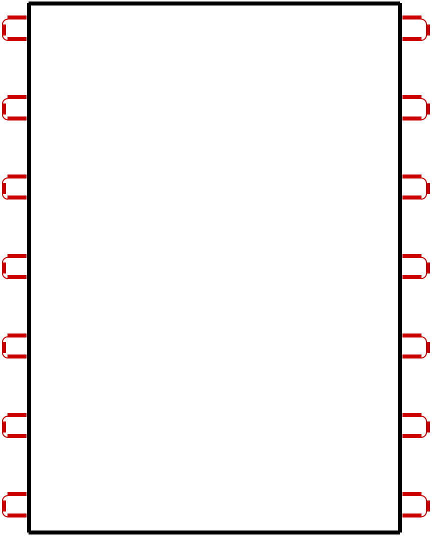
MATHEMATICS BEHIND CHIP

Branimir Šešelja
Department for Mathematics and Informatics
Faculty of Sciences, University of Novi Sad

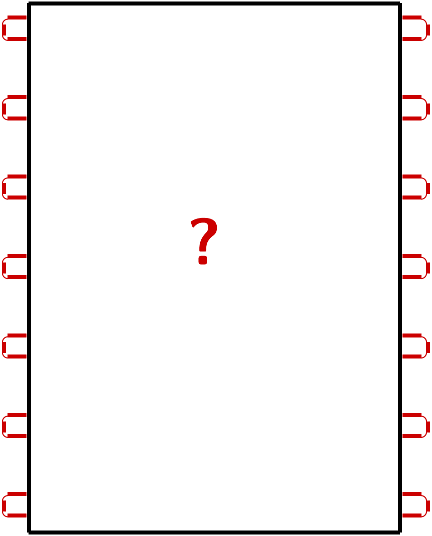
Teaching material

Chip from the outside

Chip from the outside



Chip from the outside



Digital technology

Zeroes and ones

$$\ldots \mathbf{011101010} \ldots \quad \mathbf{?} \rightarrow \mathbf{?} \quad \ldots \mathbf{011000110} \ldots$$

Power set

Power set

A - a set

Power set

A - a set

$\mathcal{P}(A) := \{X \mid X \subseteq A\}$

Power set

A - a set

$\mathcal{P}(A) := \{X \mid X \subseteq A\}$

$\mathcal{P}(A)$ is a collection of all subsets in A, it is called a **power set** of the set A.

Power set

A - a set

$\mathcal{P}(A) := \{X \mid X \subseteq A\}$

$\mathcal{P}(A)$ is a collection of all subsets in A, it is called a **power set** of the set A.

Relationship $\subseteq$ is said to be **inclusion**:

Power set

A - a set

$\mathcal{P}(A) := \{X \mid X \subseteq A\}$

$\mathcal{P}(A)$ is a collection of all subsets in A, it is called a **power set** of the set A.

Relationship $\subseteq$ is said to be **inclusion**:

$X \subseteq Y \Longleftrightarrow (\forall x)(x \in X \Rightarrow x \in Y)$

Examples

Examples

- $A = \{a, b\}$

Examples

- $A = \{a, b\}$
  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Examples

- $A = \{a, b\}$
  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $B = \{a, b, c\}$

Examples

- $A = \{a, b\}$
  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $B = \{a, b, c\}$
  $\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

Examples

- $A = \{a, b\}$
  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $B = \{a, b, c\}$
  $\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
- $\mathcal{P}(\emptyset) = ?$

Examples

- $A = \{a, b\}$
  $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $B = \{a, b, c\}$
  $\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
- $\mathcal{P}(\emptyset) =?$
  $\mathcal{P}(\emptyset) = \{\emptyset\}$

On a power set $\mathcal{P}(A)$ we define set operations:

On a power set $\mathcal{P}(A)$ we define set operations:

For $X, Y \subseteq A$

On a power set $\mathcal{P}(A)$ we define set operations:

For $X, Y \subseteq A$

$X \cap Y := \{x \mid x \in X \wedge x \in Y\}$ - **intersection**

On a power set $\mathcal{P}(A)$ we define set operations:

For $X, Y \subseteq A$

$X \cap Y := \{x \mid x \in X \wedge x \in Y\}$ - **intersection**

$X \cup Y := \{x \mid x \in X \vee x \in Y\}$ - **union**

On a power set $\mathcal{P}(A)$ we define set operations:

For $X, Y \subseteq A$

$X \cap Y := \{x \mid x \in X \wedge x \in Y\}$ - **intersection**

$X \cup Y := \{x \mid x \in X \vee x \in Y\}$ - **union**

$C_A(X) := A \setminus X = \{x \mid x \in A \wedge x \notin X\}$ - **complement** of X with respect to A

On a power set $\mathcal{P}(A)$ we define set operations:

For $X, Y \subseteq A$

$X \cap Y := \{x \mid x \in X \wedge x \in Y\}$ - **intersection**

$X \cup Y := \{x \mid x \in X \vee x \in Y\}$ - **union**

$C_A(X) := A \setminus X = \{x \mid x \in A \wedge x \notin X\}$ - **complement** of X with respect to A

It is also denoted by $C_A(X) = \overline{X}$.

Power set

Properties of set operations

$$(\mathcal{P}(A), \cap, \cup, ^{-}, \emptyset, A, \subseteq)$$

$$(\mathcal{P}(A), \cap, \cup, \bar{\ }, \emptyset, A, \subseteq)$$

Let $X, Y, Z \subseteq A$. Then:

$(\mathcal{P}(A), \cap, \cup, ^{-}, \emptyset, A, \subseteq)$

Let $X, Y, Z \subseteq A$. Then:

$$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$$

$(\mathcal{P}(A), \cap, \cup, ^{-}, \emptyset, A, \subseteq)$

Let $X, Y, Z \subseteq A$. Then:

$$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$$

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

$(\mathcal{P}(A), \cap, \cup, ^{-}, \emptyset, A, \subseteq)$

Let $X, Y, Z \subseteq A$. Then:

$$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$$

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$
$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

$(\mathcal{P}(A), \cap, \cup, ^-, \emptyset, A, \subseteq)$

Let $X, Y, Z \subseteq A$. Then:

$$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$$

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$
$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

$$X \cap X = X, \quad X \cup X = X$$

$(\mathcal{P}(A), \cap, \cup, ^{-}, \emptyset, A, \subseteq)$

Let $X, Y, Z \subseteq A$. Then:

$$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$$

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$
$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

$$X \cap X = X, \quad X \cup X = X$$

$$X \cap \overline{X} = \emptyset, \quad X \cup \overline{X} = A$$

$(\mathcal{P}(A), \cap, \cup, {}^{-}, \emptyset, A, \subseteq)$

Let $X, Y, Z \subseteq A$. Then:

$$X \cap Y = Y \cap X, \quad X \cup Y = Y \cup X$$

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$
$$X \cup (Y \cup Z) = (X \cup Y) \cup Z$$

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

$$X \cap X = X, \quad X \cup X = X$$

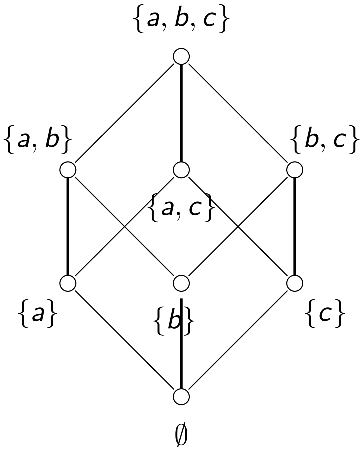
$$X \cap \overline{X} = \emptyset, \quad X \cup \overline{X} = A$$

$$X \cap A = X, \quad X \cup \emptyset = X.$$

Power set
Diagram

A power set can be represented by a diagram:

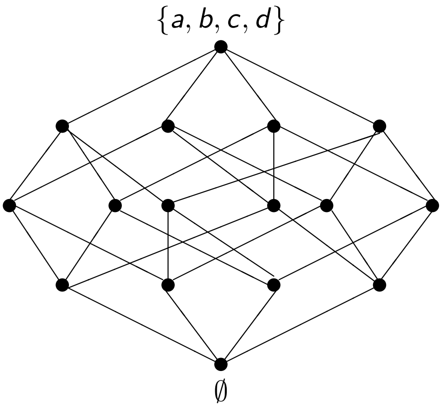
A power set can be represented by a diagram:



$(\mathcal{P}(\{a, b, c\}), \subseteq)$

Power set

Diagram



$(P(\{a, b, c, d\}), \subseteq)$

Boolean algebra

Boolean algebra

$\mathcal{B} = (B, \wedge, \vee, ', 0, 1),$

Boolean algebra

$\mathcal{B} = (B, \wedge, \vee, ', 0, 1)$,

B - a nonempty set, $\wedge$, $\vee$ - binary operations, $'$ - a unary operation, 0 and 1 - constants, and the following axioms hold:

Boolean algebra

$\mathcal{B} = (B, \wedge, \vee, {}', 0, 1)$,

B - a nonempty set, $\wedge$, $\vee$ - binary operations, $'$ - a unary operation, 0 and 1 - constants, and the following axioms hold:

b1: $x \wedge y = y \wedge x$
b2: $x \vee y = y \vee x$; (*commutativity laws*)

b3: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
b4: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ (*distributivity laws*)

b5: $x \wedge 1 = x$
b6: $x \vee 0 = x$ (*properties of* 0 *and* 1)

b7: $x \wedge x' = 0$
b8: $x \vee x' = 1$ (*properties of the complement operation*)

b9: $0 \neq 1$.

$\mathcal{B}_2 := (\{0,1\}, \wedge, \vee, {}', 0, 1)$ - a **two-element Boolean algebra**

$\mathcal{B}_2 := (\{0,1\}, \wedge, \vee, \,'\,, 0, 1)$ - a **two-element Boolean algebra**

	$'$
1	0
0	1

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

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

$\mathcal{B}_2 := (\{0,1\}, \wedge, \vee, {}', 0, 1)$ - a **two-element Boolean algebra**

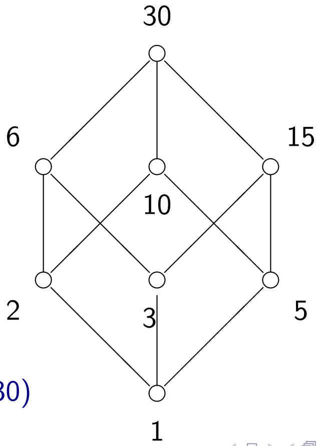
	$'$
1	0
0	1

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

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

Example with positive integers

Example with positive integers



$(D(30), gcd, lcm, 30/x, 1, 30)$

Language of Boolean algebras

Language of Boolean algebras

Boolean terms - definition:

Language of Boolean algebras

Boolean terms - definition:

- variables $x, y, z, \dots$ and constants $0, 1$ are Boolean terms;

Language of Boolean algebras

Boolean terms - definition:

- variables $x, y, z, \dots$ and constants $0, 1$ are Boolean terms;
- if A and B are Boolean terms, then also $(A \wedge B)$, $(A \vee B)$ are (A') Boolean terms;

Language of Boolean algebras

Boolean terms - definition:

- variables $x, y, z, \ldots$ and constants $0, 1$ are Boolean terms;
- if A and B are Boolean terms, then also $(A \wedge B)$, $(A \vee B)$ are (A') Boolean terms;
- Boolean terms are obtained only by the finite number of applications of the previous two rules.

Examples

Examples

- $x' \wedge (y \vee z')'$

Examples

- $x' \wedge (y \vee z')'$
- $(x \vee (y \wedge x'))' \vee z$

Examples

- $x' \wedge (y \vee z')'$
- $(x \vee (y \wedge x'))' \vee z$
- $1 \wedge x'$

Examples

- $x' \wedge (y \vee z')'$
- $(x \vee (y \wedge x'))' \vee z$
- $1 \wedge x'$
- $((u' \vee v)' \wedge (u' \wedge v')) \vee v$

Examples

- $x' \wedge (y \vee z')'$
- $(x \vee (y \wedge x'))' \vee z$
- $1 \wedge x'$
- $((u' \vee v)' \wedge (u' \wedge v')) \vee v$
- $(x_1 \wedge x_2' \wedge x_4') \vee (x_2' \wedge x_3 \wedge x_5) \vee (x_1 \wedge x_6')$

From sets to zeroes and ones:

From sets to zeroes and ones:

Characteristic function

From sets to zeroes and ones:

Characteristic function

A - set, $\quad B \subseteq A$

From sets to zeroes and ones:

Characteristic function

A - set, $\quad B \subseteq A$

$\mathcal{K}_B : A \to \{0, 1\}$

From sets to zeroes and ones:

Characteristic function

A - set, $\quad B \subseteq A$

$\mathcal{K}_B : A \to \{0,1\}$

Za $x \in A$

$$\mathcal{K}_B(x) := \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{if } x \notin B. \end{cases}$$

From sets to zeroes and ones:

Characteristic function

A - set, $\quad B \subseteq A$

$\mathcal{K}_B : A \to \{0,1\}$

Za $x \in A$

$$\mathcal{K}_B(x) := \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{if } x \notin B. \end{cases}$$

To each subset of A there corresponds a characteristic function and vice versa.

Example

Example

$$A = \{a, b, c, d\} \quad B = \{a, c\}$$

Example

$$A = \{a, b, c, d\} \qquad B = \{a, c\}$$

$$\mathcal{K}_B = \begin{pmatrix} a & b & c & d \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Example

$$A = \{a, b, c, d\} \qquad B = \{a, c\}$$

$$\mathcal{K}_B = \begin{pmatrix} a & b & c & d \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathcal{K}_\emptyset = \begin{pmatrix} a & b & c & d \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Example

$$A = \{a, b, c, d\} \qquad B = \{a, c\}$$

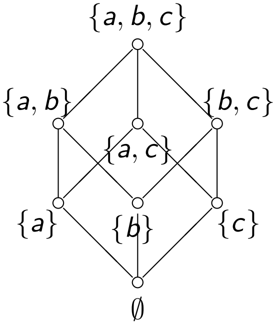
$$\mathcal{K}_B = \begin{pmatrix} a & b & c & d \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathcal{K}_\emptyset = \begin{pmatrix} a & b & c & d \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

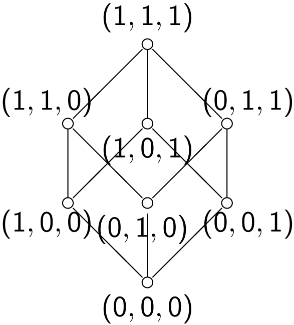
$$\mathcal{K}_A = \begin{pmatrix} a & b & c & d \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Boolean algebra of characteristic functions

Three-element set



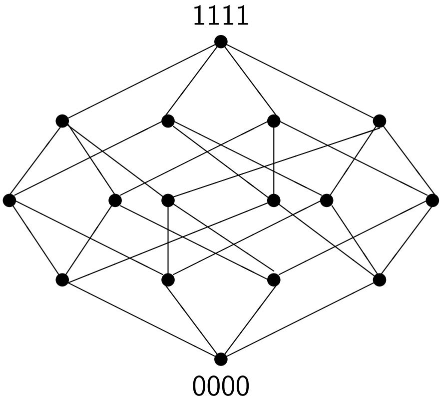
$\mathcal{P}(\{a, b, c\})$



$\{\mathcal{K}_X \mid X \subseteq \{a, b, c\}\}$

Boolean algebra of characteristic functions

Four-element set



$$\{\mathcal{K}_X \mid X \subseteq \{a, b, c, d\}\}$$

Boolean algebra of characteristic functions

Number of elements

There are as many characteristic functions on a set of n elements as there are subsets: 2^n.

There are as many characteristic functions on a set of n elements as there are subsets: 2^n*.*

$n = 1$ $\qquad$ $0 \quad 1$ $\qquad$ $2^1 = 2$

There are as many characteristic functions on a set of n elements as there are subsets: 2^n.

$n = 1$	$0 \quad 1$	$2^1 = 2$
$n = 2$	$\begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix} \qquad \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}$	$2^2 = 4$

There are as many characteristic functions on a set of n elements as there are subsets: 2^n.

$n = 1$	$0 \quad 1$	$2^1 = 2$
$n = 2$	$\begin{matrix} 0 & 0 & & 1 & 0 \\ 0 & 1 & & 1 & 1 \end{matrix}$	$2^2 = 4$
$n = 3$	$\begin{matrix} 0 & 0 & 0 & & 1 & 0 & 0 \\ 0 & 0 & 1 & & 1 & 0 & 1 \\ 0 & 1 & 0 & & 1 & 1 & 0 \\ 0 & 1 & 1 & & 1 & 1 & 1 \end{matrix}$	$2^3 = 8$

Boolean algebra of characteristic functions

Number of elements

$n = 4$

$n = 4$

0	0	0	0	1	1	0	0
0	0	0	1	1	1	0	1
0	0	1	0	1	1	1	0
0	0	1	1	1	1	1	1
0	1	0	0	1	1	0	0
0	1	0	1	1	1	0	1
0	1	1	0	1	1	1	0
0	1	1	1	1	1	1	1

$n = 4$

0	0	0	0		1	1	0	0
0	0	0	1		1	1	0	1
0	0	1	0		1	1	1	0
0	0	1	1		1	1	1	1
0	1	0	0		1	1	0	0
0	1	0	1		1	1	0	1
0	1	1	0		1	1	1	0
0	1	1	1		1	1	1	1

$2^4 = 16$

Words made of zeros and ones are used in digital technology.

Words made of zeros and ones are used in digital technology.

These are binary **codes**.

Words made of zeros and ones are used in digital technology.

These are binary **codes**.

Example of binary code:

Words made of zeros and ones are used in digital technology.

These are binary **codes**.

Example of binary code:

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{array}$$

Words made of zeros and ones are used in digital technology.

These are binary **codes**.

Example of binary code:

$$\begin{array}{cccc c cccc} 0 & 0 & 0 & 0 & \quad & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & \quad & 1 & 1 & 1 & 1 \end{array}$$

Single words are **code words**.

Counting with code words is performed coordinatewise, using two-element Boolean-algebra operations:

$\mathcal{B}_2 = (\{0, 1\}, \wedge, \vee, \,'\, , 0, 1).$

Counting with code words is performed coordinatewise, using two-element Boolean-algebra operations:

$$\mathcal{B}_2 = (\{0,1\}, \wedge, \vee, {}', 0, 1).$$

	$'$
1	0
0	1

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

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

Example

Example

$$\varphi : \{0,1\}^3 \to \{0,1\}$$

x	y	z	$\varphi(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Example

$\varphi : \{0,1\}^3 \to \{0,1\}$

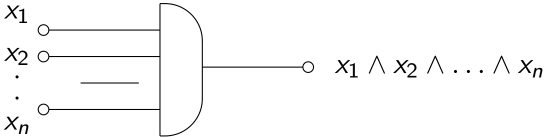
x	y	z	$\varphi(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

$$f(x,y,z) = (x' \wedge y' \wedge z') \vee (x' \wedge y \wedge z) \vee (x \wedge y' \wedge z).$$

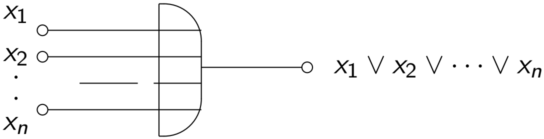
Logical circuits

Logical circuits

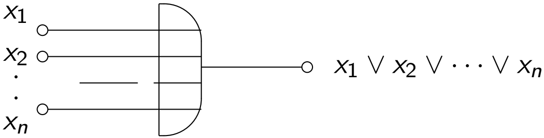
AND-gate:



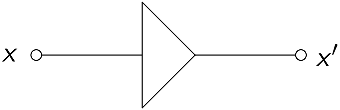
OR-gate:



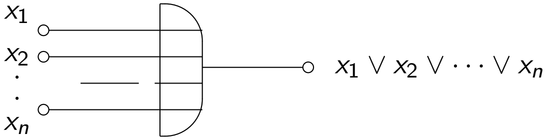
OR-gate:



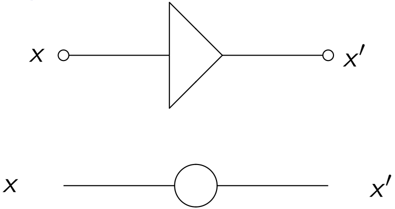
Inverter or **NOT-gate**:



OR-gate:



Inverter or **NOT-gate**:



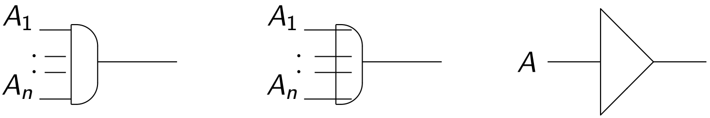
Definition of a **logical circuit**:

Definition of a **logical circuit**:

- Gates (AND, OR and NOT) are logical circuits;

Definition of a **logical circuit**:

- Gates (AND, OR and NOT) are logical circuits;
- If A, A_1, $A_2, \dots,$ A_n are logical circuits, then also objects connected by gates as presented are logical circuits.

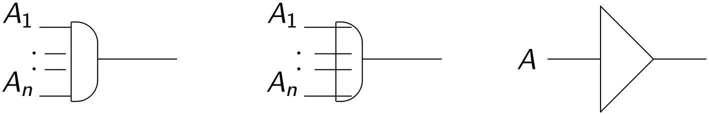


Boolean functions

Logical circuits

Definition of a **logical circuit**:

- Gates (AND, OR and NOT) are logical circuits;
- If A, A_1, A_2, . . . , A_n are logical circuits, then also objects connected by gates as presented are logical circuits.



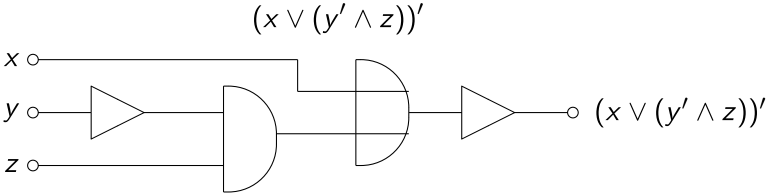
- Logical circuits are obtained only by a finite number of application of the previous two rules.

Example

Example

$$(x \vee (y' \wedge z))'$$

Example



Half adder and adder

Half adder and adder

Addition of numbers represented in binary system;
two single-digit binary numbers:

Half adder and adder

Addition of numbers represented in binary system;
two single-digit binary numbers:

x	y	$x \oplus y$	r
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Half adder and adder

Addition of numbers represented in binary system;
two single-digit binary numbers:

x	y	$x \oplus y$	r
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

$$x \oplus y = (x \vee y) \wedge (x \wedge y)' \quad \text{and} \quad r = x \wedge y.$$

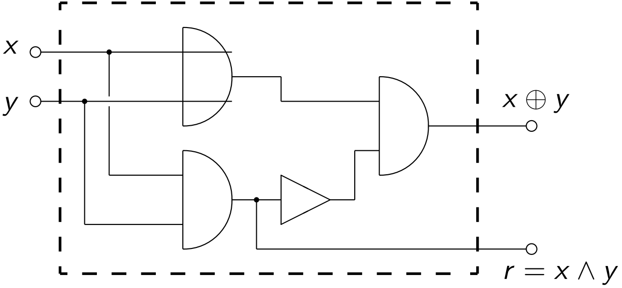
Half adder

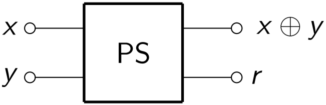
Half adder

$$x \oplus y = (x \vee y) \wedge (x \wedge y)' \qquad r = x \wedge y$$

Half adder

$$x \oplus y = (x \vee y) \wedge (x \wedge y)' \qquad r = x \wedge y$$





Addition of numbers represented in binary system;
three single-digit binary numbers::

Addition of numbers represented in binary system;
three single-digit binary numbers::

x	y	z	$x \oplus y \oplus z$	R
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Addition of numbers represented in binary system;
three single-digit binary numbers::

x	y	z	$x \oplus y \oplus z$	R
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$$R = (x' \wedge y \wedge z) \vee (x \wedge y' \wedge z) \vee (x \wedge y \wedge z') \vee (x \wedge y \wedge z) =$$

Addition of numbers represented in binary system;
three single-digit binary numbers::

x	y	z	$x \oplus y \oplus z$	R
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$$R = (x' \wedge y \wedge z) \vee (x \wedge y' \wedge z) \vee (x \wedge y \wedge z') \vee (x \wedge y \wedge z) =$$
$$(x \wedge y) \vee (z \wedge ((x' \wedge y) \vee (x \wedge y')))$$

Addition of numbers represented in binary system;
three single-digit binary numbers::

x	y	z	$x \oplus y \oplus z$	R
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$R = (x' \wedge y \wedge z) \vee (x \wedge y' \wedge z) \vee (x \wedge y \wedge z') \vee (x \wedge y \wedge z) =$
$(x \wedge y) \vee (z \wedge ((x' \wedge y) \vee (x \wedge y')))$
$(x' \wedge y) \vee (x \wedge y') = x \oplus y \quad ; \quad x \wedge y = r,$

Addition of numbers represented in binary system;
three single-digit binary numbers::

x	y	z	$x \oplus y \oplus z$	R
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$R = (x' \wedge y \wedge z) \vee (x \wedge y' \wedge z) \vee (x \wedge y \wedge z') \vee (x \wedge y \wedge z) =$
$(x \wedge y) \vee (z \wedge ((x' \wedge y) \vee (x \wedge y')))$
$(x' \wedge y) \vee (x \wedge y') = x \oplus y \quad ; \quad x \wedge y = r,$
$R = r \vee (z \wedge (x \oplus y))$; r - reminder, transfer.

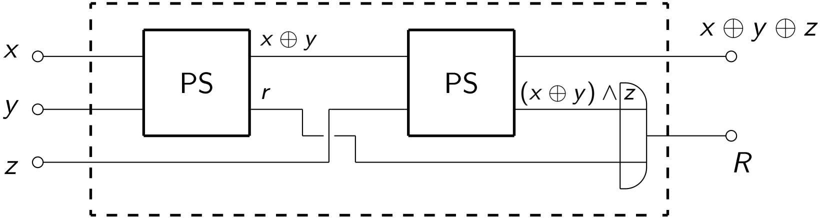
Adder

Adder

$$r = x \wedge y \quad R = r \vee (z \wedge (x \oplus y))$$

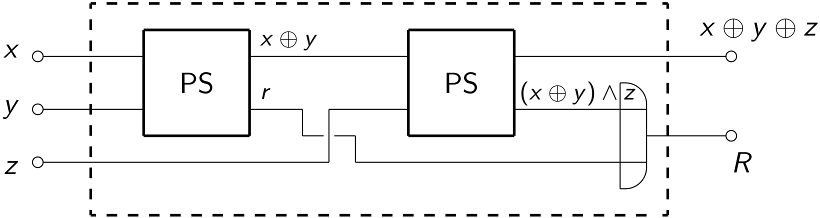
Adder

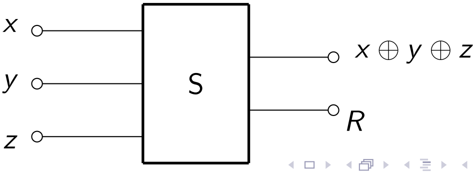
$$r = x \wedge y \quad R = r \vee (z \wedge (x \oplus y))$$



Adder

$$r = x \wedge y \quad R = r \vee (z \wedge (x \oplus y))$$





Example

Example

Construction of a logical circuit for the addition of three two-digit binary numbers.

Example

Construction of a logical circuit for the addition of three two-digit binary numbers.

$$
\begin{array}{cccc}
 & & a_1 & a_0 \\
 & & b_1 & b_0 \\
 & \oplus & c_1 & c_0 \\
\hline
d_3 & d_2 & d_1 & d_0
\end{array}
$$

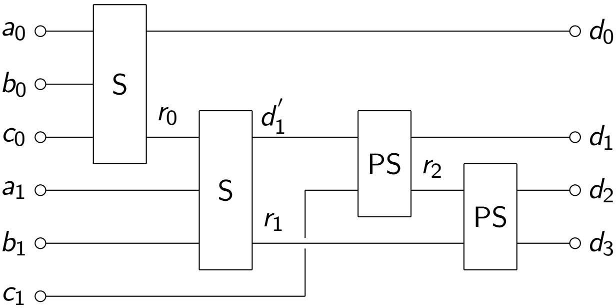
Example

Construction of a logical circuit for the addition of three two-digit binary numbers.

$$\begin{array}{cccc} & & a_1 & a_0 \\ & & b_1 & b_0 \\ & \oplus & c_1 & c_0 \\ \hline d_3 & d_2 & d_1 & d_0 \end{array}$$

Algorithm for the addition:

$$\begin{array}{rcll} a_0 \oplus b_0 \oplus c_0 & = & d_0 & \qquad \text{(transfer } r_0\text{)} \\ r_0 \oplus a_1 \oplus b_1 & = & d_1' & \qquad \text{(transfer } r_1\text{)} \\ d_1' \oplus c_1 & = & d_1 & \qquad \text{(transfer } r_2\text{)} \\ r_1 \oplus r_2 & = & d_2 & \qquad \text{(transfer } d_3\text{)} \end{array}$$



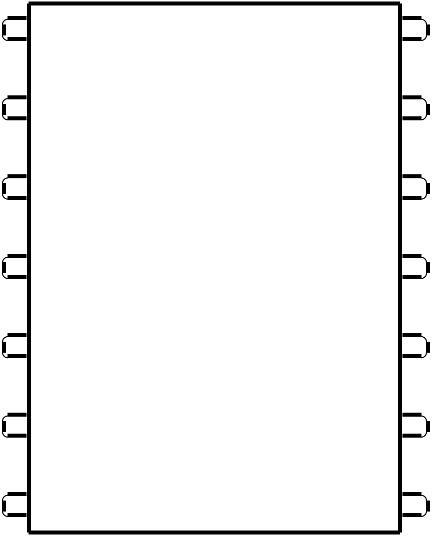
a_0
b_0
c_0
a_1
b_1
c_1
S
r_0
S
d_1'
r_1
PS
r_2
PS
d_0
d_1
d_2
d_3

Back to beginning

Chip from the inside

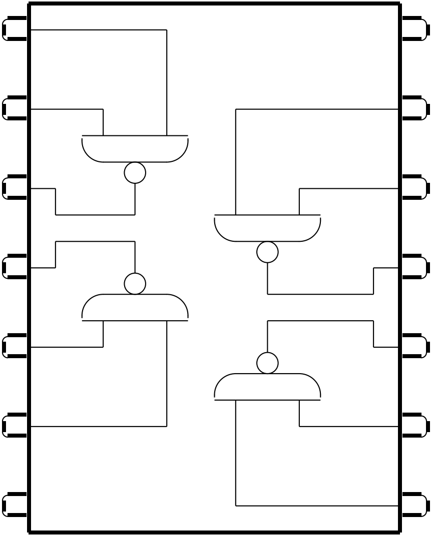
Back to beginning

Chip from the inside



Back to beginning

Chip from the inside



Field GF(2)

Field GF(2)

G*alois* **F***ield (E. Galois, French mathematician, 1811-1832.)*

Field GF(2)

G*alois* **F***ield (E. Galois, French mathematician, 1811-1832.)*

Operation $\oplus$ and $\cdot$ on the set $\{0, 1\}$, represented by tables:

Field GF(2)

***G**alois **F**ield (E. Galois, French mathematician, 1811-1832.)*

Operation $\oplus$ and $\cdot$ on the set $\{0, 1\}$, represented by tables:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Field GF(2)

***G**alois **F**ield (E. Galois, French mathematician, 1811-1832.)*

Operation $\oplus$ and $\cdot$ on the set $\{0, 1\}$, represented by tables:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

The structure $(\{0, 1\}, \oplus, \cdot)$ *is a field.*

Field GF(2)

G*alois* **F***ield (E. Galois, French mathematician, 1811-1832.)*

Operation $\oplus$ and $\cdot$ on the set $\{0, 1\}$, represented by tables:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

The structure $(\{0, 1\}, \oplus, \cdot)$ *is a field.*

When applied, field operations are performed faster then Boolean algebra operations.