Digital Logic Design: a rigorous approach ©

Chapter 1: Sets and Functions

Guy Even Moti Medina

School of Electrical Engineering Tel-Aviv Univ.

December 5, 2012

Book Homepage:
http://www.eng.tau.ac.il/~guy/Even-Medina

what is a set?

- A set is a collection of objects from a universal set.
- The universal set contains all the possible objects.
- We denote the universal set by U.

Example

- $U =$ set of all real numbers $\mathbb{R}$
- $U =$ set of all natural numbers $\mathbb{N}$ (integers ≥ 0)

set notations

- Suppose $U = \mathbb{N}$.
- $A = \{1, 5, 12\}$ means "the set A contains the elements $1, 5$, and 12".
- Membership $x \in A$ means "x is an element of A".
- Cardinality $|A|$ denotes the number of elements in A.

Example

- $12 \in A$: 12 is an element of A.
- $7 \notin A$: 7 is not an element of A.
- $|A| = 3$.

Definition

A is a subset of B if

$$\forall x \in U : x \in A \Rightarrow x \in B.$$

Notation: $A \subseteq B$.

Example

- $U = \mathbb{R}$
- $A = \{1, \pi, 4\}$
- B is the interval $[1, 10]$
- $A \subseteq B$.

equality

Definition

$A = B$ if
$$\forall x \in U : x \in A \Leftrightarrow x \in B.$$

Example

- $U = \mathbb{R}$
- $A = \{1, \pi, 4\}$
- $B = \{4, 1, \pi\}$
- $C = \{1, 2, 3, 4\}$
- $A = B$ but $A \neq C$.

Claim

$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

union

Definition

The union of A and B is the set C that satisfies

$$\forall x \in U : x \in C \quad \Leftrightarrow \quad x \in A \text{ or } x \in B.$$

Notation: $C = A \cup B$.

Example

- $U = \mathbb{R}$
- $A = \{1, \pi, 4\}$
- $C = \{1, 2, 3, 4\}$
- $A \cup C = \{1, 2, 3, 4, \pi\}$.

Claim

$A \subseteq A \cup B$.

intersection

Definition

The intersection of A and B is the set C that satisfies

$$\forall x \in U : x \in C \quad \Leftrightarrow \quad x \in A \text{ and } x \in B.$$

Notation: $C = A \cap B$.

Example

- $U = \mathbb{R}$
- $A = \{1, \pi, 4\}$
- $C = \{1, 2, 3, 4\}$
- $A \cap C = \{1, 4\}$.

Claim

$A \cap B \subseteq A$.

difference

Definition

The difference of A and B is the set C that satisfies

$$\forall x \in U : x \in C \quad \Leftrightarrow \quad x \in A \text{ and } x \notin B.$$

Notation: $C = A \setminus B$.

Example

- $U = \mathbb{R}$
- $A = \{1, \pi, 4\}$
- $B = \{1, 2, 3, 4\}$
- $A \setminus B = \{\pi\}$.

Claim

$A \setminus B \subseteq A$.

Definition

The empty set is the set that does not contain any element. It is usually denoted by $\emptyset$.

The empty set is a very important set (as important as the number zero).

Claim

- $\forall x \in U : \; x \notin \emptyset$
- $\forall A \subseteq U : \; \emptyset \subseteq A$
- $\forall A \subseteq U : \; A \cup \emptyset = A$
- $\forall A \subseteq U : \; A \cap \emptyset = \emptyset$.

specification

Sets are often specified by a condition or a property. Let P denote a property. We denote the set of all elements that satisfy property P as follows

$$\{x \in U \mid x \text{ satisfies property } P\}.$$

Example

- $\mathbb{Z} \triangleq \{x \in \mathbb{R} \mid x \text{ is a multiple of } 1\}$
- $\mathbb{N} \triangleq \{x \in \mathbb{Z} \mid x \geq 0\}$
- set of even integers is $\{x \in \mathbb{Z} \mid x \text{ is a multiple of } 2\}$

the complement set

Every set we consider is a subset of the universal set. This enables us to define the complement of a set as follows.

Definition

The complement of a set A is the set $U \setminus A$. We denote the complement set of A by $\bar{A}$.

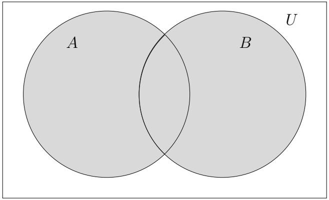
Claim

$\bar{A} = \{x \in U \mid x \notin A\}$.

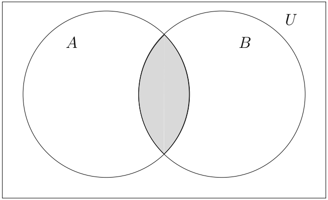
Example

- If $U = \mathbb{N}$ and $A =$ even numbers, then $\bar{A} =$ odd numbers.

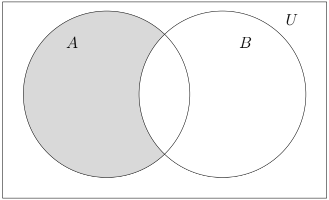
Venn diagrams



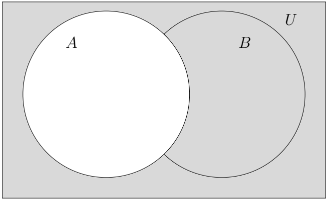
(a) Union: $A \cup B$



(b) Intersection: $A \cap B$



(c) Difference: $A \setminus B$



(d) Complement: $U \setminus A = \bar{A}$

the power set

Given a set A we can consider the set of all its subsets.

Definition

The power set of a set A is the set of all the subsets of A. The power set of A is denoted by $P(A)$ or 2^A.

Example

The power set of $A = \{1, 2, 4, 8\}$ is the set of all subsets of A, namely,

$$\begin{aligned} P(A) \;=\; & \{\emptyset, \{1\}, \{2\}, \{4\}, \{8\}, \\ & \{1,2\}, \{1,4\}, \{1,8\}, \{2,4\}, \{2,8\}, \{4,8\}, \\ & \{1,2,4\}, \{1,2,8\}, \{2,4,8\}, \{1,4,8\}, \\ & \{1,2,4,8\}\}. \end{aligned}$$

the power set (cont.)

Claim

- $B \in P(A)$ iff $B \subseteq A$.
- $\forall A : \emptyset \in P(A)$
- If A has n elements, then $P(A)$ has 2^n elements. (to be proved)

ordered pairs

We can pair elements together to obtain ordered pairs.

Definition

Two objects (possibly equal) with an order (i.e., the first object and the second object) are called an ordered pair.

- Notation: The ordered pair (a, b) means that a is the first object in the pair and b is the second object in the pair.
- Equality: Consider two ordered pairs (a, b) and (a', b'). We say that $(a, b) = (a', b')$ if $a = a'$ and $b = b'$.
- Coordinates: An ordered pair (a, b) has two coordinates. The first coordinate equals a, the second coordinate equals b.

ordered pairs (cont.)

Example

- names of people (first name, family name)
- coordinates of points in the plane (x, y).

Cartesian product

Definition

The Cartesian product of the sets A and B is the set

$$A \times B \triangleq \{(a, b) \mid a \in A \text{ and } b \in B\}.$$

Every element in a Cartesian product is an ordered pair. We abbreviate $A^2 \triangleq A \times A$.

Example

Let $A = \{0, 1\}$ and $B = \{1, 2, 3\}$. Then,

$$A \times B = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3)\}$$

Cartesian product (cont)

Example

The Euclidean plane is the Cartesian product $\mathbb{R}^2$. Every point in the plane has an x-coordinate and a y-coordinate. Thus, a point p is a pair (p_x, p_y). For example, the point $p = (1, 5)$ is the point whose x-coordinate equals 1 and whose y coordinate equals 5.

k-tuples

Definition

A k-tuple is a set of k objects with an order. This means that a k-tuple has k coordinates numbered $\{1, \ldots, k\}$. For each coordinate i, there is object in the ith coordinate.

Example

- An ordered pair is a 2-tuple.
- $(x_1, \ldots, x_k)$ where x_i is the element in the ith coordinate.
- Equality: compare in each coordinate, thus, $(x_1, \ldots, x_k) = (x'_1, \ldots, x'_k)$ if and only if $x_i = x'_i$ for every $i \in \{1, \ldots, n\}$.

k-tuples (cont.)

Definition

The Cartesian product of the sets $A_1, A_2, \ldots A_k$ is the set

$$A_1 \times A_2 \times \cdots \times A_k \triangleq \{(a_1, \ldots, a_k) \mid a_i \in A_i \text{ for every } 1 \leq i \leq k\}.$$

De Morgan's Law

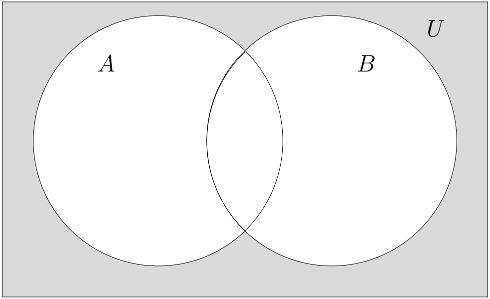


Figure: Venn diagram demonstrating the identity $U \setminus (A \cup B) = \bar{A} \cap \bar{B}$.

There is a second law:

$$U \setminus (A \cap B) = \bar{A} \cup \bar{B}.$$

relations

A set of ordered pairs is called a binary relation.

Definition

A subset $R \subseteq A \times B$ is called a *binary relation*.

Example

- Relation of games between teams in a soccer league. (Liverpool, Chelsea) means that Liverpool hosted the game. Thus the games (Liverpool,Chelsea) and (Chelsea,Liverpool) are different matches.
- Let $R \subseteq \mathbb{N} \times \mathbb{N}$ denote the binary relation "smaller than and not equal" over the natural number. That is, $(a, b) \in R$ if and only if $a < b$.

$$R \triangleq \{(0,1),(0,2),\ldots,(1,2),(1,3),\ldots\}.$$

functions

A function is a binary relation with an additional property.

Definition

A binary relation $R \subseteq A \times B$ is a function if for every $a \in A$ there exists a unique element $b \in B$ such that $(a, b) \in R$.

A function $R \subseteq A \times B$ is usually denoted by $R : A \to B$. The set A is called the domain and the set B is called the range. Lowercase letters are usually used to denote functions, e.g., $f : \mathbb{R} \to \mathbb{R}$ denotes a real function $f(x)$.

functions (cont.)

Consider relations $R_1, R_2, R_3, R_4 \subseteq \{0,1,2\} \times \{0,1,2\}$:

$$\begin{aligned} R_1 &\triangleq \{(1,1)\}\ , \\ R_2 &\triangleq \{(0,0),(1,1),(2,2)\}\ , \\ R_3 &\triangleq \{(0,0),(0,1),(2,2)\}\ , \\ R_4 &\triangleq \{(0,2),(1,2),(2,2)\}\ . \end{aligned}$$

Example

- The relation R_1 is not a function.
- R_2 is a function.
- The relation R_3 is not a function.
- The relation R_4 is a constant function.
- R_2 is the identity function.

function vs. relation

Example

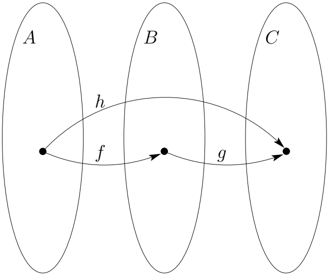
- M = set of mothers.
- C = set of children.
- $P \triangleq \{(m, c) \mid m \text{ is the mother of } c\}$.
- $Q \triangleq \{(c, m) \mid c \text{ is a child of } m\}$.
- $P \subseteq M \times C$ is a relation (usually not a function)
- $Q \subseteq C \times M$ is a function.

composition

Definition

Let $f : A \rightarrow B$ and $g : B \rightarrow C$ denote two functions. The *composed function* $g \circ f$ is the function $h : A \rightarrow C$ defined by $h(a) = g(f(a))$, for every $a \in A$.

Note that two functions can be composed only if the range of the first function is contained in the domain of the second function.



We can also define a function defined over a subset of a domain.

Lemma

Let $f : A \to B$ denote a function, and let $A' \subseteq A$. The relation $R \subseteq A' \times B$ defined by $R \triangleq \{(a, b) \in A' \times B \mid f(a) = b\}$ is a function.

Definition

Let $f : A \to B$ denote a function, and let $A' \subseteq A$. The *restriction* of f to the domain A' is the function $f' : A' \to B$ defined by $f'(x) \triangleq f(x)$, for every $x \in A'$.

strict containment:

$$A \subsetneq B \quad \Leftrightarrow \quad A \subseteq B \text{ and } A \neq B.$$

Definition

Suppose $A \subsetneq A'$ and $f : A \rightarrow B$. A function $g : A' \rightarrow B'$ is an extension of f if f is a restriction of g.

Consider a function $f : A \times B \rightarrow C$ for finite sets A and B.
The multiplication table of f is an $|A| \times |B|$ table. Entry (a, b) contains $f(a, b)$.

f	0	1	2
0	0	0	0
1	0	1	2
2	0	2	4

Table: The multiplication table of the function $f : \{0, 1, 2\}^2 \rightarrow \{0, 1, \ldots, 4\}$ defined by $f(a, b) = a \cdot b$.

Bits and Strings

Definition

A bit is an element in the set $\{0,1\}$.

$$\{0,1\}^n = \overbrace{\{0,1\} \times \{0,1\} \times \cdots \{0,1\}}^{n \text{ times}}.$$

Every element in $\{0,1\}^n$ is an n-tuple $(b_1, \ldots, b_n)$ of bits.

Definition

An n-bit binary string is an element in the set $\{0,1\}^n$.

We often denote a string as a list of bits. For example, $(0,1,0)$ is denoted by 010.

Bits and Strings (cont.)

Example

- $\{0,1\}^2 = \{00, 01, 10, 11\}$.
- $\{0,1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Boolean functions

Definition

A function $B : \{0,1\}^n \rightarrow \{0,1\}^k$ is called a Boolean function.

Truth values: "true" is 1 and "false" is 0.

Truth table: A list of the ordered pairs $(x, f(x))$.

Example

Truth table of the function $\textsc{not} : \{0,1\} \rightarrow \{0,1\}$:

x	$\textsc{not}(x)$
0	1
1	0

Important Boolean functions

Definition

- $\text{AND}(x,y) \triangleq \min\{x,y\}$.
- $\text{OR}(x,y) \triangleq \max\{x,y\}$.
- $\text{XOR}(x,y) \triangleq \begin{cases} 1 & if x \neq y \\ 0 & if x = y \end{cases}$

Truth tables:

x	y	$\text{AND}(x,y)$
0	0	0
1	0	0
0	1	0
1	1	1

x	y	$\text{OR}(x,y)$
0	0	0
1	0	1
0	1	1
1	1	1

x	y	$\text{XOR}(x,y)$
0	0	0
1	0	1
0	1	1
1	1	0

Important Boolean functions (cont.)

Truth tables:

x	y	$\text{AND}(x,y)$
0	0	0
1	0	0
0	1	0
1	1	1

x	y	$\text{OR}(x,y)$
0	0	0
1	0	1
0	1	1
1	1	1

x	y	$\text{XOR}(x,y)$
0	0	0
1	0	1
0	1	1
1	1	0

Multiplication tables:

AND	0	1
0	0	0
1	0	1

OR	0	1
0	0	1
1	1	1

XOR	0	1
0	0	1
1	1	0

Commutative Binary Operations

Definition

A function $f : A \times A \rightarrow A$ is a binary operation.

Usually, a binary operation is denoted by a special symbol (e.g., $+, -, \cdot, \div$). Instead of writing $+(a, b)$, we write $a + b$.

Definition

A binary operation $* : A \times A \rightarrow A$ is commutative if, for every $a, b \in A$:

$$a * b = b * a.$$

Example

- $x + y = y + x$
- $x \cdot y = y \cdot x.$
- $x - y \neq y - x.$

Associative Binary Operations

Definition

A binary operation $* : A \times A \to A$ is associative if, for every $a, b, c \in A$:
$$(a * b) * c = a * (b * c).$$

Example

- $(x + y) + z = x + (y + z)$
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
- $(x - y) - z \neq x - (y - z)$.

Associative $\not\Rightarrow$ Commutative

Multiplication of matrices is associative but not commutative:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

The products $A \cdot B$ and $B \cdot A$ are:

$$A \cdot B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad B \cdot A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Since $A \cdot B \neq B \cdot A$, multiplication of real matrices is not commutative.

Associative and Commutative

Claim

The Boolean functions OR, AND, XOR are commutative and associative.

a	b	c	AND(a, b)	AND(b, c)	AND(AND$(a, b), c)$	AND$(a,$ AND$(b, c))$
0	0	0	0	0	0	0
1	0	0	0	0	0	0
0	1	0	0	0	0	0
1	1	0	1	0	0	0
0	0	1	0	0	0	0
1	0	1	0	0	0	0
0	1	1	0	1	0	0
1	1	1	1	1	1	1

Table: An exhaustive proof that AND is associative

Boolean functions (cont.)

We can extend the AND and OR functions:

$$\text{AND}_3(X, Y, Z) \triangleq (X \text{ AND } Y) \text{ AND } Z.$$

Since the AND function is associative we have

$$(X \text{ AND } Y) \text{ AND } Z = X \text{ AND } (Y \text{ AND } Z).$$

Thus, we omit parenthesis and write X AND Y ANDZ.
Same holds for OR.