Digital Logic Design: a rigorous approach ©

Chapter 1: Sets and Functions

Guy Even Moti Medina

School of Electrical Engineering Tel-Aviv Univ.

June 15, 2020

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

Universal Sets

- Naive definition of sets fails due to paradoxes (Cantor, Russel). Beginning of 20th century: axiomatization of set theory (Zermelo-Fraenkel axioms).
- Bypass based on a universal set.

Definition

The universal set is a set that contains all the possible objects.

Example

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

What is a Set?

Definition

A set is a collection of objects from a universal set.

Specification

We denote the set of all elements in U that satisfy property P as follows

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

Notation: the symbol $\triangleq$

$\mathbb{N}^+ \triangleq \{n \in \mathbb{N} \mid n \geq 1\}$ means "$\mathbb{N}^+$ is defined be the set of all positive natural numbers". (Compare: $=$ and $\triangleq$)

Example

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

Set Notations

- Suppose $U \triangleq \mathbb{N}$.
- $A \triangleq \{1, 5, 12\}$ 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.
- $|A| = 3$.

Question

Is it true that $\{1, 5, 12\} = \{5, 12, 1\} = \{1, 1, 1, 12, 5\}$?

Equality and Containment

Definition

A is a subset of B if every element in A is also an element in B. Notation: $A \subseteq B$.

Definition

Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$. Notation: $A = B$.

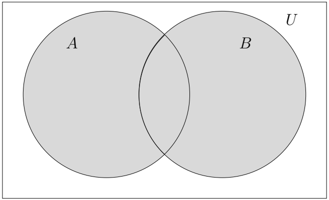
Definition (strict containment)

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

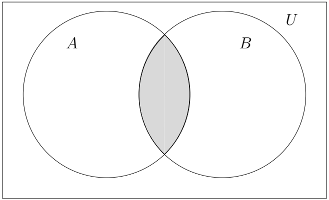
Example

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

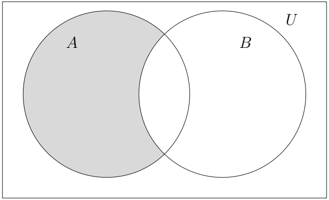
Venn diagrams



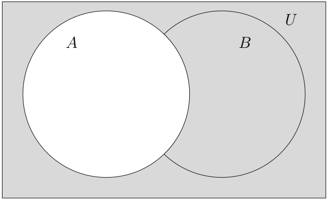
(a) Union: $A \cup B$



(b) Intersection: $A \cap B$



(c) Difference: $A \setminus B$



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

The Empty Set

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

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

The Power Set

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

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

The Power Set

Question

What is the power set of the empty set $P(\emptyset)$?

Question

What is the power set of the power set of the empty set $P(P(\emptyset))$?

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)

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.

ordered pairs (cont.)

Example

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

Equality: $(a, b) = (a', b')$ 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.

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

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

Riddle

Who invented the Cartesian product? (hint: same person invented analytic geometry)

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.

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.

Alternatively, a k-tuple is a sequence of k elements.

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 of all k-tuples $(a_1, \ldots, a_k)$, where $a_i \in A_i$.

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

If $A = A_1 = \cdots = A_k$, then we abbreviate:

$$A^k \triangleq A_1 \times A_2 \times \cdots \times A_k$$

Example

- $\mathbb{R}^3 =$ 3-dimensional Euclidean space
- $\mathbb{N}^{12} =$ all sequences of natural numbers that consist of 12 elements.

De Morgan's Law

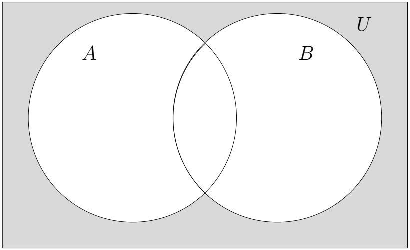


Figure: Venn diagram for $U \setminus (A \cup B) = \bar{A} \cap \bar{B}$.

Theorem (De Morgan's Laws)

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

To be proved in chapter on Propositional Logic...

Relations

Definition

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

Example

- Relation of matches between teams in a soccer league. (Liverpool, Chelsea) means that Liverpool hosted the match. Thus the matches (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

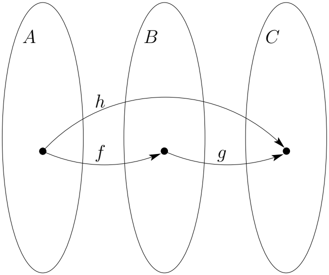
Example

- $M \triangleq$ set of mothers.
- $C \triangleq$ set of children.
- $P \triangleq \{(m, c) \mid m$ is the biological mother of $c\}$.
- $Q \triangleq \{(c, m) \mid c$ 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.

Definition

Let $f : A \to B$ and $g : B \to C$ denote two functions. The composed function $g \circ f$ is the function $h : A \to C$ defined by $h(a) \triangleq g(f(a))$, 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.



restricting the domain of a function

Lemma

Let $f : A \to B$ denote a function, and let $A' \subseteq A$. The relation $R \triangleq (A' \times B) \cap f$ is a function $R : A' \to B$.

R is called the restriction of f to the domain A'.

Extension of a Function

Definition

Let f and g denote two functions. g is an extension of f if $f \subseteq g$ (every ordered pair in f is also an ordered pair in g).

Claim

If $f : A \to B$ and g is an extension of f, then f is a restriction of g to the domain A.

Example

- $f : \mathbb{R} \times \{0\} \to \mathbb{R}$ defined by $f(x, 0) \triangleq |x|$.
- $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ defined by $g(x, y) \triangleq \sqrt{x^2 + y^2}$.

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

Example

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

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

Bits and Strings

Definition

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

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

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 $B : \{0,1\}^n \to \{0,1\}^k$ 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 $\textsc{not} : \{0,1\} \to \{0,1\}$:

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

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

Equivalent definitions

Claim

- $\textsc{not}(x) = 1 - x$.
- $\textsc{and}(x, y) = x \cdot y$.
- $\textsc{or}(x, y) = x + y - (x \cdot y)$.
- $\textsc{xor}(x, y) = \text{mod}((x + y), 2)$

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 $f : A \times A \to A$ 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 $* : A \times A \to A$ is commutative if, for every $a, b \in A$:

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

Example

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

Commutative Binary Operations

Definition

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

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

Riddle

Why do we care about commutative operations in a logic design course? (hint: Suppose we solder 2 wires to a gate, do we care which wire is soldered to which input?)

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 Binary Operations

Definition

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

$$(a * b) * c = a * (b * c).$$

Riddle

Why do we care about associative operations in a logic design course? (hint: using 2 gates to compute an operation over 3 bits.)

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.

Riddle

Find a Boolean binary function that commutative but not associative.

Associative and Commutative Boolean Functions

Question

Given a multiplication table of a binary operator $f : A \times A \to A$, how can we check that f is commutative? Is there in general a faster way than checking all pairs?

Question

Given a multiplication table of a binary operator $f : A \times A \to A$, how can we check that f is associative? Is there in general a faster way than checking all triples?

Question

Prove that both min and max are commutative and associative. What does this imply about AND and OR?

Associative and Commutative Boolean Functions

Claim

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

Proof.

Follows from the (algebraic) definitions of the functions. □

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 AND Z.
Same holds for OR.