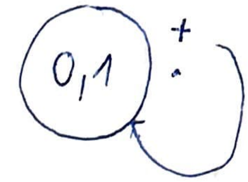
12. 3. 2025

22. Booleova algebra a její využití

- základ počítačových věd
- snažil pracovat s logickými výrazy jako s matematickými (před tím jen filosofie)

tautologie, kontingence, kontradikce

Logická hodnota = základní prvek B.a. představuje pravdivostní stav výroku či signálu
- nabývá 2 stavů: 0 – nepravda
  1 – pravda



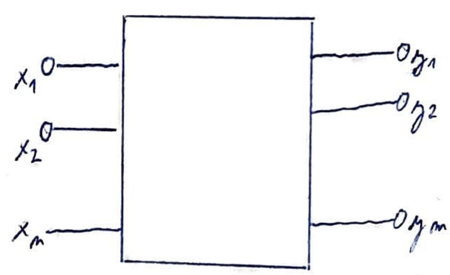
Logická proměnná = je symbol, který nabývá (0 nebo 1), v log. funkcích označení jako A, B, C...
- v praxi reprezentují vstupní a výstupní signály v digitálních obvodech (drát, rádio)
  [illegible]

Logická funkce = je obecné funkce – zobrazení, které n-tici nezávislých logických proměnných x_i zobrazuje na m-tici stavů závislé proměnných y_j

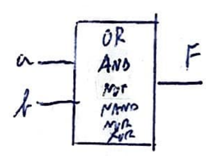
$$x_1, x_2, \dots, x_n \to y_1, y_2, \dots, y_m$$

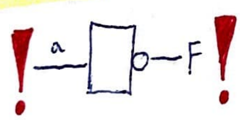
- lze poskládat z jednoduchých funkcí

$$y_j = f_j(x_1, x_2, \dots, x_n)$$



- **Logický součet** ⇒ Disjunkce, NEBO, **OR** $(\vee, +)$
- **Logický součin** ⇒ Konjunkce, A, **AND** $(\wedge, \cdot)$
- **Negace logické proměnné** ⇒ NE, **NOT** $(\neg a, \bar{a})$





- všechny logické funkce 2 a více proměnných lze vyjádřit jako: – součet součinů
  – součin součtů

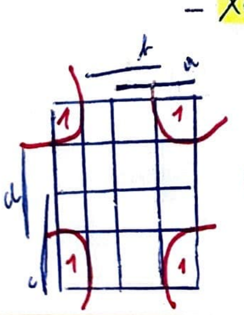
⇒ **DNF = Disjunktní forma** $(A \wedge \neg B) \vee (\neg A \wedge B)$
↳ Disjunctive Normal form

⇒ **CNF = Konjunktní forma** $(A \vee \neg B) \wedge (\neg A \vee B)$
↳ Conjunctive Normal form

$\{\wedge ; \neg\}$ funkcionálně kompletní
↳ lze jím realizovat libovolnou NAND logickou funkci

- **NAND** – negace logického součinu $(F = \overline{a \cdot b},\ F = \overline{a \wedge b},\ F = \overline{ab})$
- **NOR** – negace logického součtu $(F = \overline{a + b},\ F = \overline{a \vee b})$
- **XOR** – exclusive OR $(F = \bar{a}b + a\bar{b},\ F = a \oplus b,\ F = a \not\equiv b)$
  ↳ součet modulo 2

a	b	NAND	NOR	XOR
0	0	1	1	0
0	1	1	0	1
1	0	1	0	1
1	1	0	0	0



$\Rightarrow \bar{b}\bar{d}$

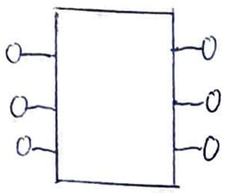
Logické konstanty = hodnoty, jichž mohou nabývat logické proměnné (0,1 => false, true)

Logický obvod = je fyzická realizace logické funkce pomocí logických členů (hradla)

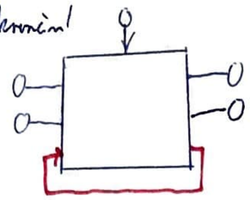
NEBO definice Moodle:

- Fyzikální systém, v nějž hodnoty vstupní, výstupní či vnitřní fyzikální veličiny nabývají v ustáleném stavu pouze dvou, jasně rozlišitelných, diskrétních hodnot
- typy: - **Kombinační** - realizují logickou funkci vstupních proměnných
  - **Sekvenční** - realizují logickou funkci vstupních proměnných a předchozích stavů (analogie s iteračním výpočtem)
    ↳ FEEDBACK LOOP (uchovávání předchozí stav => výsledek závisí i na předchozím stavu)

Kombinační



Sekvenční



Logický člen (hradlo) = Elementární zařízení, které realizuje elementární logickou funkci v číslicových počítačích nebo jiných číslicových zařízeních (např. AND, OR, NOT, ...)

- jsou základními stavebními prvky všech složitějších počítačových obvodů
- realizovány pomocí obvodů a tranzistorů

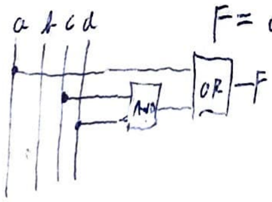
Vyjadřování logických funkcí

- pravdivostní tabulka (bitová na dálky)
- logické mapy => Karnaughova mapa, (Vennův diagram)
- rovnice => např. $F = A \cdot B + \bar{C}$

$F = a + ac + \bar{a}\bar{b}cd + bcd + cd$

$\Downarrow$

$F = a + cd$



		b	a
0	0	1	1
0	0	1	1
1	1	1	1
0	0	1	1

(d – 2. a 3. řádek, c – 3. a 4. řádek)

Karnaughova mapa

=> TOROID = donut

- vychází z Vennova diagramu
- matice logických stavů
- slouží pro minimalizaci
  ↳ levnější, rychlejší obvody
  ↳ co nejmenší počet co největších smyček

realizují sousední a pravidelné plochy o velikosti mocniny čísla 2

Udělej negaci této funkce

$F = a\bar{b} + c + (\bar{a} + bc)$

$\bar{F} = \overline{a\bar{b} + c + (\bar{a} + bc)}$

$\bar{F} = \neg((a \wedge \neg(\neg b \vee c)) \vee (\neg a \vee (b \wedge c)))$

$\bar{F} = \neg(a \wedge (b \wedge c)) \wedge \neg(\neg a \vee (b \wedge c))$

$\bar{F} = (\neg a \vee \neg(b \wedge c)) \wedge (a \wedge \neg(b \wedge c))$

$\bar{F} = (\neg a \vee \neg b \vee \neg c) \wedge (a \wedge (\neg b \vee \neg c))$

pokud $\bar{F}$ => vyjádřím nejdříve 0 a pak 1

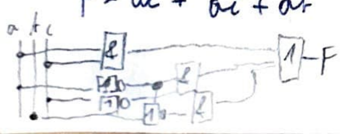
$F = ac + abc + \bar{a}b\bar{c} + \bar{a}\bar{b}\bar{c} + \bar{a}\bar{b}c$

POZOR JEN 3 PROMĚNNÉ

		b	a
1	1		
1		1	1

(c – 2. řádek)

$F = ac + \bar{a}\bar{c} + \bar{a}\bar{b}$



Jestli dosadím hodnoty: $a=0$, $b=0$, $c=1$

$F = a\bar{b} + \bar{c} + (\bar{a} + bc)$

$(0 \wedge 1 \wedge (1 \vee 0)) \vee (1 \vee (0 \wedge 1)) \Rightarrow 0 \vee 1 \Rightarrow \underline{1}$

$p \to q \equiv \neg p \vee q$

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

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

$p \oplus q = (p \vee q) \wedge \neg(p \wedge q)$

$p \wedge \mathbb{F} = \mathbb{F}$

$p \vee \mathbb{T} = \mathbb{T}$

2

! PRIORITIES !

1. ()
2. $\neg$
3. $\wedge$
4. $\vee$
5. $\Rightarrow$
6. $\Leftrightarrow$

Double negation	$\neg(\neg p) \equiv p$
Excluded middle	$p \vee \neg p \equiv \mathbb{T}$
Contradiction	$p \wedge \neg p \equiv \mathbb{F}$
Identity laws	$\mathbb{T} \wedge p \equiv p$ $\mathbb{F} \vee p \equiv p$
Idempotent laws	$p \wedge p \equiv p$ $p \vee p \equiv p$
Commutative laws	$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$
Associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
DeMorgan's laws	$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q)$ $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$

Figure 2.2: *Laws of Boolean Algebra. These laws hold for any propositions p, q, and r.*

! 2^n řádků v pravdivostní tabulce při n proměnných !

"has the same value as, no matter what logical values p, q, and r have".

2.2.1 Basics of Boolean Algebra

Many of the rules of Boolean algebra are fairly obvious, if you think a bit about what they mean. Even those that are not obvious can be verified easily by using a truth table. Figure 2.2 lists the most important of these laws. You will notice that all these laws, except the first, come in pairs: each law in the pair can be obtained from the other by interchanging $\wedge$ with $\vee$ and $\mathbb{T}$ with $\mathbb{F}$. This cuts down on the number of facts you have to remember.[6]

Just as an example, let's verify the first rule in the table, the Law of Double Negation. This law is just the old, basic grammar rule that two neg-

[6] It is also an example of a more general fact known as *duality*, which asserts that given any tautology that uses only the operators $\wedge$, $\vee$, and $\neg$, another tautology can be obtained from it by interchanging $\wedge$ with $\vee$ and $\mathbb{T}$ with $\mathbb{F}$. We won't attempt to prove this here, but we encourage you to try it!

2.2 Boolean Algebra

25. 2. 2025

1)

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

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

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

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$(p \vee q)$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

2)

a) $\neg(p \wedge q) \not\equiv (\neg p) \wedge (\neg q)$

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$
0	0	0	1	1	1	1
0	1	0	1	1	0	0
1	0	0	1	0	1	0
1	1	1	0	0	0	0

b) $\neg(p \vee q) \not\equiv (\neg p) \vee (\neg q)$

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
0	0	0	1	1	1	1
0	1	1	0	1	0	1
1	0	1	0	0	1	1
1	1	1	0	0	0	0

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

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$(\neg p) \vee (\neg q)$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

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

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

3)

a) $\neg(p \to q) \not\equiv (\neg p) \to (\neg q)$

p	q	$p \to q$	$\neg(p \to q)$	$\neg p$	$\neg q$	$(\neg p) \to (\neg q)$
0	0	1	0	1	1	1
0	1	1	0	1	0	0
1	0	0	1	0	1	1
1	1	1	0	0	0	1

b) $\neg(p \to q) \not\equiv (\neg p) \to q$

p	q	$p \to q$	$\neg(p \to q)$	$\neg p$	$(\neg p) \to q$
0	0	1	0	1	0
0	1	1	0	1	1
1	0	0	1	0	1
1	1	1	0	0	1

c) $\neg(p \to q) \not\equiv p \to (\neg q)$

p	q	$p \to q$	$\neg(p \to q)$	$\neg q$	$p \to (\neg q)$
0	0	1	0	1	1
0	1	1	0	0	1
1	0	0	1	1	1
1	1	1	0	0	0

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

4)

Is $\neg(p \leftrightarrow q)$ logically equivalent to $(\neg p) \leftrightarrow (\neg q)$? **NO**

p	q	$p \leftrightarrow q$	$\neg(p \leftrightarrow q)$	$\neg p$	$\neg q$	$(\neg p) \leftrightarrow (\neg q)$
0	0	1	0	1	1	1
0	1	0	1	1	0	0
1	0	0	1	0	1	0
1	1	1	0	0	0	1

dosazení ⇒ logická metoda

$p = q = 0 \Rightarrow$ false $\not\equiv$ true

5)

In the algebra of numbers:

distributive law of multiplication over addition: $x(y+z) = xy + xz$

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

↳ boolean algebra

$x = 2$

$y = 3$

$z = 4$

$2(3+4) = 2 \cdot 3 + 2 \cdot 4$

$14 = 14$

It is valid in the algebra of numbers.

25.2.2025

2.2. Boolean algebra

6) The right distributive laws

$(p \lor q) \land r \equiv (p \land r) \lor (q \land r)$

$(p \land q) \lor r \equiv (p \lor r) \land (q \lor r)$

Show they are valid laws of Boolean algebra.

$p = 0$, $q = 0$, $r = 0$

$(0 \lor 0) \land 0 \equiv (0 \land 0) \lor (0 \land 0)$

$0 \land 0 \equiv 0 \lor 0$

$0 \equiv 0$

$(0 \land 0) \lor 0 \equiv (0 \lor 0) \land (0 \lor 0)$

$0 \lor 0 \equiv 0 \land 0$

$0 \equiv 0$

7) show that $p \land (q \lor r \lor s) \equiv (p \land q) \lor (p \land r) \lor (p \land s)$

$p \land (q \lor r \lor s) \equiv p \land ((q \lor r) \lor s)$

$\equiv (p \land (q \lor r)) \lor (p \land s)$

$\equiv (p \land q) \lor (p \land r) \lor (p \land s)$

8) $p \land \mathbb{F} = \mathbb{F}$

$p \lor \mathbb{T} = \mathbb{T}$

p	$p \land F$
0	0
1	0

p	$p \lor \mathbb{T}$
0	1
1	1

9) **a)** $p \land (q \land p)$, $p \land q$

$p \land (q \land p) \equiv p \land q \land p$

idempotent $\equiv (p \land p) \land q$

$\equiv p \land q$

b) $(\lnot p) \rightarrow q$, $p \lor q$

$(\lnot p) \rightarrow q \equiv \lnot(\lnot p) \lor q$

double negation $\equiv p \lor q$

c) $(p \lor q) \land \lnot q$, $p \land \lnot q$

$(p \lor q) \land \lnot q \equiv (p \land \lnot q) \lor (q \land \lnot q)$

distribution $\equiv (p \land \lnot q) \lor F$ excluded middle contradiction

$\equiv p \land \lnot q$

d) $p \rightarrow (q \rightarrow r)$, $(p \land q) \rightarrow r$

$p \rightarrow (q \rightarrow r) \equiv \lnot p \lor (\lnot q \lor r)$

DE MORGANŮV ZÁKON $\equiv \boxed{\lnot p \lor \lnot q} \lor r$

$\equiv \lnot(p \land q) \lor r$

$\equiv (p \land q) \rightarrow r$

e) $(p \rightarrow r) \land (q \rightarrow r)$, $(p \lor q) \rightarrow r$

$(p \rightarrow r) \land (q \rightarrow r) \equiv (\lnot p \lor r) \land (\lnot q \lor r)$ distribution

$\equiv r \lor (\lnot p \land \lnot q)$ de morgan

$\equiv \lnot(p \lor q) \lor r$

$\equiv (p \lor q) \rightarrow r$

f) $p \rightarrow (p \land q)$, $p \rightarrow q$

$p \rightarrow (p \land q) \equiv \lnot p \lor (p \land q)$ distribution

$\equiv (\lnot p \lor p) \land (\lnot p \lor q)$ excluded middle contradiction

$\equiv \mathbb{T} \land (\lnot p \lor q)$ identity

$\equiv \lnot p \lor q$

$\equiv p \rightarrow q$

10) Simplify as much as possible

excluded middle contradiction

a) $(p \land q) \lor \lnot q \equiv (p \lor \lnot q) \land \boxed{q \lor \lnot q}$ distribution

$\equiv (p \lor \lnot q) \land \mathbb{T}$ identity

$\equiv p \lor \lnot q$

$\equiv \lnot q \lor p$

$\equiv q \rightarrow p$

b) $\lnot(p \lor q) \land p \equiv ((\lnot p) \land (\lnot q)) \land p$ de morgan

$\equiv (\lnot p \land p) \land (\lnot q \land p)$ distribution ex. m. contradiction

$\equiv F \land (\lnot q \land p)$ log.

$\equiv F$

c) $p \rightarrow \lnot p \equiv \lnot p \lor \lnot p$ idempotent

$\equiv \lnot p$

d) $\lnot p \land (p \lor q) \equiv (\lnot p \land p) \lor (\lnot p \land q)$ distribution ex. m. contradiction

$\equiv F \lor (\lnot p \land q)$ identity

$\equiv \lnot p \land q$

e) $(q \land p) \rightarrow p \equiv \lnot(q \land p) \lor p$ distribution

$\equiv ((\lnot q) \lor (\lnot p)) \lor p$

$\equiv ((\lnot q) \lor p) \lor ((\lnot p) \lor p)$ ex. m. contradiction

$\equiv ((\lnot q) \lor p)) \lor \mathbb{T}$ log.

$\equiv \mathbb{T}$

f) $(p \rightarrow q) \land (\lnot p \rightarrow q) \equiv ((\lnot p) \lor q) \land (p \lor q)$ distribution

$\equiv q \lor ((\lnot p) \land p)$ ex. m. contradiction

$\equiv q \lor F$ identity

$\equiv q$