1b. Podstawy logiki matematycznej: zastosowania

Grzegorz Kosiorowski

Uniwersytet Ekonomiczny w Krakowie

1. Zastosowania: metody dowodzenia
2. Zastosowanie: związek z teorią zbiorów
3. Zastosowanie: bramki i sieci logiczne

Motywacja

- Oparcie na logice i ścisłe dowodzenie każdego twierdzenia - podstawa matematyki.
- Wiemy, że twierdzenia matematyczne to pewne implikacje (lub równoważności).
- Mamy zestaw założeń: $Z_1, Z_2, \ldots, Z_n$. Dowodem jest uzyskanie tezy T za pomocą przekształceń logicznych z wykorzystaniem założeń i innych zdań zawsze prawdziwych.
- Jakimi metodami można dojść od założeń do tezy?

Dowód wprost

Najpowszechniejszy typ dowodu:

Dowód wprost

Dowód wprost jest ciągiem implikacji od założeń do tezy:

$$Z_1 \wedge Z_2 \wedge \ldots \wedge Z_n \Rightarrow \ldots \Rightarrow T$$

Dowód wprost - przykład

Dowodem wprost jest poniższy dowód zdania:

Zdanie

Jeśli m i n są liczbami naturalnymi nieparzystymi, to ich iloczyn mn jest liczbą naturalną nieparzystą.

Dowód: m, n są nieparzyste (z założenia). Istnieją liczby naturalne k i l takie, że $m = 2k + 1$ i $n = 2l + 1$ (z własności liczb nieparzystych). Zatem $mn = (2k + 1)(2l + 1) = 2(2kl + k + l) + 1$ (wykonywanie mnożenia). $2(2kl + k + l)$ jest podzielne przez 2 (prawa działań na liczbach naturalnych), czyli parzyste, więc $mn = (2k + 1)(2l + 1) = 2(2kl + k + l) + 1$ jest nieparzyste (twierdzenia o liczbach parzystych i nieparzystych). QED.

Dowód nie wprost

Czasem potrzebny jest:

Dowód nie wprost

Dowód nie wprost polega na udowodnieniu kontrapozycji:

$$\sim T \Rightarrow \ldots \Rightarrow \sim (Z_1 \wedge Z_2 \wedge \ldots \wedge Z_n)$$

Dowód nie wprost - przykład

Dowodem nie wprost jest poniższy dowód zdania:

Zdanie

Niech m i n będą liczbami naturalnymi. Jeśli $m + n \geqslant 9$ to $m \geqslant 5$ lub $n \geqslant 5$.

Dowód: Dowodzimy kontrapozycji: jeżeli nieprawdą jest, że ($m \geqslant 5$ lub $n \geqslant 5$), to nieprawdą jest, że $m + n \geqslant 9$. Zakładamy więc zaprzeczenie ($m \geqslant 5$ lub $n \geqslant 5$). Z prawa de Morgana i faktu, że m, n są liczbami naturalnymi, założenie to jest równoważne koniunkcji ($m \leqslant 4 \wedge n \leqslant 4$). Dodając stronami te nierówności (i korzystając z faktu, że możemy tak robić) dostajemy $m + n \leqslant 8$, czyli, że nieprawdą jest, że $m + n \geqslant 9$. QED.

Dowód przez sprowadzenie do sprzeczności

Wariantem dowodu nie wprost jest:

Dowód przez sprowadzenie do sprzeczności

Dowód przez sprowadzenie do sprzeczności (w skrócie: przez sprzeczność) polega na udowodnieniu zdania:

$$(Z_1 \wedge Z_2 \wedge \ldots \wedge Z_n) \wedge (\sim T) \Rightarrow \ldots \Rightarrow 0.$$

Chodzi o to, by do startowych założeń dołączyć zaprzeczenie tezy i pokazać, że ten nowy zestaw założeń prowadzi do oczywistego fałszu.

Przykład

Dowodem przez sprzeczność jest poniższy dowód zdania:

Zdanie

Jeżeli $x^2 = 2$ to x jest liczbą niewymierną.

Dowód: Zakładamy, że $x^2 = 2$ i x jest liczbą wymierną. Wtedy istnieją liczby całkowite p, q $(q \neq 0)$, nie mające wspólnych dzielników poza 1, takie, że $x = \frac{p}{q}$. Wtedy $\left(\frac{p}{q}\right)^2 = 2$, a zatem $p^2 = 2q^2$. Zatem p^2 jest liczbą parzystą, skąd łatwo wywnioskować, że p jest liczbą parzystą, czyli $p = 2k$ dla pewnej liczby całkowitej. Stąd $(2k)^2 = 2q^2$, czyli $2k^2 = q^2$. Czyli q^2 jest liczbą parzystą, a więc i q jest liczbą parzystą. Zatem p i q nie mają wspólnych dzielników poza 1, ale są liczbami parzystymi, co musi być fałszem (bo 2 jest dzielnikiem każdej liczby parzystej). Zatem x nie może być liczbą wymierną. QED.

Teoria zbiorów

Logika jest używana jako narzędzie podstawy matematyki jaką jest teoria zbiorów. Pozwala zdefiniować podstawowe działania na zbiorach, jak i badać twierdzenia tej teorii. Przypomnijmy podstawowe oznaczenia zbiorów:

- $\mathbb{N}$ - liczby naturalne (z zerem), $\mathbb{N}_+$ - liczby naturalne dodatnie, $\mathcal{P}$ - liczby pierwsze.
- $\mathbb{Z}$ - liczby całkowite.
- $\mathbb{R}$ - liczby rzeczywiste.
- $\mathbb{C}$ - liczby zespolone.
- $\emptyset$ - zbiór pusty.

W ramach tego kursu, jeśli wyraźnie nie zaznaczymy inaczej, domyślnie liczby pochodzą ze zbioru $\mathbb{Z}$.

Relacje na zbiorach - przypomnienie

Relacje na zbiorach i ich elementach definiujemy następująco:

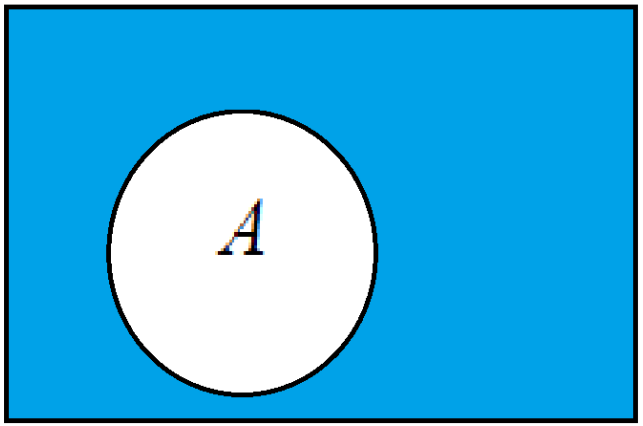
- $x \in A$ (x zazwyczaj nie jest zbiorem!)- x należy do zbioru A, x jest elementem zbioru A. Fakt, że x nie należy do zbioru A można zapisać $x \notin A$.
- $A \subset B$ (A i B są zbiorami!) - A jest podzbiorem B lub A zawiera się w B, co logicznie możemy zapisać jako $x \in A \Rightarrow x \in B$ (odpowiednik implikacji).
- $A = B$ - można logicznie zapisać: $x \in A \Leftrightarrow x \in B$ (odpowiednik równoważności).

Działania na zbiorach - przypomnienie

Działania na zbiorach i ich elementach definiujemy następująco:

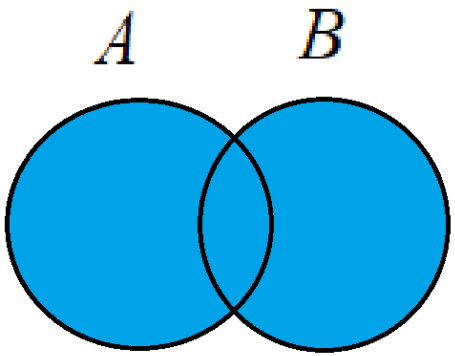
- Jeśli z kontekstu wynika, że działamy w ramach jakiegoś większego zbioru X, którego A jest podzbiorem, to A^c lub A' nazywamy dopełnieniem zbioru A do zbioru X (X w tym kontekście jest czasem nazywane uniwersum) i definiujemy jako $x \in A^c \Leftrightarrow \sim (x \in A)$ (odpowiednik negacji).
- *Sumę* zbiorów $A \cup B$ definiujemy: $x \in A \cup B \Leftrightarrow (x \in A \vee x \in B)$ (odpowiednik alternatywy).
- *Przecięcie* lub *część wspólną* zbiorów $A \cap B$ definiujemy: $x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B)$ (odpowiednik koniunkcji).
- *Różnicę* zbiorów $A \setminus B$ definiujemy: $x \in A \setminus B \Leftrightarrow (x \in A \wedge x \notin B)$.
- Dla dowolnego zbioru skończonego X, $|X|$ oznacza *moc* X, czyli po prostu liczbę jego elementów.

Działania na zbiorach - ilustracja

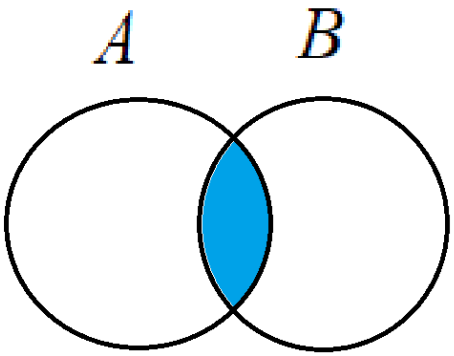


$A' = A^c$

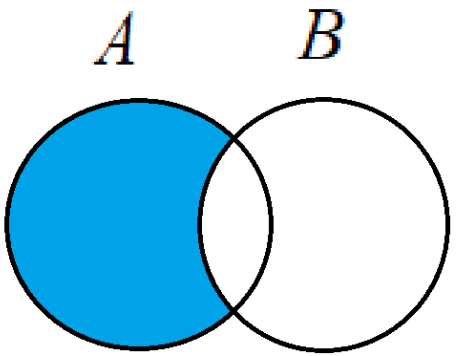
X



$A \cup B$



$A \cap B$



$A \setminus B$

Działania na zbiorach - iloczyn kartezjański

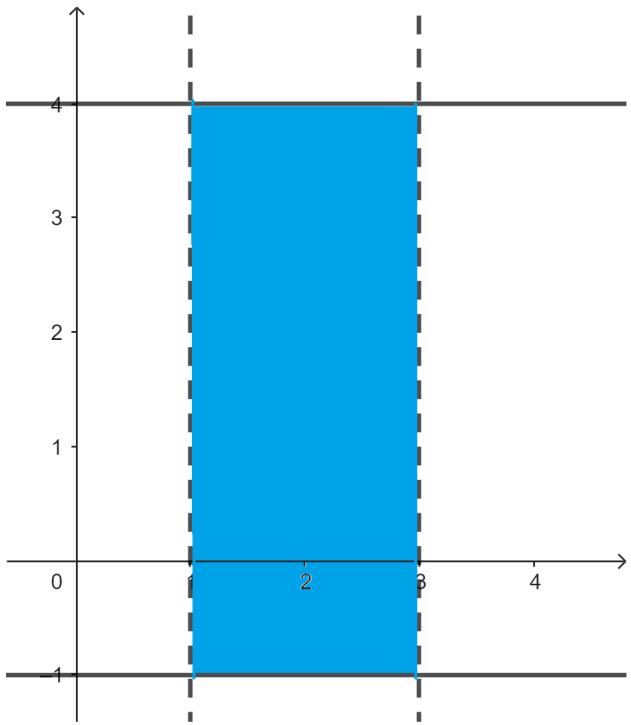
Iloczyn kartezjański

Iloczynem kartezjańskim $A \times B$ zbiorów A i B nazywamy zbiór par (uporządkowanych, czyli zadanych w konkretnej kolejności) elementów tych zbiorów takich, że pierwszy element pary należy do A, a drugi do B.

$$(a, b) \in A \times B \Leftrightarrow (a \in A \wedge b \in B).$$

Iloczyn kartezjański - przykłady

Jeśli $A = \{x, y\}$, a $B = \{y, 0, 1\}$ to
$A \times B = \{(x, y),\ (x, 0), (x, 1), (y, y), (y, 0), (y, 1)\}$.
Iloczyn podzbiorów $\mathbb{R}$ często zaznacza się na płaszczyźnie, jak poniżej $(1, 3) \times [-1, 4]$:



Prawa logiki i zagadnienia teorii zbiorów

Praw logiki używamy do dowodzenia zawierań i równości zbiorów.

Zadanie

Niech $A, B \subset X$ dla pewnego zbioru X. Udowodnić, że $(A \cap B)^c = A^c \cup B^c$.

Z definicji równości, mamy udowodnić prawdziwość zdania:

$$x \in (A \cap B)^c \Leftrightarrow x \in (A^c \cup B^c).$$

Logika i zbiory

$$x \in (A \cap B)^c \Leftrightarrow x \in (A^c \cup B^c)?$$

Założymy lewą stronę równoważności i korzystając z definicji oraz praw logiki spróbujemy ją przekształcić równoważnie do prawej:

$$x \in (A \cap B)^c \Leftrightarrow \sim (x \in A \cap B) \Leftrightarrow \sim (x \in A \wedge x \in B)$$

wykorzystujemy jedno z praw de Morgana:

$$\sim (x \in A \wedge x \in B) \Leftrightarrow [\sim (x \in A) \vee \sim (x \in B)] \Leftrightarrow$$

$$\Leftrightarrow (x \in A^c \vee x \in B^c) \Leftrightarrow x \in (A^c \cup B^c).$$

Z przechodniości równoważności otrzymujemy tezę.

Działania na wielu zbiorach

Oczywiście, można wykonywać wprowadzone działania na więcej niż 2 zbiorach:
Suma zbiorów $A_1, A_2, \ldots, A_k$:

$$\bigcup_{i=1}^{k} A_i = A_1 \cup A_2 \cup \ldots \cup A_k$$

Przecięcie zbiorów $A_1, A_2, \ldots, A_k$:

$$\bigcap_{i=1}^{k} A_i = A_1 \cap A_2 \cap \ldots \cap A_k$$

Działania na wielu zbiorach

Iloczyn kartezjański $A_1, A_2, \ldots, A_k$ to zbiór ciągów k-elementowych, których kolejne elementy należą do kolejnych zbiorów z tej listy:

$$\prod_{i=1}^{k} A_i = A_1 \times A_2 \times \ldots \times A_k.$$

W szczególności, definiujemy:

$$A^n = A \times A \times \ldots \times A,$$

gdzie iloczyn kartezjański występuje $(n-1)$ razy.
Dlatego $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ to typowe oznaczenie płaszczyzny kartezjańskiej, czyli zbioru par liczb rzeczywistych.

Przydatne oznaczenia

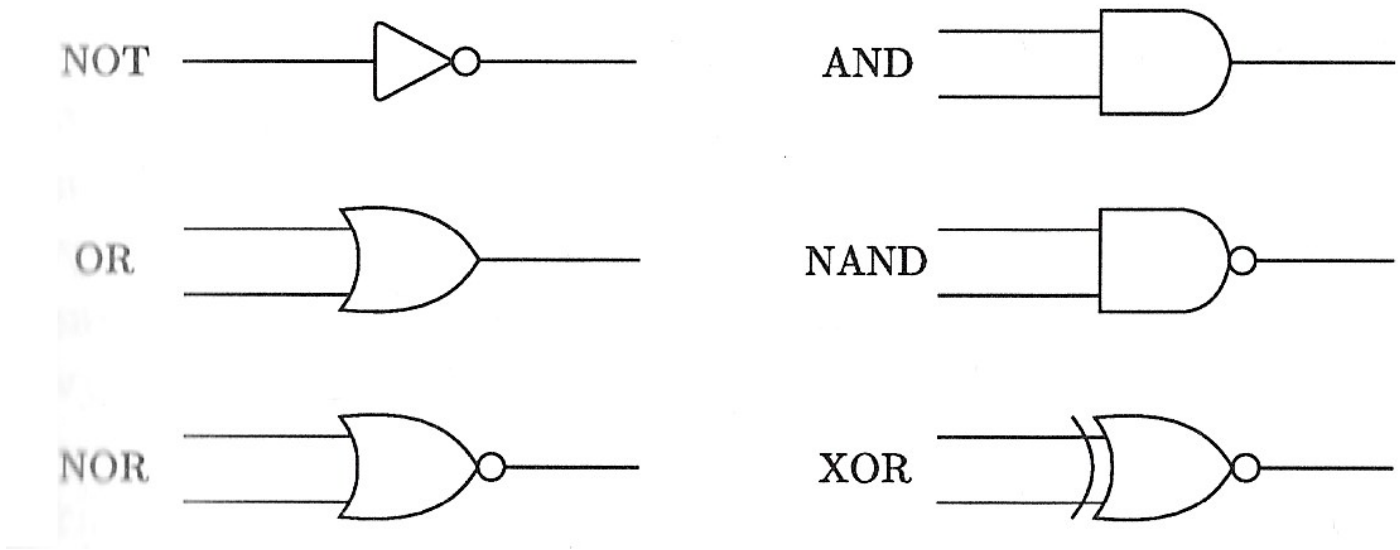
Mogą się jeszcze czasem przydać oznaczenia:

- Zbiór wszystkich podzbiorów zbioru A (w tym zbioru pustego i samego zbioru A): $P(A)$ lub 2^A.
- Zbiór wszystkich funkcji z A do B: B^A.

Bramki i sieci logiczne - motywacja

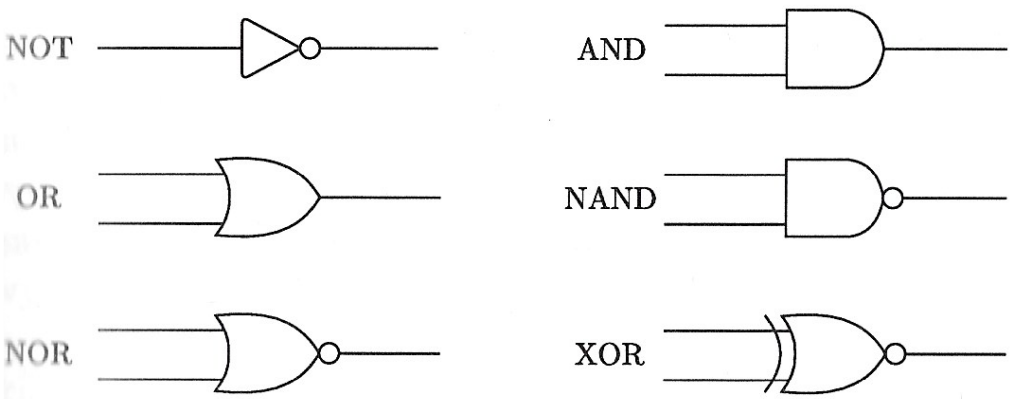
- Informatyka na poziomie sprzętowym: projektowanie urządzeń, które dają właściwe wyniki dla danych wejściowych.
- Wyniki i dane można przedstawić jako zera i jedynki, co oznacza, że zagadnienia projektowania takich układów można zapisać językiem logiki.
- Takie układy nazywamy *sieciami logicznymi*. Buduje się je z pojedynczych jednostek: *bramek logicznych*. Sprzętowe odpowiedniki tych jednostek są dostępne na rynku (zwykle 0-brak sygnału, 1-sygnał).
- Schematy takich sieci logicznych mają ustandaryzowany sposób zapisu.

Bramki logiczne - symbole



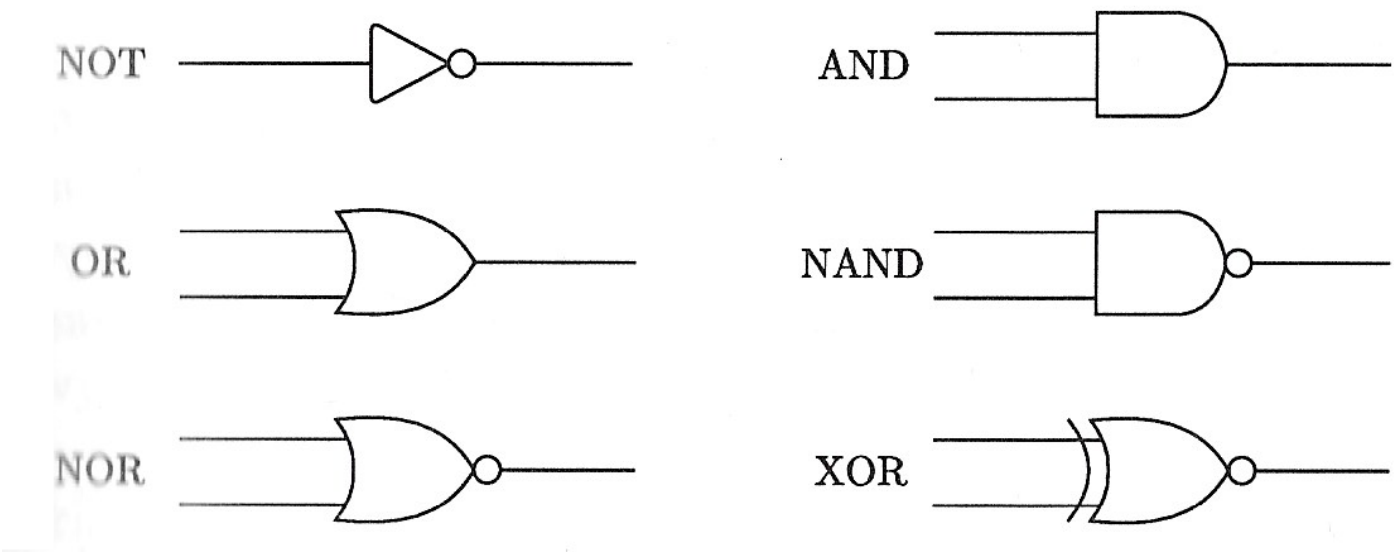
Symbole najbardziej podstawowych bramek (zgodne z tzw. standardem ANSI/IEEE). Przyjmuje się, że linie dochodzące do danego symbolu z lewej strony są liniami wejściowymi (wprowadzającymi zmienne o wartościach 0 lub 1), a po prawej: linią wyjściową (generująca wartość 0 lub 1).

Bramki logiczne - symbole



Bramka NOT realizuje zaprzeczenie (czyli wartość zmienia w jej „dopełnienie"). Bramka AND - koniunkcję (czyli dwie zmienne przeprowadza w wartość ich koniunkcji), OR - alternatywę, NAND i NOR są ich zaprzeczeniami (zwróćmy uwagę na kółka odróżniające je od AND i OR), a XOR - alternatywę wykluczającą. Na kolejnym slajdzie przypomnienie ich matryc dla sygnałów x i y.

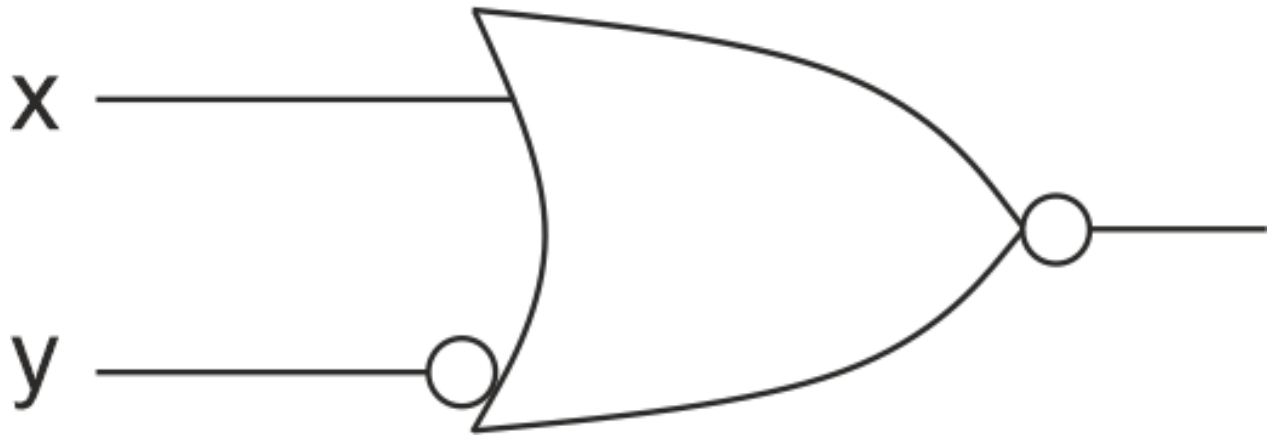
Bramki logiczne - symbole



x	y	$NOT(x)$	OR	NOR	AND	NAND	XOR
1	1	0	1	0	1	0	0
1	0	0	1	0	0	1	1
0	1	1	1	0	0	1	1
0	0	1	0	1	0	1	0

Sieci logiczne - przykład

Małe kółko na jakiejś linii w zapisie zastępuje całą bramkę NOT, czyli oznacza przejście na „sygnał dopełniający" sygnału tej linii.

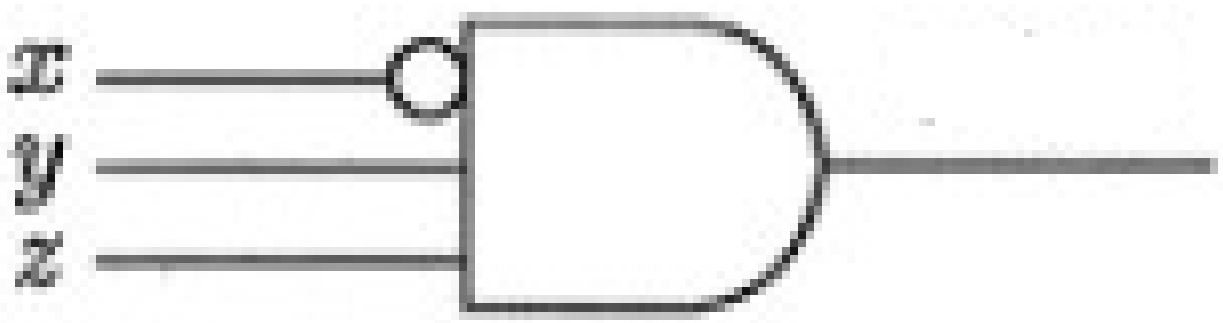


Przedstawiona powyżej bramka realizuje wyrażenie:

$$\sim (x \vee \sim y).$$

Sieci logiczne - przykład

Tak jak możliwe są uogólnienia funktorów dwóch zmiennych do funktorów większej liczby zmiennych, tak bramki AND, OR, NAND i NOR są dostępne z większą liczbą danych wejściowych.



Przedstawiona powyżej bramka realizuje wyrażenie:

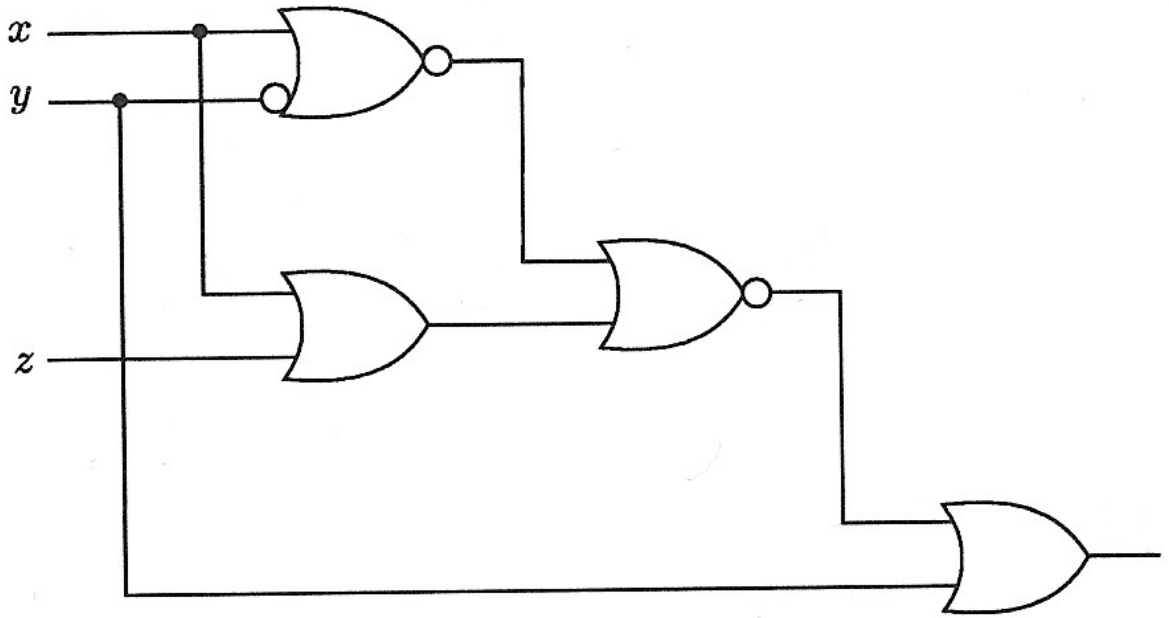
$$(\sim x) \wedge y \wedge z.$$

Zastosowanie logiki w sieciach

Urządzenia oparte na sieciach logicznych operują na gigantycznej liczbie zmiennych i bramek. Stworzenie układu, który realizuje dowolne przejście od danych do wyników jest proste. Ale warto go zoptymalizować, przykładowo, ze względu na:

- Jak najmniejszą liczbę bramek;
- Jak najmniejszą długość najdłuższego ciągu bramek;
- Inne, szczegółowe wymagania zależne od konkretnego problemu.

Sieci logiczne - przykład



Ta sieć poprawnie realizuje wyrażenie logiczne:

$$\sim [\sim (x \vee \sim y) \vee (x \vee z)] \vee y.$$

Ale jest niepotrzebnie skomplikowana.

Bramki logiczne - symbole

Zbadajmy tabelę logiczną tego wyrażenia (kroki pośrednie do sprawdzenia jako zadanie):

$$\sim [\sim (x \vee \sim y) \vee (x \vee z)] \vee y.$$

x	y	z	$\sim [\sim (x \vee \sim y) \vee (x \vee z)] \vee y$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	1

Bramki logiczne - symbole

Okazuje się, że dokładnie taki sam jest wynik dużo prostszego wyrażenia:

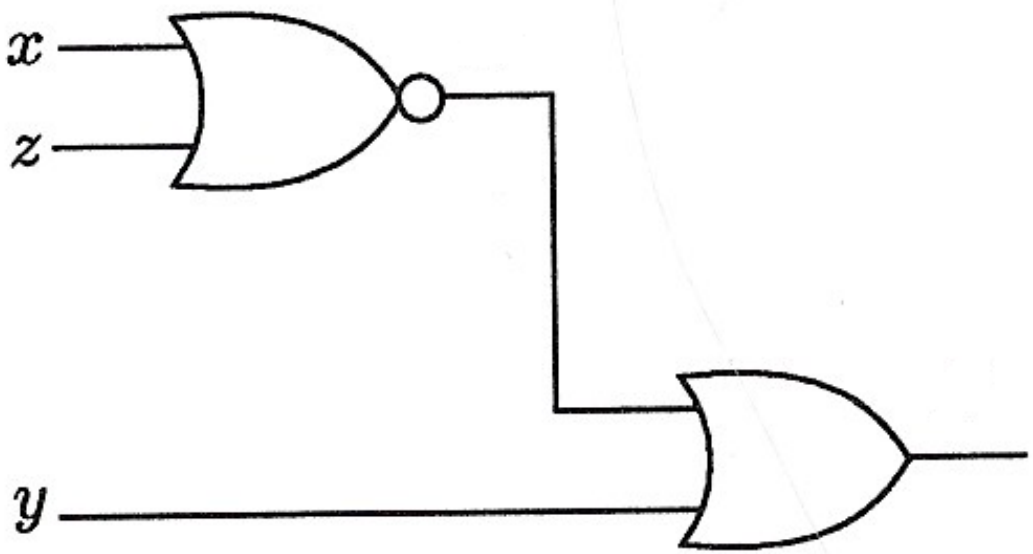
$$\sim (x \vee z) \vee y.$$

x	y	z	$\sim (x \vee z) \vee y$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	1

Sieci logiczne - przykład

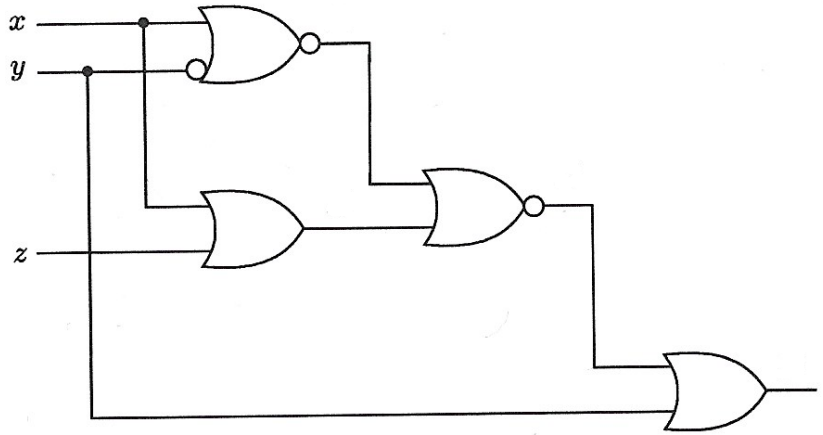
$$\sim (x \vee z) \vee y.$$

Jest wyrażone siecią logiczną o wiele prostszą (zużywającą mniej bramek i mającą krótsze ciągi bramek).

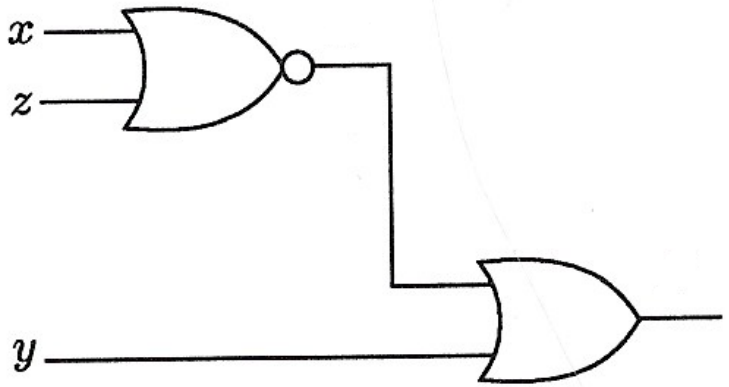


Sieci logiczne - przykład

Podsumowując, sieć:



można zastąpić dużo prostszą siecią



Sieci logiczne - algorytmy optymalizacji

Generalnie, tworzenie optymalnych sieci logicznych to fascynujące, acz trudne zagadnienie, które da się w pewnym stopniu zalgorytmizować. Wykracza to poza materiał naszego wykładu. Osobom zainteresowanym tą tematyką polecam poszukanie informacji o:

- Metodzie tablic Karnaugha;
- Metodzie Quine'a-McCluskeya.