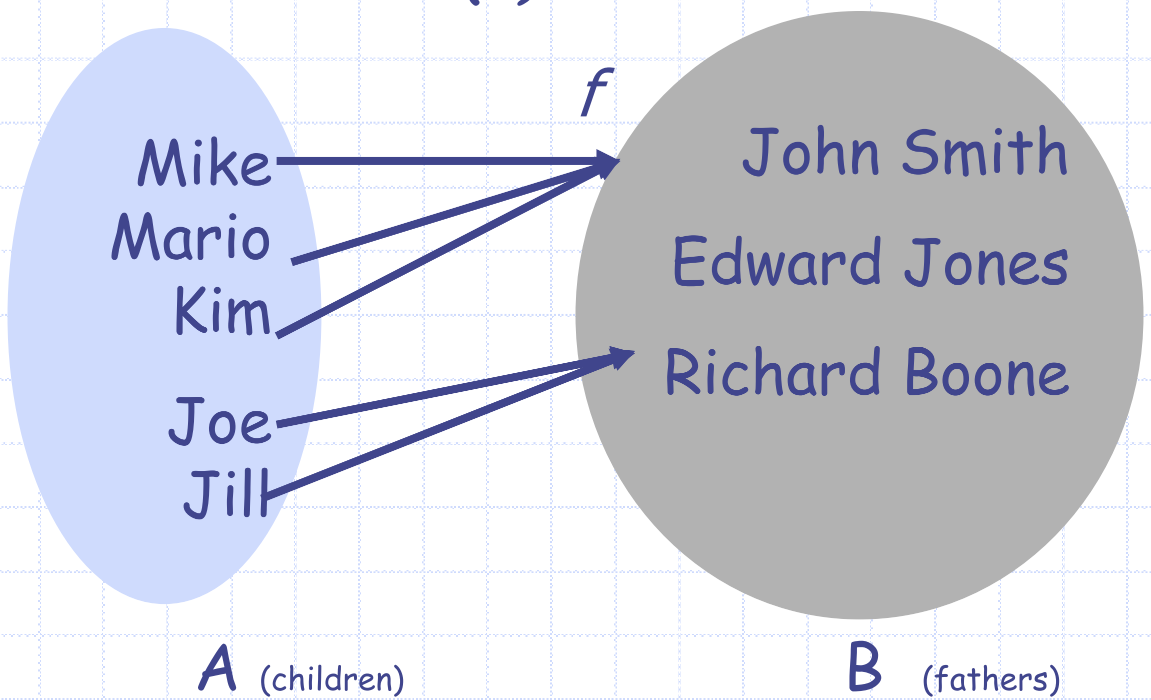
A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a in A. If f is a function from A to B, we write $f : A \to B$.

Functions are sometimes called *mappings*.

Example

A = {Mike, Mario, Kim, Joe, Jill}
B = {John Smith, Edward Jones, Richard Boone}

Let $f{:}A \rightarrow B$ where $f(a)$ means father of a.



Can grandmother of a be a function ?

Functions as Ordered Pairs

- A function $f : A \rightarrow B$ can be represented as a set of ordered pairs (recall, a relation)

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

- For every $a \in A$, there is exactly one pair $(a, f(a))$.

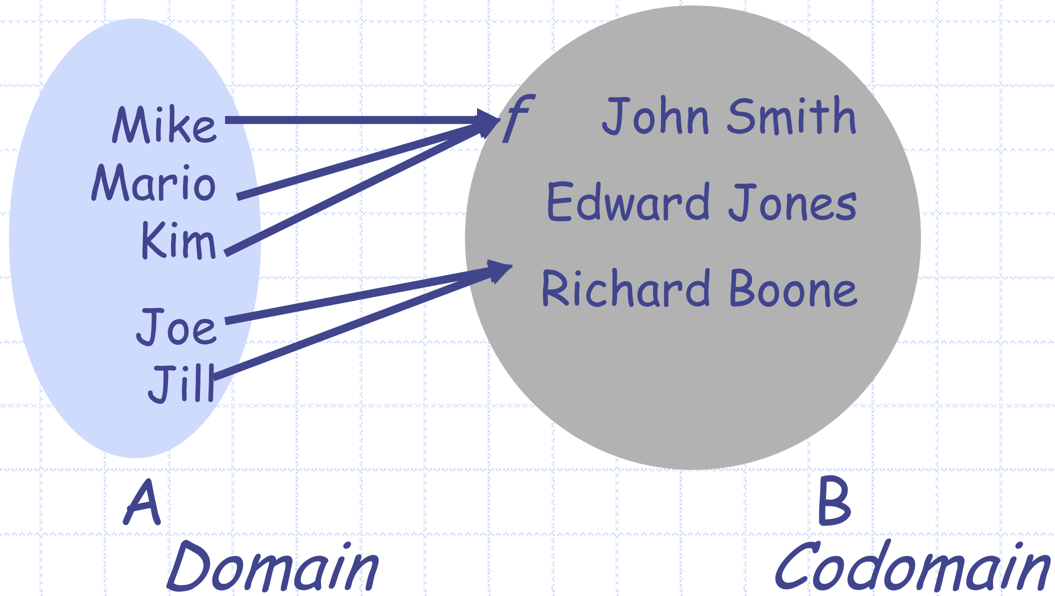
Function Terminology

Given a function $f{:}A \to B$

- A is the **domain** of f.
- B is the **codomain** of f.
- If $f(a)=b$ then b is the **image** of a under f.
- a is the **pre-image** of b under f.
  - In general, b may have more than 1 pre-image.
- The **range** R of f (or image of f) is :

  $R = \{b \mid \exists a\ f(a)=b\}$. The set of all images of a's.
- For any set $S \subseteq A$, the **image** of S,
  - $f(S) = \{ b \in B \mid \exists a \in S, f(a) = b\}$
- For any set $T \subseteq B$, the **inverse image** of T
  - $f^{-1}(T) = \{ a \in A \mid f(a) \in T \}$

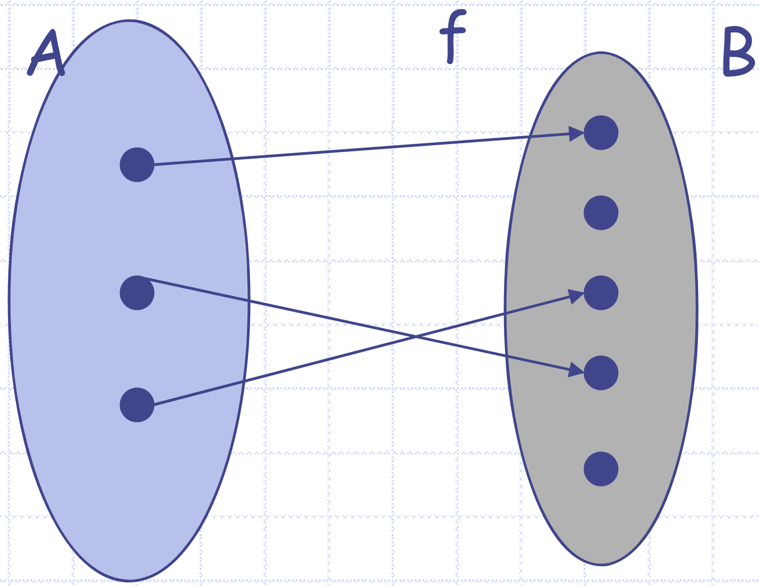
Example



- The image of Mike under f is John Smith
  - Mike is a pre-image of John Smith under f
- R (f) = {John Smith, Richard Boone}
- f(Mike,Mario,Jill) = {John Smith, Richard Boone}
- f^{-1}(Richard Boone) = {Joe, Jill}

Injective Functions (one-to-one)

- A function f: $A \rightarrow B$ is one-to-one (injective, an injection) iff $f(x) = f(y) \rightarrow x = y$ for all x and y in the domain of f $(\forall x \forall y (f(x) = f(y) \rightarrow x = y))$
- Equivalently: $\forall x \forall y (x \neq y \rightarrow f(x) \neq f(y))$

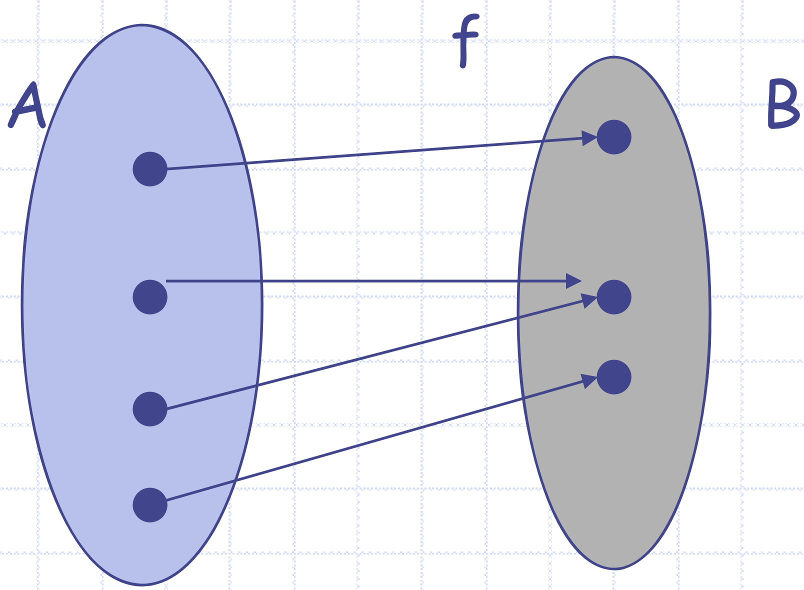


Every $b \in B$ has at most 1 pre-image

Surjective Functions (onto)

- A function f: $A \rightarrow B$ is onto (surjective, an surjection)

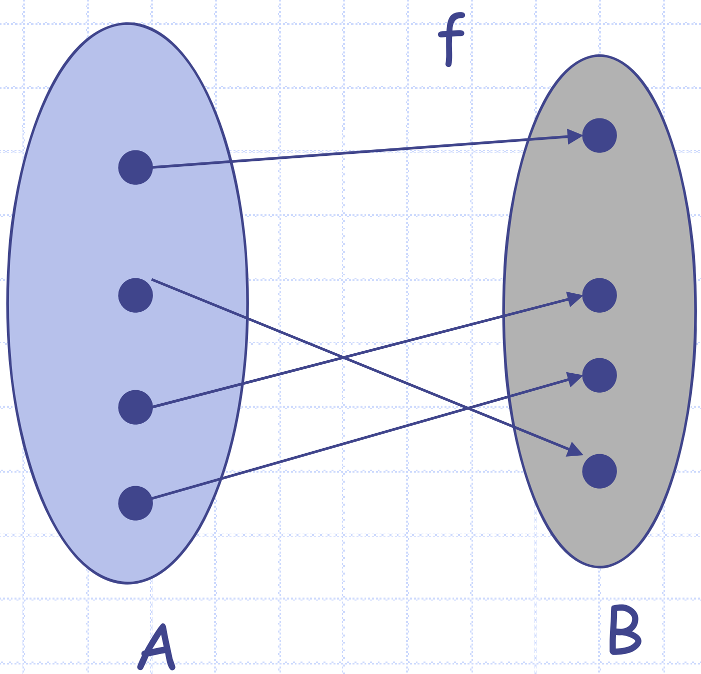
  iff $\forall y \exists x(f(x) = y)$ where $y \in B$, $x \in A$



Every $b \in B$ has at least one pre-image

Bijective Functions

- A function $f: A \to B$ is bijective iff it is one-to-one and onto (a one-to-one correspondence)



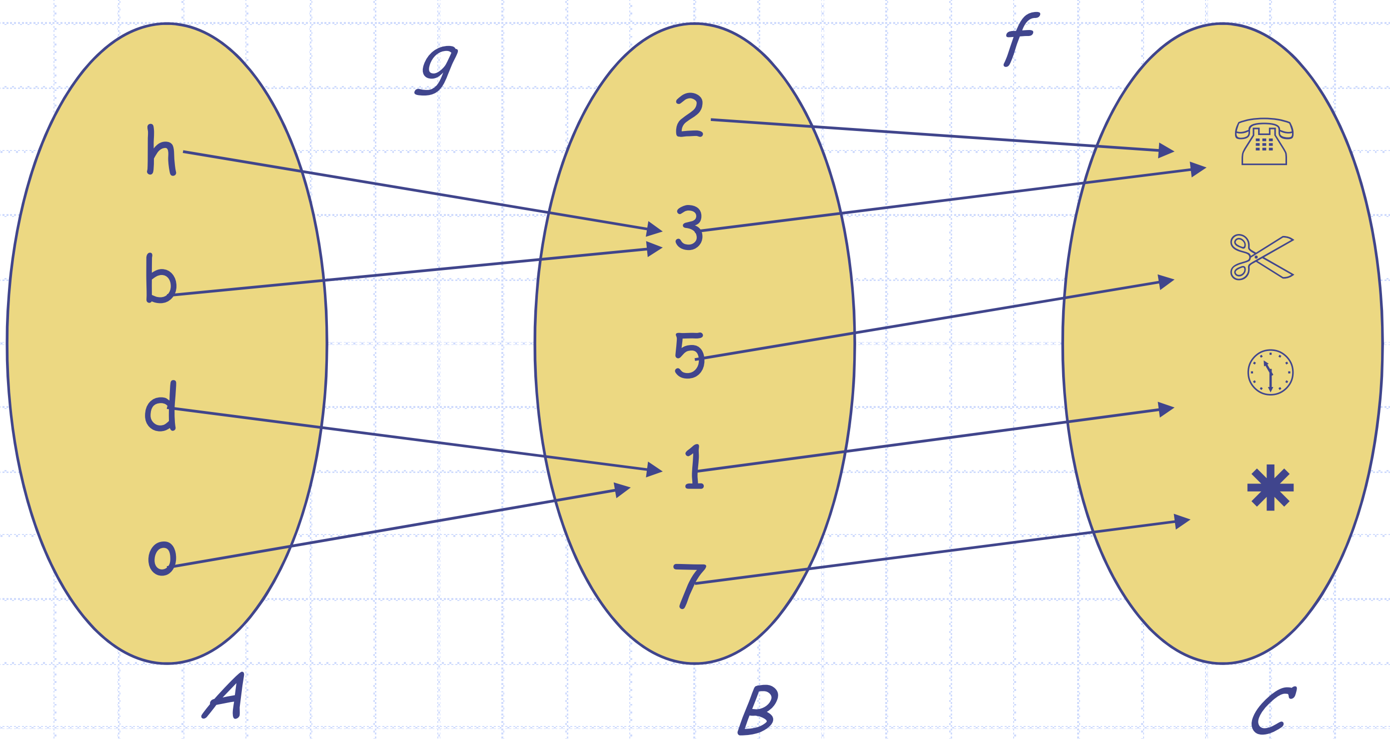
The domain cardinality equals the codomain cardinality

Function Composition

Given the functions $g: A \to B$ and $f: B \to C$, the composition of f and g, $f \circ g: A \to C$ defined as

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

$f \circ g(h)$?



Function Composition

Properties

- *Associative*: Given the functions $g: A \to B$ and $f: B \to C$ and $h: C \to D$ then

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

$$but\ (f \circ g) \neq (g \circ f)$$ not Commutative

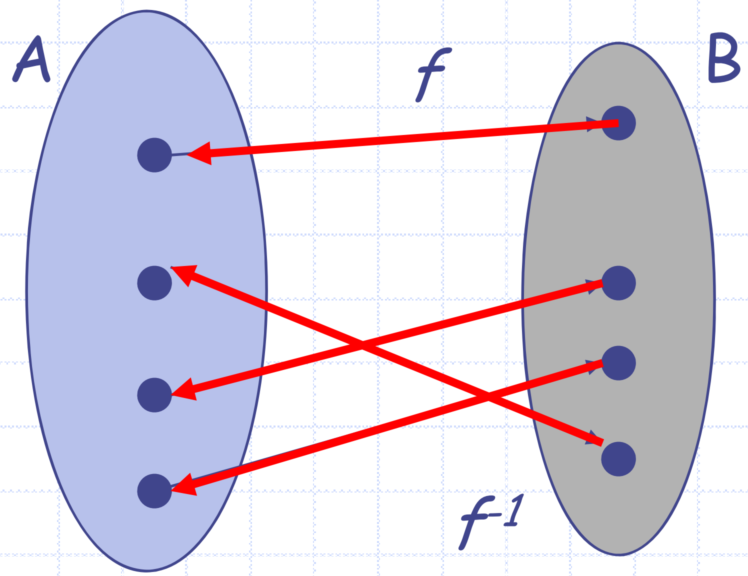
Inverse Functions

- Let $f : A \rightarrow B$ be a bijection, the inverse of f,

$$f^{-1}: B \rightarrow A$$

such that for any $b \in B$,

$$f^{-1}(b) = a \text{ when } f(a) = b$$

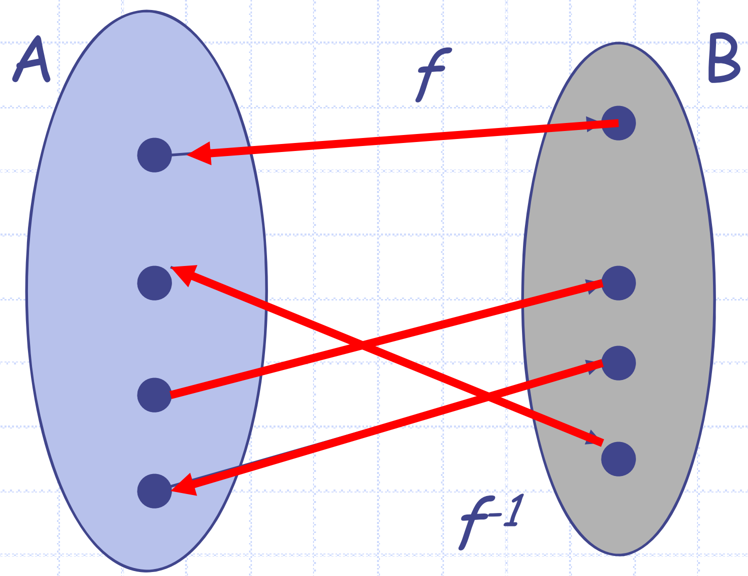


Inverse Functions

- Let $f: A \rightarrow B$ be a bijection, and $f^{-1}: B \rightarrow A$ be the inverse of f:

$$f^{-1} \circ f = I_A = (f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$$

$$f \circ f^{-1} = I_B = (f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b$$



Floor and Ceiling Function

Definition: The *floor* function $\lfloor . \rfloor : \mathbf{R} \rightarrow \mathbf{Z}$, $\lfloor x \rfloor$ is the largest integer which is less than or equal to *x*.

- $\lfloor x \rfloor$ reads the floor of x

Definition: The *ceiling* function $\lceil . \rceil : \mathbf{R} \rightarrow \mathbf{Z}$, $\lceil x \rceil$ is the smallest integer which is greater than or equal to *x*.

- $\lceil x \rceil$ reads the ceiling of x

Ceiling and Floor Properties

Let n be an integer

(1a)	$\lfloor x \rfloor = n$ if and only if $n \le x < n+1$
(1b)	$\lceil x \rceil = n$ if and only if $n-1 < x \le n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x-1 < n \le x$
(1d)	$\lceil x \rceil = n$ if and only if $x \le n < x+1$
(2)	$x-1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x+1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x+n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x+n \rceil = \lceil x \rceil + n$

Boolean Algebras (Chapter 11)

- Boolean algebra provides the operations and the rules for working with the set **{0, 1}**.
- These are the rules that underlie **electronic and optical circuits**, and the methods we will discuss are fundamental to **VLSI design**.

Boolean Algebra

- The minimal Boolean algebra is the algebra formed over the set of truth values {0, 1} by using the operations functions +, ·, - (sum, product, and complement).

- The minimal Boolean algebra is equivalent to propositional logic where
  - 0 corresponds to False
  - 1 corresponds to True
  - • corresponds logical operator AND
  - + corresponds logical operator OR
  - - corresponds logical operator NOT

Equal Boolean Functions

- Two Boolean functions F and G of degree n are equal iff for all $(x_1,..x_n) \in B^n$, $F(x_1,..x_n) = G(x_1,..x_n)$

- Example: $F(x,y,z) = x(y+\overline{z})$, $G(x,y,z) = xy + \overline{z}x$

Boolean Expressions

- Let $x_1, \ldots, x_n$ be n different Boolean variables.
- A *Boolean expression* is a string of one of the following forms (recursive definition):
  - **0**, **1**, $x_1, \ldots,$ or x_n are Boolean Expressions
  - If E_1 and E_2 are Boolean expressions then $-E_1$, (E_1E_2), or (E_1+E_2) are Boolean expressions.

Example:

$E_1 = x$
$E_2 = y$
$E_3 = z$
$E_4 = E_1 + E_2 = x + y$
$E_5 = E_1E_2 = x\, y$
$E_6 = -E_3 = -z$
$E_7 = E_6 + E_4 = -z + x + y$
$E_8 = E_6\, E_4 = -z\,(x + y)$

Note: equivalent notation: $-E = \overline{E}$ for complement

Functions and Expressions

- A Boolean expression represents a Boolean function.
  - Furthermore, *every* Boolean function (of a given degree) can be represented by a Boolean expression with n variables.

x_1	x_2	x_3	$F(x_1,x_2,x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

$$F(x_1,x_2,\overline{x_3}) = \overline{x_1}(x_2+x_3)+x_1x_2x_3$$

Boolean Functions

- Two Boolean expressions e_1 and e_2 that represent the exact *same* function F are called *equivalent*

x_1	x_2	x_3	$F(x_1,x_2,x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

$$F(x_1,x_2,\overline{x_3}) = \overline{x_1}(x_2+x_3)+x_1x_2x_3$$

$$F(x_1,x_2,\overline{x_3}) = \overline{x_1}\,\overline{x_2}+x_1x_3+x_1x_2x_3$$

Boolean Identities

- Double complement:
  $\overline{\overline{x}} = x$
- Idempotent laws:
  $x + x = x, \qquad x \cdot x = x$
- Identity laws:
  $x + 0 = x, \qquad x \cdot 1 = x$
- Domination laws:
  $x + 1 = 1, \qquad x \cdot 0 = 0$
- Commutative laws:
  $x + y = y + x, \qquad x \cdot y = y \cdot x$
- Associative laws:
  $x + (y + z) = (x + y) + z$
  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- Distributive laws:
  $x + y \cdot z = (x + y) \cdot (x + z)$
  $x \cdot (y + z) = x \cdot y + x \cdot z$
- De Morgan's laws:
  $\overline{(x \cdot y)} = \overline{x} + \overline{y}, \quad \overline{(x + y)} = \overline{x} \cdot \overline{y}$
- Absorption laws:
  $x + x \cdot y = x, \quad x \cdot (x + y) = x$

the Unit Property: $x + \overline{x} = 1$ and Zero Property: $x \cdot \overline{x} = 0$

DNF: Disjunctive Normal Form

- A *literal* is a Boolean variable or its complement.
- A *minterm* of Boolean variables $x_1, \ldots, x_n$ is a Boolean product of n literals $y_1 \ldots y_n$, where y_i is either the literal x_i or its complement $\overline{x_i}$.

minterms

Example:

$$\overbrace{\bar{x}\,\bar{y}\,\bar{z}} + \overbrace{\bar{x}\,y\,\bar{z}} + \overbrace{\bar{x}\,y\,z}$$

Disjunctive Normal Form: sum of products

We have seen how to develop a DNF expression for a function if we're given the function's "truth" table.

CNF: Conjunctive Normal Form

- A *literal* is a Boolean variable or its complement.
- A *maxterm* of Boolean variables $x_1,\dots,x_n$ is a Boolean sum of n literals $y_1 \dots y_n$, where y_i is either the literal x_i or its complement $\overline{x_i}$.

maxterms

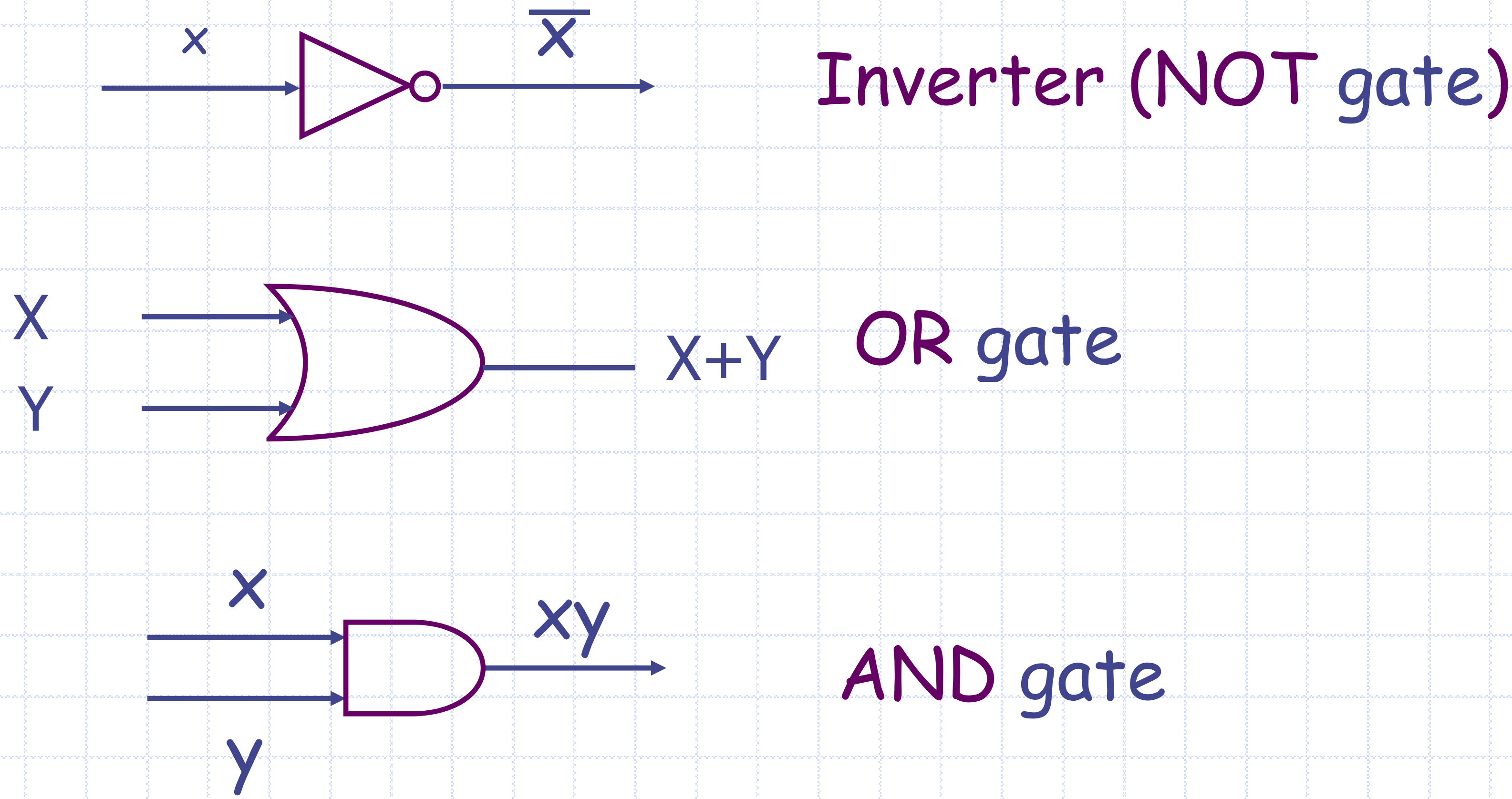
Example:

$$(x + y + z) \bullet (x + \overline{y} + z) \quad \bullet (\overline{x} + \overline{y} + z)$$

Conjuctive Normal Form: product of sums

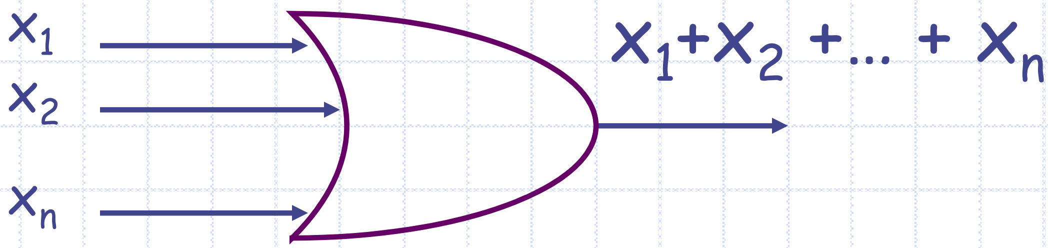
Logic Gates: the basic elements of circuits

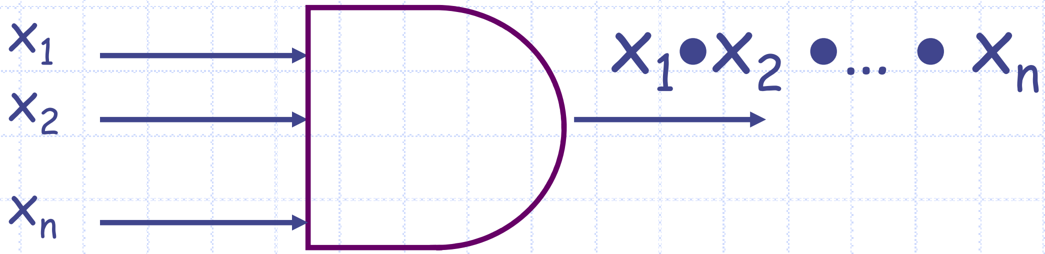
- Electronic circuits consist of so-called gates connected by wires



Multiway Logical Gates

- Multiple Input AND, OR Gates





Three Variable Karnaugh Maps

- With the three variables x, y, z, we can let x and $\overline{x}$ be on the vertical side as before
- The table will now have 4 columns: yz, $\overline{y}$z, $\overline{y}\overline{z}$, and y$\overline{z}$
  - Order is important! Columns must be *adjacent* to each other
- We also consider the first and last columns to be adjacent
  - Picture the table as a flattened cylinder
- A block of 2 cells cancels out 1 variable
- A block of 4 cells cancels out 2 variables
- What if we have a block of 8 cells?

3-Variable Example

- $xyz + \bar{x}yz + x\bar{y}z + \bar{x}\bar{y}z + xy\bar{z} = z + xy$

	yz	$\bar{y}z$	$\bar{y}\bar{z}$	$y\bar{z}$
x	1	1		1
$\bar{x}$	1	1		

implicant, prime implicant, essential prime implicant

Analysis of Algorithms

- Analyzing an algorithm
  - Time complexity
  - Space complexity
- Time complexity
  - Running time needed by an algorithm as a function of the size of the input
  - Denoted as T(N)
- We are interested in measuring how fast the time complexity increases as the input size grows
  - Asymptotic Time Complexity of an Algorithm

Algorithm Complexity

- Worst Case Analysis
  - Largest number of operations to solve a problem of a specified size.
  - Analyze the worst input case for each input size.
  - Upper bound of the running time for any input.
  - Most widely used.

- Average Case Analysis
  - Average number of operations over all inputs of a given size
    - Sometimes it's too complicated

Search Algorithms

- Search Algorithm Problem:
  Find an element *a* in a list $a_1,\ldots a_n$ (not necessarily ordered)

- Linear Search Strategy:
  Examine the sequence one element after another until all the elements have been examined or the current element being examined is the element *a*.

Sorting Algorithms

Problem: Given a sequence of numbers, sort the sequence in weakly increasing order.

Sorting Algorithms:

Input:

A sequence of n numbers $a_1, a_2, \ldots, a_n$

Output:

A re-ordering of the input sequence $(a'_1, a'_2, \ldots, a'_n)$ such that $a'_1 \leq a'_2 \leq \ldots \leq a'_n$

Sequences (Section 2.4)

Def. :A sequence is a function from a subset of integers I to a set S, $(I \subseteq Z)$

$$f: I \to S$$

- Usually, the domain I is either a set of positive or non-negative consecutive integers $\{1,2,3\ldots\}$ or $\{0,1,2,3\ldots\}$.
- We will usually be using as the domain of I the sequence:

$$I = \{i \in Z \mid i > 0\}$$

Notation:

Let $i \in I$, the image $f(i)$ is denoted as a_i, where $a_i \in S$

a_i is called a **term** of the sequence

$\{a_i\}$ represents the entire sequence

Note:

If the domain I is finite, the sequence is finite, otherwise the sequence is infinite.

Sequences

Examples:

Let the sequence $\{a_i\}$ be defined as

$a_i = i + 3$:

Terms: $a_1, a_2, a_3, \ldots$

Sequence $\{a_i\}$: $\{4, 5, 6, 7, 8 \ldots\}$

$a_i = i^2$:

Terms: $a_1, a_2, a_3, \ldots$

Sequence $\{a_i\}$: $\{1, 4, 9, 16, 25 \ldots\}$

$a_i = 1/i$:

Terms: $a_1, a_2, a_3, \ldots$

Sequence $\{a_i\}$: $\{1, 1/2, 1/3, 1/4, 1/5 \ldots\}$

Sequences

Def.:An arithmetic progression is a sequence of the form

$$a, a + d, a + 2d, a + 3d,\ldots$$

where $a \in R$ is the initial term, and $d \in R$ is the common difference,

Observe that if I = {i where i >= 0 },

- $a_i = a + i*d$
- $a_{i+1} = a_i + d$

Example:

Let d = 3, $\{a_n\}$ such that a=2, d=3

$\{a_n\} = \{2, 5, 8, 11, 14,\ldots\}$

Sequences

Def.: A geometric progression is a sequence of the form

$$a, ar, ar^2, ar^3, \ldots$$

where $a \in R$ is the initial term, and $r \in R$ is the common ratio.

Observe that if $I = \{i \mid i >= 0\}$,

- $a_i = ar^i$
- $a_{i+1} = a_i r$, where a is the first term
- It grows exponentially

Some Useful Sequences

$n^2 = 1, 4, 9, 16, 25, 36, \ldots$

$n^3 = 1, 8, 27, 64, 125, 216, \ldots$

$n^4 = 1, 16, 81, 256, 625, 1296, \ldots$

$2^n = 2, 4, 8, 16, 32, 64, \ldots$

$3^n = 3, 9, 27, 81, 243, 729, \ldots$

$n! = 1, 2, 6, 24, 120, 720, \ldots$

Summations

Let $\{a_i\}$ be a sequence. We can create the following summation of this sequence

$$\sum_{i=j}^{k} a_i :\equiv a_j + a_{j+1} + \ldots + a_k$$

- i is called the *index of summation*
- $j \in Z^+$ is the *lower bound* (or *limit*)
- $k \in Z^+$, $k \geq j$ is the *upper bound*

(Also have Π for product.)

Summations

Example

$$\sum_{i=3}^{5} i^2$$

$$\sum_{k=1}^{5} (k+1)$$

$$\sum_{j=0}^{4} (-2)^j$$

$$\sum_{j=0}^{4} \left(2^{j+1} - 2^j\right)$$

Cardinality

Def.: The cardinality of a set is the number of elements in the set.

Def.: Let A and B be two sets.

A and **B** have the same cardinality **iff** there is a one-to-one correspondence (bijection) between A and B

Countable Sets and Uncountable Sets

Def.: Set A is **countable** if it is finite or if it has the same cardinality as the set of positive integers. Otherwise it is **uncountable**.

$\aleph_0$ (aleph) denotes the cardinality of infinite countable sets

Examples:

- Infinite Countable Sets: N, Z^+, Z^-, Z
- Infinite Uncountable Sets: R, R^+, R^-

Countable Sets and Uncountable Sets

How do you demonstrate that a set is countable ?

Suppose A is a set. If there is a one-to-one and onto function $f: A \to Z^+$, then A is countable. Recall,

one-to-one means $\forall x \forall y(f(x) = f(y) \to x = y)$

onto means $\forall y \exists x(f(x) = y)$

Uncountable sets

Theorem: The set of real numbers is uncountable.

If a subset of a set is uncountable, then the set is uncountable.
The cardinality of a subset is at least as large as the cardinality of the entire set.

It is enough to prove that there is a subset of R that is uncountable

Theorem: The open interval of real numbers
$[0,1) = \{r \in \mathbf{R} \mid 0 \leq r < 1\}$ is uncountable.

Proof by contradiction using the *Cantor diagonalization argument* (Cantor, 1879)

Uncountable Sets: R

Proof (BWOC) using *diagonalization*: Suppose **R** is countable (then any subset say [0,1) is also countable). So, we can list them: $r_1, r_2, r_3, \ldots$ where

$r_1 = 0.d_{11}d_{12}d_{13}d_{14}\ldots$ the d_{ij} are digits 0-9

$r_2 = 0.d_{21}d_{22}d_{23}d_{24}\ldots$

$r_3 = 0.d_{31}d_{32}d_{33}d_{34}\ldots$

$r_4 = 0.d_{41}d_{42}d_{43}d_{44}\ldots$

etc.

Now let $r = 0.d_1d_2d_3d_4\ldots$ where $d_i = 4$ if $d_{ii} \neq 4$

$d_i = 5$ if $d_{ii} = 4$

But r is not equal to any of the items in the list so it's missing from the list so we can't list them after all.

r differs from r_i in the i^{th} position, for all i. So, our assumption that we could list them all is incorrect.

Order of Growth Terminology

Best

$O(1)$	Constant
$O(\log cn)$	Logarithmic ($c \in Z^+$)
$O(\log^c n)$	Polylogarithmic ($c \in Z^+$)
$O(n)$	Linear
$O(n^c)$	Polynomial ($c \in Z^+$)
$O(c^n)$	Exponential ($c \in Z^+$)
$O(n!)$	Factorial

Worst

Complexity of Problems

- **Tractable**
  - A problem that can be solved with a deterministic polynomial (or better) worst-case time complexity.
  - Also denoted as P
  - Example:
    - Search Problem
    - Sorting problem
    - Find the maximum

Complexity of Problems

- **Intractable**
  - Problems that are not tractable.
  - Example:
    - Traveling salesperson problem
  - Wide use of greedy algorithms to get an approximate solution.
    - For example under certain circumstances you can get an approximation that is at most double the optimal solution.

Big-O Notation

- Big-O notation is used to express the time complexity of an algorithm

  - We can assume that any operation requires the same amount of time.
  - The time complexity of an algorithm can be described independently of the software and hardware used to implement the algorithm.

Big-O Notation

Def.: Let f, g be functions with domain $\mathbf{R}_{\geq 0}$ or $\mathbf{N}$ and codomain $\mathbf{R}$.

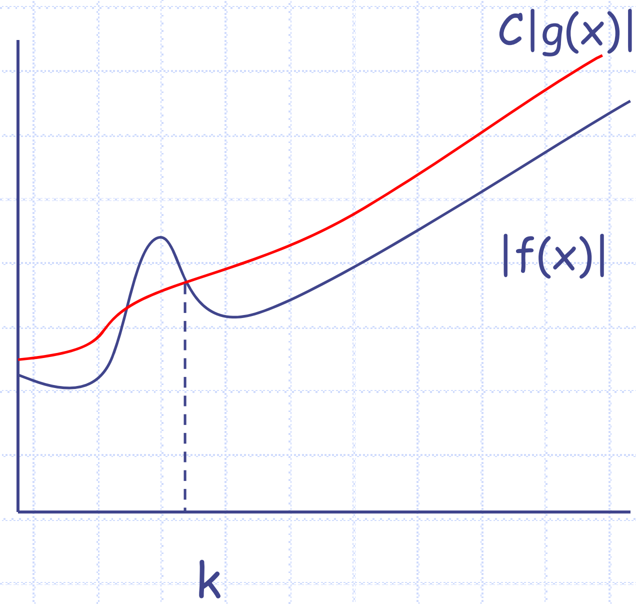
f(x) is O(g(x)) if there are constants ***C*** and ***k*** st

$$\forall\, x > k,\ |f(x)| \leq C \cdot |g(x)|$$

$f(x)$ is asymptotically dominated by $g(x)$

C|g(x)| is an upper bound of f(x).

C and k are called witnesses to the relationship between f & g.



Big-O Properties

- **Transitivity:** if f is $O(g)$ and g is $O(h)$ then f is $O(h)$
- **Sum Rule:**
  - *If* f_1 is $O(g_1)$ and f_2 is $O(g_2)$ then f_1+f_2 is $O(\max(|g_1|,|g_2|))$
  - *If* f_1 is $O(g)$ and f_2 is $O(g)$ then f_1+f_2 is $O(g)$
- **Product Rule**
  - *If* f_1 is $O(g_1)$ and f_2 is $O(g_2)$ then $f_1 f_2$ is $O(g_1 g_2)$
- For all $c > 0$, $O(cf)$, $O(f + c)$, $O(f - c)$ are $O(f)$

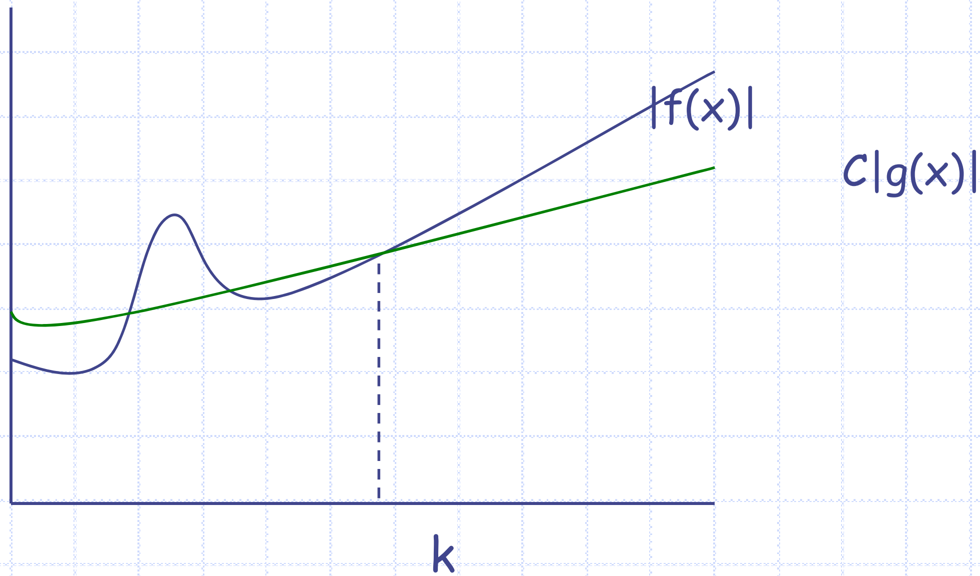
Big-Omega Notation

Def.: Let f, g be functions with domain $R_{\geq 0}$ or N and codomain R.

f(x) is $\Omega(g(x))$ if there are positive constants C and k such that

$$\forall x > k,\ C \cdot |g(x)| \leq |f(x)|$$

- $C \cdot |g(x)|$ is a lower bound for $|f(x)|$



Big-Theta Notation

Def.:Let f , g be functions with domain $\mathbf{R}_{\geq 0}$ or $\mathbf{N}$ and codomain $\mathbf{R}$.

f(x) is Θ(g(x)) if f(x) is O(g(x)) and f(x) is Ω(g(x)).

Big Summary

Upper Bound – Use Big-Oh

Lower Bound – Use Big-Omega

Upper and Lower (or Order of Growth) –

Use Big-Theta

Number Theory

- Elementary number theory, concerned with numbers, usually integers and their properties or rational numbers
  - mainly divisibility among integers
  - Modular arithmetic
- Some Applications
  - Cryptography
    - E-commerce
    - Payment systems
    - …
  - Random number generation
  - Coding theory
  - Hash functions (as opposed to stew functions ☺)

Number Theory - Division

Let a, b and c be integers, st $a \neq 0$, we say that "a divides b" or $a|b$ if there is an integer c where

$$b = a \cdot c \,.$$

- a and c are said to ***divide b*** (or are ***factors***)

$$a \mid b \wedge c \mid b$$

- b is a ***multiple*** of both a and c

Example:

$5 \mid 30$ and $5 \mid 55$ but $5 \nmid 27$

Number Theory - Division

Theorem 3.4.1: for all $a, b, c \in \mathbf{Z}$:

1. $a|0$
2. $(a|b \wedge a|c) \rightarrow a \mid (b + c)$
3. $a|b \rightarrow a|bc$ for all integers c
4. $(a|b \wedge b|c) \rightarrow a|c$

Proof: (2) a|b means b = ap, and a|c means c = aq

b + c = ap + aq = a(p + q)

therefore, a|(b + c), or (b + c) = ar where r = p+q

Proof: (4) a|b means b = ap, and b|c means c = bq

c = bq = apq

therefore, a|c or c = ar where r = pq

The Division Algorithm

Division Algorithm Theorem: Let a be an integer, and d be a positive integer. There are unique integers q, r with $r \in \{0,1,2,\ldots,d-1\}$ (ie, $0 \leq r < d$) satisfying

$$a = dq + r$$

- d is the divisor
- q is the quotient

  q = a **div** d

- r is the remainder

  r = a **mod** d

Mod Operation

Let $a, b \in \mathbf{Z}$ with $b > 1$.

$$a = q \cdot b + r, \text{ where } 0 \le r < b$$

Then a **mod** b denotes the remainder r from the division "algorithm" with dividend a and divisor b

109 **mod** 30 = ?

- $0 \le a \ \mathbf{mod}\ b \le b - 1$

Modular Arithmetic

- Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$

  Then *a is congruent to b modulo m* **iff** $m \mid (a-b)$.

- Notation:
  - "$a \equiv b \pmod{m}$" reads a is congruent to b modulo m
  - "$a \not\equiv b \pmod{m}$" reads a is not congruent to b modulo m.

- Examples:
  - $5 \equiv 25 \pmod{10}$
  - $5 \not\equiv 25 \pmod{3}$

Modular Arithmetic

Theorem 3.4.3: Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then

$a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Proof: (1) given $a \bmod m = b \bmod m$ we have

$a = ms + r$ or $r = a - ms$,

$b = mp + r$ or $r = b - mp$,

$a - ms = b - mp$

which means $a - b = ms - mp$

$= m(s - p)$

so $m \mid (a - b)$ which means

$a \equiv b \pmod{m}$

Modular Arithmetic

Theorem 3.4.3: Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then

$$a \equiv b \pmod{m} \text{ iff } a \bmod m = b \bmod m$$

Proof: (2) given $a \equiv b \pmod{m}$ we have $m \mid (a - b)$

let $a = mq_a + r_a$ and $b = mq_b + r_b$

so, $m \mid ((mq_a + r_a) - (mq_b + r_b))$

or $m \mid m(q_a - q_b) + (r_a - r_b)$

recall $0 \le r_a < m$ and $0 \le r_b < m$

therefore $(r_a - r_b)$ must be 0

that is, the two remainders are the same

which is the same as saying

$a \bmod m = b \bmod m$

Modular Arithmetic

Theorem 3.4.4: Let $a, b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:

$a \equiv b \pmod{m}$ **iff** there exists a $k \in \mathbf{Z}$ st

$$a = b + km.$$

Proof: a = b + km means

a – b = km which means

m | (a – b) which is the same as saying

$a \equiv b \pmod{m}$

(to complete the proof, reverse the steps)

Examples:

$27 \equiv 12 \pmod{5}$	$27 = 12 + 5k$	$k = 3$
$105 \equiv -45 \pmod{10}$	$105 = -45 + 10k$	$k = 15$

Modular Arithmetic

Theorem 3.4.5: Let $a, b, c, d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

1. $a + c \equiv b + d \pmod{m}$,
2. $a - c \equiv b - d \pmod{m}$,
3. $ac \equiv bd \pmod{m}$

Proof: $a = b + k_1 m$ and $c = d + k_2 m$

$$a + c = b + d + k_1 m + k_2 m$$

or $a + c = b + d + m(k_1 + k_2)$

which is

$$a + c \equiv b + d \pmod{m}$$

others are similar

Number Theory - Primes

A positive integer $n > 1$ is called ***prime*** if it is only divisible by 1 and itself (i.e., only has 1 and itself as its positive factors).

Example: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 97

A number $n \geq 2$ which isn't prime is called ***composite***.

Example:

All even numbers > 2 are composite.

By convention, 1 is neither prime or composite.

Number Theory - Primes

Fundamental Theorem of Arithmetic

Every positive integer greater than 1 has a *unique* representation as the product of a non-decreasing series of one or more primes

Examples:

- $2 = 2$
- $4 = 2 \cdot 2$
- $100 = 2 \cdot 2 \cdot 5 \cdot 5$
- $200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$
- $999 = 3 \cdot 3 \cdot 3 \cdot 37$

Number Theory – Prime Numbers

Theorem 3.5.3: There are infinitely many primes.

We proved earlier in the semester that for any integer x, there exists a prime number p such that $p > x$.

Let $\Pi(n) = |\{p \mid p \leq n \text{ and } p \text{ is prime}\}|$

Greatest Common Divisor

Let a,b be integers, $a \neq 0$, $b \neq 0$, not both zero.

The ***greatest common divisor*** of a and b is the biggest number d which divides both a and b.

Example: gcd(42,72)

Positive divisors of 42: 2,3,6,7,14,21,

Positive divisors of 72: 2,3,4,6,8,9,12,24,36

gcd(42,72)=6

Least Common Multiple

The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*.

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}.$$

Example: $\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^4 3^5 7^2$

Modular Exponentiation

- For large b, n and m, we can compute the modular exponentiation using the following property:

  $a \cdot b \bmod m = (a \bmod m)(b \bmod m) \bmod m$

AIC1

- Therefore, $b^n \pmod{m} = (b \bmod m)^n \pmod{m}$

- In fact, we can take (mod m) after each multiplication to keep all values low.

AIC1

Note: if a equiv b (mod m) and
c equiv d (mod m)
then
ac equiv bd (mod m)

also if a equiv b (mod m)
then a mod m = b mod m

cool!

AI Center, 10/17/2006

Proving Properties of Infinite Sets

- Given a predicate P(n), UD(n)={$n > k$, $n \in N$ }
- To prove the proposition

  $$\forall n\, P(n)$$

  - We need to proof that the statement is true for all $n > k$
  - It is not enough to give some few examples:

- Example:

  Claim: P(n): $n^2 + n + 41$ is a prime number

  41, 43, 47, 53, 61, 71, 83, 97, 113, 131 are all prime

  Have we proved that P(n) is true for all $n > 0$?

  No Actually: P(41) = 1763 = 41*43 is not prime

Weak Mathematical Induction

Principle of Weak Mathematical Induction

1) [***Base Case***] $P(m)$ is true for some $m \in \mathbf{N}$

   Usually (but not always) the base case is proved for m = 0 or 1

2) [***Inductive Step***]

   Inductive Hypothesis: Assume that P(n) is true, for an arbitrary n such that $n \geq m$

   Prove

$$P(n) \rightarrow P(n+1)$$

3) Then:

   $\forall n \geq m \; P(n)$ is true

Idea: If it's true for n=1, then it's true for n=2. If it's true for n=2, then it's true for n=3. If it's true for n=3, then it's true for n = 4 …

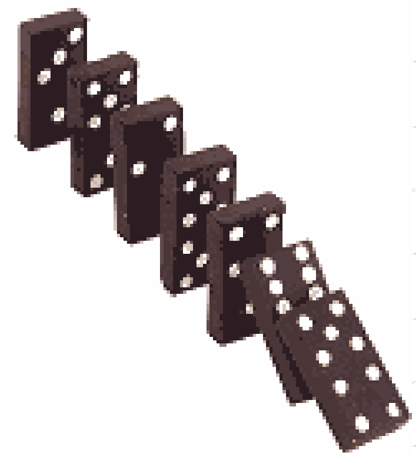
$$[P(m) \wedge \forall n \geq m \, (P(n) \rightarrow P(n+1))] \rightarrow \forall n \geq m \, P(n)$$

Strong Induction

In a proof by mathematical induction, the inductive step shows that if the inductive hypothesis P(k) is true, then P(k+1) is also true. In a proof by strong induction, the inductive step shows that if P(j) is true for all positive integers not exceeding k, then P(k+1) is true.

For the inductive hypothesis we assume that P(j) is true for j = 1, 2, 3, …, k.

Yes, they are equivalent. But now we get to use P(1), P(2), … P(k) to prove P(k+1) not just P(k)!



Strong Induction

Principle of Strong Induction

1) [***Base Case***] show $P(1)$ is true

2) [***Inductive Step***] assume P(j) for j = 1,2,…,k
Inductive Hypothesis: Prove

$$P(1) \wedge P(2) \wedge \ldots \wedge P(k) \rightarrow P(k+1)$$

Recursively Defined Sequence

In a recursively defined sequence:

1. **Base or Initial Conditions**
   - The first term(s) of the sequence are defined
2. **Recursion or Recursive Step**
   - The n^{th} term is defined in terms of previous terms

- The formula to express the n^{th} term is called a recurrence formula

Arithmetic Series:

Base: $a_0=1$, $r=3$

Recursion: $a_n=a_{n-1}+r$, $n > 0$

Recurrence Formula

Geometric Series

Base: $a_0=3$, $r=2$

Recursion: $a_n=a_{n-1}r$, $n > 0$

Recursively Defined Function

A function $f(n)$ with domain **N** or a subset of **N** is defined recursively, when $f(n)$ is defined in terms of the previous functions of $m < n$

Basis: $f(0) = 1$

Recursion:

Define $f(n)$ from f defined on smaller terms

Example

Let $f : \mathbf{N} \to \mathbf{N}$ defined recursively as

Basis: $f(0) = 1$

Recursion: $f(n + 1) = (n + 1) \cdot f(n)$.

- What are the values of the following?

  $f(1)= 1$ $f(2)= 2$ $f(3)= 6$ $f(4)= 24$

- What does this function compute? $n!$

Recursively Defined Set

- An infinite set *S* may be defined recursively, by giving:
  - Basis Step: A finite set of base elements
  - Recursive Step: a rule for forming new elements in the set from those already in the set
  - Exclusion Rule: specifies that the set only contains those elements specified in the basis step or those generated by the recursive step

Example:

Let S be defined as follows

Basis Step: $1 \in S$

Recursive Step: if $n \in S$ then $2n \in S$

$$S = \{2^k \mid k \in N\}$$

Set of Strings

Def.: An alphabet Σ is a finite non-empty set of symbols (e.g., $\Sigma = \{0, 1\}$)

Def.: A String over an alphabet Σ is a finite sequence of symbols from Σ (e.g., 11010)

The set Σ^* of strings over Σ can be defined as:

Basis Step: $\lambda \in \Sigma^*$ where λ is the empty string containing no symbols

Recursive Step: if $w \in \Sigma^*$ and $x \in \Sigma$ then $wx \in \Sigma^*$

Is Σ^* countable or uncountable ?

Recursive Definition on Strings

- Concatenation (combining two strings)

  Basis Step: if $w \in \Sigma^*$ then $w \cdot \lambda = w$, where λ is the empty string containing no symbols.

  Recursive Step: if $w_1 \in \Sigma^*$, $w_2 \in \Sigma^*$ and $x \in \Sigma$ then $w_1 \cdot (w_2\, x) \in \Sigma^*$ (same as $(w_1 \cdot w_2)\, x \in \Sigma^*$)

Example:

$\Sigma = \{a, b\}$

Let w_1=aba, w_2=a and x=b then abaab $\in \Sigma^*$

Counting (now in chapter 5)

The basic counting principles are the product rule and sum rule.

Product Rule: Suppose that a procedure can be broken down into a sequence of two tasks. If there are n ways to do the first task and for each of these ways of doing the first task, there are m ways to do the second task, then there are $n \cdot m$ ways to do the procedure.

Sum Rule: If a task can be done either in one of n ways or in one of m ways, where none of the set of n ways is the same as any of the set of m ways, then there are $n + m$ ways to do the task.

Counting

The Pigeonhole Principle: If k is a positive integer and k+1 or more objects are placed in k boxes, then there is at least one box containing two or more of the objects. (prove BWOC)

Of 367 people, at least two have the same birth day.

For every integer n there is a multiple of n that has only 0s and 1s in its decimal expansion.

Counting

- Part of *combinatorics*, the study of arrangements of objects. (Sets, sequences, sebsets, etc.)

- Counting relies on two important, but simple principles: the **Product Rule** and **Sum Rule**

Counting

- Note that sometimes we will not be able to make our subtasks completely distinct. Some ways of solving a problem might fall into multiple subtasks.
- This leads to the **Subtraction Principle**.

- Before introducing this principle, let's consider the set versions of the Product and Sum Rules.
  - If A and B are sets, then $|A \times B| = |A| \cdot |B|$
  - If A and B are disjoint sets, then $|A \cup B| = |A| + |B|$

The Pigeonhole Principle

- For $k \in \mathbf{Z}^+$, if $k+1$ or more objects are placed into k slots, there is at least one slot containing two or more objects.

- Generalized!!!!
- **If N objects are placed into k slots, then there is at least one slot containing at least $\lceil N/k \rceil$ objects.**

Permutations and Combinations

- A permutation of a set of distinct objects is an ordered arrangement (list) of these objects.
- An *r*-permutation of a set of distinct objects is an ordered arrangement of a subset of size *r*.

- The number of *r*-permutations of a set with *n* elements is given by the product rule

$$P(n,r) = n \cdot (n-1) \cdot \ldots \cdot (n-r+1), \text{ or}$$

$$P(n,r) = n! \,/\, (n-r)!, \text{ for } 0 \leq r \leq n$$

- Example: How many ways to award medals in a race with 8 people?

Permutations and Combinations

- An r-combination of a set of distinct objects is an unordered arrangement (subset) of size r.
- The number of r-combinations of a set with n elements is given by

  $$C(n,r) = n! \,/\, [r!\,(n-r)!], \text{ for } 0 \le r \le n$$

- The binomial coefficient symbolism is also used. (More on that later!)
- Examples:
  - How many 5 card poker hands are there?
  - How many bitstrings of length six contain exactly three 0's?

Probability

We can understand probability by considering sets of outcomes:

We define a set S to be a *sample space*, a set of all possible outcomes of some experiment.

We define a set $E \subseteq S$, the set of all outcomes in which the event occurs.

We further assume that all outcomes in S are equally likely.

Then the probability of the event occurring is:

$$p(E) = |E| / |S|$$

Probability

- We use p(E) to denote the probability that an event occurs.

- We use $p(\overline{E})$ to denote the probability that an event does not occur.

$$P(\overline{E}) = 1 - p(E)$$

If a coin is flipped 5 times, what is the probability of *at least* one head coming up?

Probability

- If E_1 and E_2 are two events in the same sample space, then
$$p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$$
- It's just the subtraction principle again!

A number is selected at random from the set of positive integers less than or equal to 100.

What is the probability the number is divisible by either 2 or 5?

Probability Theory

- When dealing with experiments for which there are multiple outcomes- $x_1, x_2, \ldots, x_n$ –we require
  - $0 \le p(x_i) \le 1$ for $i = 1, 2, \ldots, n$ and
  - $\sum(i=1, n)\ p(x_i) = 1$
- We can treat p as a function that maps elements from the sample space to real values in the range [0,1]. We call such a function a probability distribution.

Probability Theory

Uniform Probability Distribution:

$p(x_i) = 1/n$, for $i = 1, 2, \ldots, n$

All outcomes are equally probable.

Probability Theory

- Note that sum and product rules apply when dealing with probabilities too!
- Sequences of events are products
- Either/or requires sum rule and subtraction principle
- Complementary rule works too!

Conditional Probability

The *conditional probability* of E given F is

$$P(E \mid F) = p(E \cap F) \,/\, p(F)$$

This is the probability that E will/has occurred if we know that F has/will occur.

Independence

Two events, E and F, are **independent** iff

$$p(E_1 \cap E_2) = p(E_1)\, p(E_2)$$

The two events don't influence one another!

Repeated trials

If there are a number of trials being conducted, each of which has a probability of success of p and a probability of failure of $q = 1 - p$, then the probability of *exactly* k successes in n independent trials is

$$C(n,k)p^k q^{n-k}$$

This is called the *binomial distribution.*

Bayes' Theorem

Consider the following problem:

There are two boxes holding red and green balls.

Box 1 contains 2G, 7R.

Box 2 contains 4G, 3R.

A ball is selected by choosing a box at random, then choosing a bal at random from that box.

If a red ball is selected, what is the probability it cam from the first box?

Bayes' Theorem

Let E be "a red ball is chosen"

So $\overline{E}$ is "a green ball is chosen"

Let F be "a ball is chosen from box 1"

So $\overline{F}$ is "a ball is chosen from box 2"

We want to know $p(F|E)$.

Bayes' Theorem

By conditional prob, $p(F|E) = p(F \cap E)/p(E)$.

We know $p(E|F) = 7/9$ and $p(E|\overline{F}) = 3/7$

We know $p(F) = p(\overline{F}) = 1/2$

By conditional prob, $p(E|F) = p(E \cap F)/p(F)$

So, $p(E \cap F) = p(E|F)p(F) = (7/9)(1/2) = 7/18$

By the same logic, $p(E \cap \overline{F}) = p(E|\overline{F})p(\overline{F}) = 3/14$

Since $p(E) = p(E \cap F) + p(E \cap \overline{F})$, $p(E) = 38/63$.

$p(F|E) = p(F \cap E)/p(E) = (7/18)(63/38) = 49/76 \approx 64.5\%$

Bayes' Theorem

Given events E and F such that $p(E) \neq 0$, $p(F) \neq 0$,

$$p(F|E) = \frac{p(E|F)p(F)}{p(E|F)p(F) + p(E|\overline{F})p(\overline{F})}$$

This is the equation resulting from the reasoning we just went through. It provides a means for calculating conditional probabilities in terms of other, related conditional probabilities.

Why do this? *Some conditional probabilities are easier than others to calculate directly.*

Expected Values

We sometimes use the syntax $X(s)$ to represent a random variable over some sample space S.

For example, consider a random variable corresponding to the number of heads that come up when flipping a coin 2 times.

The sample space S is {HH, HT, TH, TT}

$X(HH) = 2$, $X(HT) = 1$, $X(TH) = 1$, $X(TT) = 0$

The "s" in $X(s)$ refers to an element of S.

Expected Values

There is a formal way to determine this calculation.

For a random variable X(s) over sample space S, the *expected value of X* is

$$E(X) = \sum_{s \in S} p(s)X(s)$$

You might prefer to think of it this way…

$$E(X) = \sum_{r \in X(s)} p(X=r)r$$

Variance

Expected value gives us an important piece of information regarding a distribution or random variable.

It's like knowing the *average* grade for the class.

But the class average doesn't tell us how *spread out* the classes scores were. For that we need another measure- a measure of ***spread.***

Variance

Variance is a measure of spread.

For a ranom variable X over a sample space S, the variance of X is given by

$$V(X) = \sum_{s \in S} (X(s) - E(X))^2 \, p(s)$$

You may prefer the following form (I certainly do!):

$$V(X) = E(X^2) - E(X)^2$$

Standard Deviation

Combined, variance and expected value can give a lot of information. Many distributions, such as the Normal distribution (bell curve), are defined in terms of these two parameters.

The *standard deviation* of X is sometimes used instead of variance. It has nice properties that you may learn about if you take a course in probability of statistics.

The standard deviation of X is given by

$$\sigma(X) = V(X)^{\frac{1}{2}}$$

Intro to Recurrence Relations

Earlier in the semester, we saw how we could define sequences recursively or functionally.

Specifically, we learned how to take functionally-defined sequences and transform them to recursively-defined sequences.

Example: $a_n = 2^n$ becomes

$$
\begin{aligned}
a_0 &= 1 \\
a_{n+1} &= 2^{n+1} = 2 \cdot 2^n \\
&= 2a_n, \text{ for } n \geq 1.
\end{aligned}
$$

Intro to Recurrence Relations

- Solving recurrence relations works in the opposite direction.
- But there's a catch… (Isn't there always?)

- A recursive definition of a sequence involves a recursive formula and a set of basis values.
- The formula itself, without the initial conditions, is a recurrence relation.

- We are going to be interested in *solving* relations both with, and without, initial conditions.

Intro to Recurrence Relations

Without initial conditions, a recurrence relation defines a set, or family, of sequences.

Consider $a_{n+1} = 2a_n$.

If $a_0 = 1$, $a_n = 2^n$.

But if $a_0 = 3$, $a_n = 3 \cdot 2^n$.

These two sequences are clearly similar. This is because $a_{n+1} = 2a_n$ defines a family of sequences, $a_n = a_0 \cdot 2^n$, for $n \geq 1$.

Intro to Recurrence Relations

A recurrence relation along with initial conditions specify a single sequence. Any such sequence is a *solution* to the relation.

We can check solutions using substitution.

Consider the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$.
Is $a_n = 3n$ a solution for $n \geq 1$? Try it out!

$$\begin{aligned} a_n &= 2a_{n-1} - a_{n-2} = 2 \cdot 3(n-1) - 3(n-2) \\ &= 6n - 6 - 3n + 6 \\ &= 3n \\ &= a_n \end{aligned}$$

Intro to Recurrence Relations

Finally, let's see how we can apply recurrence relations and their solutions to a tough counting problem.

How many bitstrings of length n do not contain consecutive 0's?

The techniques we've studied so far can't solve this without ridiculous amounts of effort!

One solution is $5^{-\frac{1}{2}}((1+5^{\frac{1}{2}})/2)^{n+2} - 5^{-\frac{1}{2}}((1-5^{\frac{1}{2}})/2)^{n+2}$.

We can find a more elegant and easier solution!!!