Tautologie: $\varphi \in \mathcal{L}(\mathcal{P})$

$\models \varphi$ jeśli dla dowolnej wartościowania $\pi : \mathcal{P} \to \{0, 1\}$

mamy $\widetilde{\pi}(\varphi) = 1$,

uwaga: $\top$ $\quad \pi(\top) = 1$ $\quad$ true

$\bot$ $\quad \pi(\bot) = 0$ $\quad$ false

① $\models (\neg(\neg p)) \leftrightarrow p$ $\quad$ prawo podwójnego negacji

$\models p \vee (\neg p)$ $\quad$ prawo wyłączonego środka

$\models \neg(p \wedge \neg p)$

Oznaczenie: $\varphi \equiv \psi$ oznacza $\models (\varphi \leftrightarrow \psi)$

Uwaga: $\varphi \equiv \psi$ gdy dla dowolnej wartościowania $w : \mathcal{P} \to \{0,1\}$ mamy $\pi(\varphi) = \pi(\psi)$

(1°) $\neg(\neg p) \equiv p$ $\quad \models (\neg(\neg p) \leftrightarrow p)$

$p \vee \neg p \equiv \top$ $\quad \models p \vee \neg p$

$p \wedge \neg p \equiv \bot$ $\quad \models \neg(p \wedge \neg p)$

W1. 1) $\varphi \equiv \varphi$ (zwrotność)

2) jeśli $\varphi \equiv \psi$ to $\psi \equiv \varphi$. (symetria)

3) jeśli $\varphi \equiv \psi$ i $\psi \equiv \eta$ to $\varphi \equiv \eta$ (przechodniość)

(2)
$$\left.\begin{array}{l} p \vee q \equiv q \vee p \\ p \wedge q \equiv q \wedge p \end{array}\right\} \text{przemienność}$$

$$\left.\begin{array}{l} p \vee p \equiv p \\ p \wedge p \equiv p \end{array}\right\} \text{idempotentność}$$

Uwaga: $x \# y \equiv x^y$ (w $\mathbb{R}$)

$2^3 \neq 3^2$ $\quad (2 \# 3) \neq (3 \# 2)$

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

Uwaga: $\circ$ - łączne

$(x \circ y) \circ (z \circ u) = (x \circ y) \circ a = x \circ (y \circ a)$

$a = x \circ (y \circ (z \circ u))$

$(x \circ (y \circ z)) \circ u = \ldots = x \circ (y \circ (z \circ u))$

$x \circ (y \circ (z \circ u)) = x \circ y \circ z \circ u$

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

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

rozdzielność

rozdzielność

$x \cdot (y + z) = x \cdot y + x \cdot z$

R

③ $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$

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

} prawa de Morgana

④ $\neg((\neg p) \wedge (\neg q)) \equiv (\neg(\neg p)) \vee (\neg(\neg q)) \equiv p \vee q$

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

④ $\underbrace{(p \to q)}_{L} \equiv \underbrace{(\neg p \vee q)}_{P}$ prawo eliminacji implikacji

L jest fałszywe iff $\pi(p) = 1$ i $\pi(q) = 0$

P jest fałszywe iff $\pi(\neg p) = 0$ i $\pi(q) = 0$

iff $\pi(p) = 1$ i $\pi(q) = 0$

⑤ $\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv (\neg\neg p) \wedge \neg q \equiv p \wedge \neg q$

⑤ $(p \leftrightarrow q) \equiv \big((p \to q) \wedge (q \to p)\big)$ prawo eliminacji równoważności

iff ≡ if and only if

WNIOSEK: Układ $\{\neg, \wedge\}$ wystarcza do zdefiniowania pozostałych spójn. logicznych.

Zadanie: $p \uparrow q \overset{def}{\equiv} (\neg p) \wedge (\neg q)$

↑ wystarcza do zdef. pozostałych spójników.

p	q	$p \uparrow q$
1	1	0
1	0	0
0	1	0
0	0	1

Uwaga: $\models (p \vee q) \leftrightarrow (q \vee p)$

$\varphi, \psi \in \mathcal{L}(\mathcal{P})$

$\models (\varphi \vee \psi) \leftrightarrow (\psi \vee \varphi)$

Ogólniej: tzn. że $\varphi(p_1, \ldots, p_n) \in \mathcal{L}(\mathcal{P})$ oraz $\models \varphi(p_1, \ldots, p_n)$. Niech $\varphi_1, \ldots, \varphi_n \in \mathcal{L}(\mathcal{P})$ wtedy

$\models \varphi(\varphi_1, \ldots, \varphi_n)$.

ZADANIE

Def. $p \oplus q \overset{def}{\equiv} (p \wedge \neg q) \vee (\neg p \wedge q)$ XOR

- $p \oplus p \equiv (p \wedge \neg p) \vee (\neg p \wedge p)$
  $\equiv \bot \vee \bot \equiv \bot$
- $p \oplus q \equiv q \oplus p$
- $p \oplus (q \oplus r) \equiv (p \oplus q) \oplus r$

p	q	p ⊕ q
1	1	0
1	0	1
0	1	1
0	0	0

alternatywa wykluczająca

zadanie tabelkowe 0-1

Wniosek: $(p \oplus q) \oplus q \equiv$

$\equiv p \oplus (q \oplus q) \equiv p \oplus \bot \overset{def}{\equiv} (p \wedge \top) \vee (\neg p \wedge \bot)$

$\equiv p \vee \bot \equiv p$

$$(p \oplus q) \oplus q \equiv p$$

Bob Alicja

KLUCZ: 01011001001 ... 0110

sekret A z B.

A: JUTRO WAGARY

ASCII

X = 010100001 11001010 ... 01001011 1101 ...

K = 01011000 00010110

Y = X⊕K = 00001001 ...

Bob Y⊕K 01011000 ...

X = 01010 ...

Y ← przesyłana informacja

p
$Y = 0110110111001\ldots$
$K^* = 101101\ldots$
q
$X^* = 110110111\ldots$

$X =$ "LUBIE HISTORIE"

$X^* = 1101101\ldots$

$p \oplus X \equiv q$ szukamy X

$p \oplus (p \oplus X) \equiv p \oplus q$ $\quad X = p \oplus q$

$(p \oplus p) \oplus X \equiv \bot \oplus X \equiv X$