**Na podstawie materiałów dostarczonych
przez prof. Antoniego Ligęze
zebrał i uzupełnił Konrad Kułakowski**

Elementy matematyki dyskretnej

wykłady cz. I

Czym jest matematyka dyskretna?

Matematyka dyskretna *to zbiorcza nazwa wszystkich działów matematyki, które zajmują się badaniem struktur nieciągłych, to znaczy zawierających zbiory co najwyżej przeliczalne (czyli właśnie dyskretne).*

(źródło: Wikipedia, http://pl.wikipedia.org).

Literatura

[1] Norman L. Biggs. *Discrete mathematics.* Oxford University Press, Inc., 1986.

[2] Witold Lipski. *Kombinatoryka dla programistów.* Wydawnictwa Naukowo-Techniczne, 2004.

[3] Helena Rasiowa. *Wstęp do matematyki współczesnej.* Wydawnictwo Naukowe PWN, 1998.

[4] Marek Skomorowski. *Wstęp do projektowania układów cyfrowych.* Uniwersytet Jagielloński, 1994.

[5] Kenneth A. Ross, Charles R.B. Wright. *Matematyka dyskretna.* Wydawnictwo Naukowe PWN, 2003.

Zbiory

Pojęcie zbioru

Pojęcie *zbioru* jest powszechnie stosowane w matematyce i w języku codziennym. Przyjmuje się, że pojęcia zbioru nie definiuje się (pojęcie pierwotne). Intuicyjnie, oznacza ono zestaw lub kolekcję pewnych elementów. Zwykle przyjmuje się, że są to elementy podobne, jednakowego typu. Jednak znane są próby definicji tego pojęcia, np.

Definicja 1 *Przez* ***zbiór*** *rozumiemy złączenie M określonych rozróżnialnych obiektów naszego doświadczenia poglądowego lub naszej wyobraźni w jedną całość (*Georg Cantor, 1845-1918*).*

Te rozróżnialne obiekty nazywamy właśnie elementami zbioru M. Stosowana jest następująca notacja:

- $m \in M$: obiekt (element) m należy do zbioru M,
- $m \notin M$: obiekt (element) m nie należy do zbioru M,
- $M = \{m_1, m_2, \ldots, m_k\}$: zbiór M składa się (tylko i wyłącznie) z elementów $m_1, m_2, \ldots, m_k$,
- $M = \{m \in U : \phi(m)\}$: zbiór M składa się (tylko i wyłącznie z tych elementów zbioru U (universum), które spełniają warunek (logiczny) zdefiniowany formułą $\phi(m)$.

Kolejność elementów w zbiorze nie jest istotna. Każdy element zbioru może wystąpić w nim tylko raz. Zbiory mogą być skończone (k-elementowe, $k \geq 0$) lub nieskończone.
Liczbę elementów zbioru M oznaczamy przez $||M||$, $\mathrm{card}(M)$, lub $\#M$.

Zbiory

Definiowanie zbiorów

Zbiory mogą być definiowane w następujący sposób:

- **ekstensjonalnie**, tzn. poprzez wyliczenie wszystkich elementów, np. $\{pon., wt., śr., czw., pt., so., niedz.\}$, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, lub $\{a, b, c, \ldots, x, y, z\}$, $\{1, 2, 3, \ldots\}$, $\{1, 3, 5, 7, 11, 13, 17, \ldots\}$,
- **intensjonalnie**, tzn. poprzez zdefiniowanie własności elementów, najczęściej z pewnego uniwersum (tzn. zadanie dziedziny i warunku), np. $\{n \in N : 2|n\}$,
- **rekurencyjnie**, tzn. poprzez zdefiniowanie pewnego elementu (elementów) bazowego i reguły produkcji, np. $x_1 = 1$, $x_2 = 1$, $x_i = x_{i-1} + x_{i-2}$ dla $i \geq 3$,
- za pomocą operacji algebry zbiorów (zadawanie wtórne),
- za pomocą operacji logicznych (zadawanie wtórne),
- domyślnie.

Operacje algebry zbiorów

Dwa zbiory X i Y są równe $X = Y$, wtw. gdy każdy element X należy do Y i na odwrót. Zbiór X jest podzbiorem (właściwym) zbioru Y wtw. każdy element X należy do zbioru Y, co notujemy $X \subseteq Y (X \subset Y$ gdy $X \neq Y)$.
Suma zbiorów: $X \cup Y = \{x : x \in X \vee x \in Y\}$,
Iloczyn (przecięcie zbiorów: $X \cap Y = \{x : x \in X \wedge x \in Y\}$,
Różnica zbiorów: $X \setminus Y = \{x : x \in X \wedge \neg x \in Y\}$,
Dopełnienie zbioru X (do uniwersum U): $\overline{X} = U \setminus X$.
Zbiór pusty oznaczamy przez $\emptyset$. Zbiór wszystkich podzbiorów U przez 2^U. Związki pomiędzy zbiorami wygodnie jest przedstawiać za pomocą tzw. diagramów Venna.

Zbiory

Wybrane zbiory liczbowe

- $\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, \ldots\}$ – zbiór liczb naturalnych,
- $\mathbb{P} = \{1, 2, 3, 4, 5, 6, 7, \ldots\}$ – zbiór liczb całkowitych dodatnich,
- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ – zbiór liczb całkowitych,
- $\mathbb{Q} = \{m/n : \ m \in \mathbb{Z}, n \in \mathbb{Z}\}$ – zbiór liczb wymiernych,
- $\mathbb{R}$ – zbiór liczb wymiernych,

Zachodzi:

$$\mathbb{P} \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

2^S – Zbiór wszystkich podzbiorów zbioru S (zbiór potęgowy).

$card(2^S) = 2^n$ gdzie $n = card(S)$

Przedziały

- $[a, b] = \{x \in \mathbb{R} : \ a \leq x \leq b\}$ – przedział obustronnie domknięty,
- $(a, b) = \{x \in \mathbb{R} : \ a < x < b\}$ – przedział obustronnie otwarty,
- $(a, b] = \{x \in \mathbb{R} : \ a < x \leq b\}$ – przedział lewostronnie otwarty i prawostronnie domknięty,
- $[a, b) = \{x \in \mathbb{R} : \ a \leq x < b\}$ – przedział lewostronnie domknięty i prawostronnie otwarty.

Zbiory

Prawa algebry zbiorów

- $X \cup Y = Y \cup X$ – przemienność sumy,
- $X \cap Y = Y \cap X$ – przemienność iloczynu,
- $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ – łączność sumy,
- $(X \cap Y) \cap Z = X \cap (Y \cap Z)$ – łączność iloczynu,
- $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z) =$ – rozdzielność sumy względem iloczynu,
- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ – rozdzielność iloczynu względem sumy,
- $X \cup X = X$, $X \cap X = X$ – idempotentność,
- $X \cup \emptyset = X$, $X \cap U = X$ – identyczność; element neutralny,
- $X \cup U = U$, $X \cap \emptyset = \emptyset$ – identyczność; element przeciwny,
- $\overline{\overline{X}} = X$ – prawo podwójnego dopełnienia,
- $X \cup \overline{X} = U$, $X \cap \overline{X} = \emptyset$,
- $\overline{U} = \emptyset$, $\overline{\emptyset} = U$,
- $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$ – prawo De morgana dla dopełnienia sumy,
- $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$, – prawa De Morgana dla dopełnienia iloczynu.

Zbiory z powtórzeniami

Zbiory z powtórzeniami to zbiory w których identyczne elementy mogą występować wielokrotnie; inne stosowane nazwy to *multizbiory* lub *wielozbiory*.

Definicja 2 *Zbiorem z powtórzeniami M określonym nad pewnym zbiorem U nazywamy dowolny zbiór par $\{(r_M(u), u) : u \in U, r_M(u) \in N \cup \{0\}\}$, gdzie r_M jest funkcją typu $r_M : U \longrightarrow N \cup \{0\}$.*

Wielozbiory zapisywane są w postaci $M = \sum r_M(u) * u$ lub jako zbiory par postaci $M = \{(r_M(u_1), u_1), (r_M(u_2), u_2), \ldots, (r_M(u_k), u_k)\}$ (dla $r_M(u) \neq 0$). Liczbę $r_M(u)$ nazywa się *krotnością* elementu u w wielozbiorze M lub *współczynnikiem repetycji*. **Suma zbiorów (teoriomnogościowa):**

$$M_1 \cup M_2 = \sum_{u \in U} max(r_{M_1}(u), r_{M_2}(u)) * u$$

Przecięcie (iloczyn teoriomnogościowy):

$$M_1 \cap M_2 = \sum_{u \in U} \min(r_{M_1}(u), r_{M_2}(u)) * u$$

Różnica zbiorów:

$$M_1 \setminus M_2 = \sum_{u \in U} max((r_{M_1}(u) - r_{M_2}(u)), 0) * u$$

Dodawanie (suma arytmetyczna):

$$M_1 + M_2 = \sum_{u \in U} (r_{M_1}(u) + r_{M_2}(u)) * u$$

M**nożenie skalarne**:

$$k \cdot M = \sum_{u \in U} (k \cdot r_M(u)) * u$$

Zawieranie:

$$M_1 \subseteq M_2 \;\; wtw. \;\; \forall u \in U \;\; r_{M_1}(u) \leq r_{M_2}(u)$$

Równość:

$$M_1 = M_2 \;\; wtw. \;\; \forall u \in U \;\; r_{M_1}(u) = r_{M_2}(u).$$

Relacje

Pojęcie relacji

Pojęcie realacji jest stosowane zarówno w języku potocznym jak i w naukach ścisłych. Intuicyjnie, *relacja* oznacza pewien związek zachodzący pomiędzy dwoma lub więcej elementami, inaczej – pewną własność spełnianą przez te elementy. Przykładami tak rozumianej relacji mogą być szeroko pojmowane związki rodzinne (relacje rodzinne, relacje pokrewieństwa), zależności służbowe (relacje przełożony – podwładny), stosunki pomiędzy państwami (relacje międzypaństwowe), itp. Relacje takie określane są poprzez nazwę kryjącą pewne znaczenie, określającą rodzaj związku, a odnoszoną do elementów spełniających tą relację (najczęściej dwóch).

Przykłady relacji rozumianej jako związek lub własność zawarte są np. w następujących stwierdzeniach:

Jest pięknie.

Adam *ma brata*.

Jan *jest bratem* Adama.

Jan *jest średnim bratem* Adama i Karola.

Powyższe własności stanowią przykłady relacji zero-, jedno-, dwu- oraz trzyargumentowych; nazwę realacji wyróżniono kursywą, imiona braci stanowią argumenty relacji. Tak rozumiane relacje można definiować na dwa podstawowe sposoby: *ekstensjonalnie*, tzn. poprzez wyliczenie wszystkich krotek (k-elementowych ciągów) tworzących tą relację oraz *intensjonalnie*, tzn. poprzez podanie warunku który muszą spełniać elementy relacji, zazwyczaj podając równocześnie uniwersum.

W istocie, relacja może mieć dowolną całkowitą, nieujemną liczbę argumentów. Relacjami najczęściej rozważanymi w matematyce są relacje dwuargumentowe (dwuczłonowe) stanowiące klasę relacji dla których zedifiniowano szereg istotnych własności i znajdujących szerokie zastosowanie.

Relacje dwuargumentowe

Iloczyn kartezjański dwóch zbiorów

Definicja 3 *Iloczynem kartezjańskim $X \times Y$ (dowolnych) zbiorów X oraz Y nazywamy zbiór wszystkich par postaci (x, y), takich że $x \in X$ i $y \in Y$; formalnie*

$$X \times Y = \{(x, y) : x \in X \wedge y \in Y\}$$

Liczba elementów skończonego iloczynu kartezjańskiego wynosi $||X|| \cdot ||Y||$.

Przykład
Niech $X = \{x_1, x_2, x_3, x_4\}$ a $Y = \{y_1, y_2, y_3\}$. Iloczyn kartezjański $X \times Y = \{(x_1, y_1), (x_1, y_2), (x_1, y_3), (x_2, y_1), (x_2, y_2), (x_2, y_3), (x_3, y_1), (x_3, y_2), (x_3, y_3), (x_4, y_1), (x_4, y_2), (x_4, y_3)\}$ ma 12 elementów.

Praktyczne znaczenie iloczynu kartezjańkiego: zawiera on *wszystkie* możliwe połączenia elementów pierwszego zbioru z elementami drugiego zbioru.

Definicja relacji dwuargumentowej

Poniżej przedstawiono definicję pojęcia *relacji dwuargumentowej*. Relacja taka nazywana jest również *relacją binarną* lub *relacją dwuczłonową*.

Definicja 4 *Niech X oraz Y będą dowolnymi zbiorami. Relacją binarną nazywamy każdy zbiór R bedący podzbiorem iloczynu kartezjańskiego tych zbiorów.*

$$R \subset X \times Y$$

Skończone relacje binarne wygodnie jest przedstawiać w postaci tablic dwuwymiarowych (macierzy), grafów lub tablic dwukolumnowych.

Relacje dwuargumentowe

Struktura, definiowanie, notacja

Relacja dwuargumentowa jest *zbiorem* par elementów, takich, że pierwszy element należy do zbioru X a drugi do zbioru Y. Elementy relacji posiadają zatem pewną strukturę – w przypadku relacji binarnej są *ciągami* o długości 2. Powyższa definicja ma charakter *ekstensjonalny*. Iloczyn kartezjański $X \times Y$ tworzy pewne uniwersum. Relację R można też zadać *intensjonalnie* (w tym uniwersum) poprzez zdefiniowanie *funkcji charakterystycznej* relacji lub *formuły logicznej* definiującej własność elementów relacji. Stosowana notacja:

- $(x, y) \in R$ (para (x, y) należy do relacji R),
- xRy (x spełnia relację R z y; tzw. notacja infiksowa),
- $R(x, y)$ (zachodzi relacja R od x, y; tzw. notacja prefiksowa).

Dziedzina i przeciwdziedzina relacji

Definicja 5 *Zbiór*

$$D(R) = \{x : \exists y \ (x, y) \in R\}$$

nazywany jest dziedziną relacji R, a zbiór

$$D'(R) = \{y : \exists x \ (x, y) \in R\}$$

nazywany jest przeciwdziedziną relacji R.

Dla dowolnej relacji $R \subseteq X \times Y$ zachodzi własność $R \subseteq D(R) \times D'(R)$ oraz $D(R) \subseteq X$ i $D'(R) \subseteq Y$. Jeżeli zatem zbiory X oraz Y nie są zadane jawnie, to można przyjąć, że uniwersum dla relacji R (zadawanej intensjonalnie) stanowi zbiór $D(R) \times D'(R)$. Ma to istotne znaczenie praktyczne, np. dla zapewnienia możliwości konstruktywnego wyznaczenia dopełnienia relacji.

Projekcja i rozszerzenie cylindryczne

Ze względu na strukturę elementów (w postaci par) dla relacji definiuje się pewne specyficzne operacje wykraczające poza klasyczną algebrę zbiorów.

Definicja 6 *Niech $R \subseteq X \times Y$ będzie dowolną relacją. Rzutem (projekcją) relacji $\pi_X(R)$ na zbiór X (analogicznie $\pi_Y(R)$ na zbiór Y) nazywamy zbiór*

$$\pi_X(R) = \{x : \exists y \ (x, y) \in R\}$$

oraz analogicznie

$$\pi_Y(R) = \{y : \exists x \ (x, y) \in R\}.$$

Łatwo zauważyć, że w przypadku relacji dwuargumentowej $\pi_X(R) = D(R)$, a $\pi_Y(R) = D'(R)$. Zamiast $\pi_X(R)$ można też pisać $\pi_1(R)$ (rzut na pierwszą składową), a zamiast $\pi_Y(R)$ można pisać $\pi_2(R)$ (rzut na drugą składową). Operacja projekcji na wybraną składową pozwala uzyskać specyfikację zbioru elementów wchodzących w relację związanych z tą składową; powoduje ona utratę informacji o powiązaniach z elementami drugiego zbioru; nie jest zatem operacją odwracalną. Można jednak zdefiniować pewną operację pozwalającą uzyskać pokrycie *wszystkich* możliwych relacji, które mogłyby po projekcji na daną składową dać wynik identyczny z otrzymanym.

Definicja 7 *Niech $R \subseteq X \times Y$ będzie dowolną relacją, $\pi_X(R)$ jej rzutem (projekcją) na zbiór X, a $\pi_Y(R)$ rzutem na zbiór Y.* Rozszerzeniem cylindrycznym *rzutu $\pi_X(R)$ (odpowiednio rzutu $\pi_Y(R)$) relacji R nazywamy relację $\rho(\pi_X(R))$ (odpowiednio $\rho(\pi_Y(R))$) określoną jako*

$$\rho(\pi_X(R)) = \{(x, y) \in X \times Y : x \in \pi_X(R)\}$$

oraz odpowiednio

$$\rho(\pi_Y(R)) = \{(x, y) \in X \times Y : y \in \pi_Y(R)\}$$

tzn. rozszerzenie cylindryczne jest największą *relacją zdefiniowaną w $X \times Y$, która w wyniku projekcji na pierwszą składową daje $\pi_X(R)$ (odpowiednio, na drugą składową daje $\pi_Y(R)$).*

Można zauważyć, że $\rho(\pi_X(R)) = \pi_X(R) \times Y$ oraz $\rho(\pi_Y(R)) = X \times \pi_Y(R)$.

Obcięcie, dopełnienie i domknięcie

Definicja 8 *Niech R będzie dowolną relacją a U oraz V pewnymi zbiorami. Lewostronnym obcięciem relacji R do zbioru U nazywamy zbiór*

$$U|R = \{(x, y) : (x, y) \in R \wedge x \in U\}.$$

Prawostronnym obcięciem relacji R do zbioru V nazywamy zbiór

$$R|V = \{(x, y) : (x, y) \in R \wedge y \in V\}.$$

Obustronnym obcięciem relacji R do pary zbiorów U oraz V nazywamy zbiór

$$U|R|V = \{(x, y) : (x, y) \in R \wedge x \in U \wedge y \in V\}.$$

Operacje obcięcia pełnią rolę „filtrów" – poprzez odpowiedni dobór zbiorów U oraz V z relacji R można otrzymać pewien interesujący nas podzbiór.

Definicja 9 *Niech $R \subseteq X \times Y$ będzie dowolną relacją. Dopełnieniem relacji R nazywamy relację $\overline{R} = (X \times Y) \setminus R$.*

Dopełnienie relacji stanowi jej uzupełnienie do pełnego iloczynu kartezjańskiego. Jeżeli X, Y nie są zadane jawnie, to dopełnienie można zdefiniować jako $\overline{R} = (D(R) \times D'(R)) \setminus R$.
Często celowe jest uzupełnienie zadanej reacji o pewne elementy, tak aby uzyskać pożądane jej własności, takie jak *symetrię* lub *przechodniość*.

Definicja 10 *Niech $R \subseteq X \times X$ będzie dowolną relacją. Domknięciem symetrycznym relacji R nazywamy relację $R^S = R \cup \{(y, x) : (x, y) \in R\}$.*

Definicja 11 *Niech $R \subseteq X \times X$ będzie relacją. Domknięciem przechodnim relacji R nazywamy relację R^* będącą najmniejszym zbiorem takim, że:*

- $R \subseteq R^*$,
- *jeżeli $(x, y) \in R^*$ oraz $(y, z) \in R^*$) to także $(x, z) \in R^*$.*

Powyższa definicja ma charakter rekurencyjny. Domknięcie tranzytywne relacji otrzymuje się jako *punkt stały* operacji dołączania) par spełniających warunki defincji.

Obraz zbioru i złożenie relacji

Relacja dwuargumentowa może być traktowana jako pewnego rodzaju przyporządkowanie – elementom dziedziny przypisane są elementy przeciwdziedziny; zatem relacja może posłużyć do konstrukcji zbioru elementów przypisanych pewnemu podzbiorowi jej dziedziny.

Definicja 12 *Niech R będzie dowolną relacją, a U pewnym zbiorem. Obrazem zbioru U poprzez relację R nazywamy zbiór*

$$R * U = \{y : \exists x \in U \ \ (x, y) \in R\}.$$

Zamiast $R * U$ stosowany również bywa zapis $R(U)$. Obrazem dziedziny relacji poprzez tą relację jest jej przeciwdziedzina. Analogicznie definiuje się przeciwobraz zbioru V poprzez relację R.

Ponieważ relacje mogą być interpretowane jako odwzorowania, można zdefiniować złożenie relacji które odpowiada pojęciu złożenia odwzorowań.

Definicja 13 *Niech $R \subseteq X \times Y$ oraz $S \subseteq U \times V$ będą dowolnymi relacjami. Złożeniem relacji R oraz S nazywamy relację*

$$S \circ R = \{(x, v) : \exists y \in Y \cap U \ \wedge \ (x, y) \in R \wedge (y, v) \in S\}.$$

Potęga relacji: $R^1 = R$, $R^{n+1} = R^n \circ R$. Złożenie relacji zawsze istnieje; może ono być zbiorem pustym (jeżeli $Y \cap U = \emptyset$). Złożenie relacji jest łączne, ale nie jest przemienne. Operacja składania relacji pozwala łączyć informację zawartą w dwóch relacjach poprzez utworzenie (wychwycenie) związku pomiędzy elementami skrajnymi relacji R i S przez wspólny element wewnętrzny y. Złożenie relacji skończonych można otrzymać poprzez *zestawienie* elementów relacji R i S, każdy z każdym, przy czym dla każdej pary elementów tych relacji mających zgodny element łączący y tworzony jest element relacji wynikowej; pary elementów relacji nie dające się połączyć należy pominąć.

Przykład Rozważmy relację $R = \{(a, b), (a, c), (b, a), (b, d), (c, d)\}$ oraz relację $S = \{(b, a), (b, e), (c, f)\}$. Złożeniem relacji R oraz S jest relacja $S \circ R = \{(a, a), (a, e), (a, f), \}$.

Własności relacji dwuargumentowych

Relacje dwuargumentowe mogą posiadać szereg interesujących własności nadających im pewnego rodzaju *regularność*. Będziemy rozważać relacje określone w pewnym zbiorze X (typu $R \subseteq X \times X$).

Definicja 14 *Relację $R \subseteq X \times X$ nazywamy zwrotną jeżeli spełnia ona następujący warunek*

$$\forall x \in X \;\; (x, x) \in R \tag{1}$$

Definicja 15 *Relację $R \subseteq X \times X$ nazywamy przeciwzwrotną jeżeli spełnia ona następujący warunek*

$$\forall x \in X \;\; (x, x) \notin R \tag{2}$$

Definicja 16 *Relację $R \subseteq X \times X$ nazywamy symetryczną jeżeli spełnia ona następujący warunek*

$$\forall x, y \in X \;\; (x, y) \in R \Rightarrow (y, x) \in R \tag{3}$$

Definicja 17 *Relację $R \subseteq X \times X$ nazywamy asymetryczną lub przeciwsymetryczną jeżeli spełnia ona następujący warunek*

$$\forall x, y \in X \;\; (x, y) \in R \Rightarrow (y, x) \notin R \tag{4}$$

Definicja 18 *Relację $R \subseteq X \times X$ nazywamy antysymetryczną jeżeli spełnia ona następujący warunek*

$$\forall x, y \in X \;\; (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y \tag{5}$$

Definicja 19 *Relację $R \subseteq X \times X$ nazywamy przechodnią lub tranzytywną jeżeli spełnia ona następujący warunek*

$$\forall x, y, z \in X \;\; (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R \tag{6}$$

Definicja 20 *Relację $R \subseteq X \times X$ nazywamy spójną jeżeli spełnia ona następujący warunek*

$$\forall x, y \in X \;\; (x, y) \in R \vee (y, x) \in R \tag{7}$$

Relacje równoważności i klasy równoważności

Definicja 21 *Relację, która jest zwrotna, symetryczna i przechodnia nazywamy relacją równoważnościową lub równoważnością.*

Definicja 22 *Niech R będzie dowolną relacją równoważnościową określoną w zbiorze X. Klasą abstrakcji (klasą równoważności) elementu x względem relacji R nazywamy zbiór $[x]_R = \{y : (x, y) \in R\}$.*

Relacja równoważnościowa dzieli zbiór w którym jest określona na tzw. *klasy abstrakcji* lub klasy *równoważnośći* elementów tego zbioru względem tej relacji.

Twierdzenie 1 *Niech R będzie dowolną relacją równoważnościową określoną w niepustym zbiorze X. Relacja R dzieli zbiór X na klasy równoważności (wyznacza te klasy), przy czym spełnione są następujące warunki:*

1. $\forall x \in X \;\; [x]_R \neq \emptyset$ *(klasy równoważności są niepustymi podzbiorami X),*
2. $\forall x_1, x_2 \in X \;\; x_1 R x_2 \Leftrightarrow [x_1]_R = [x_2]_R$,
3. $\forall x_1, x_2 \in X \;\; [x_1]_R \neq [x_2]_R \Rightarrow [x_1]_R \cap [x_2]_R = \emptyset$ *(klasy równoważności są rozłącznymi podzbiorami X),*
4. $\bigcup_{x \in X} [x]_R = X$ *(suma wszystkich klas równoważności daje cały zbiór X).*

Mówimy wówczas, że relacja R wyznacza podział (rozkład) zbioru X na klasy równoważności $[x]_R$.

Dowód:

1. R – jest zwrotna, zatem $\forall x \in X : (x, x) \in R$ tzn. na mocy definicji klasy abstrakcji $x \in [x]_R$ cbdu.

2. „⇒” $\forall y \in X : y \in [x_1]_R \Rightarrow (y, x_1) \in R$, jest też $(x_1, x_2) \in R$. Relacja R jest przechodnia zatem $(x_2, y) \in R$ a stąd $y \in [x_2]_R$. Zatem $[x_1]_R = [x_2]_R$ cbdu.
   „⇐” z tezy 1 otrzymujemy $x_1 \in [x_1]_R$. Równocześnie $[x_1]_R = [x_2]_R$ zatem $x_1 \in [x_2]_R \Rightarrow (x_2, x_1) \in R \Rightarrow (x_1, x_2) \in R \Rightarrow x_1 R x_2$ cbdu.

3. Hipoteza: $[x_1]_R \neq [x_2]_R$ oraz $[x_1]_R \cap [x_2]_R \neq \emptyset$. Zatem $\exists x \in X : x \in [x_1]_R \wedge x \in [x_2]_R$. Na mocy definicji klasy abstrakcji $(x_1, x) \in R \wedge (x, x_2) \in R \Rightarrow (x_1, x_2) \in R \Leftrightarrow x_1 R x_2$. Na mocy tezy 2 wnioskujemy $[x_1]_R = [x_2]_R$. Sprzeczność. cbdu.

4. „⇒” $\forall x_1 \in \bigcup_{x \in X} [x]_R \Rightarrow \exists x_i \in X : [x_i]_R \ni x_1$ ale $[x_i]_R \subset X$ zatem $x_1 \in X$
   „⇐” $\forall x_1 \in X : x_1 \in [x_1]_R$ zatem $x_1 \in ([x_1]_R \cup \bigcup_{x \in X} [x]_R) = \bigcup_{x \in X} [x]_R$. cbdu.

Ustanowienie relacji równoważności prowadzi do abstrakcji poprzez utożsamienie pewnych elementów; korzyścią takiej abstrakcji jest ograniczenie liczby rozpatrywanych elementów (redukcja rozmiarów zbioru).

Relacje n–argumentowe

Definicja 23 *Iloczynem kartezjańskim (n zbiorów)* $X_1 \times X_2 \times \ldots \times X_n$ *zbiorów* $X_1, X_2, \ldots X_n$ *nazywamy zbiór wszystkich n-elementowych ciągów postaci* $(x_1, x_2, \ldots, x_n)$*, takich że* $x_1 \in X_1$*,* $x_2 \in X_2$*, ...* $x_n \in X_n$*; formalnie*

$$X_1 \times X_2 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) : x_1 \in X_1, x_2 \in X_2, \ldots, x_n \in X_n\}.$$

Iloczyn kartezjański postaci $X \times X \times \ldots \times X$ (n razy) nazywany jest *n-tą potęgą kartezjańską* zbioru X i oznaczany jako X^n. Jeżeli zbiory $X_1, X_2, \ldots X_n$ są skończone, liczba elementów zbioru X_i jest równa m_i, $i = 1, 2, \ldots, n$, to liczba elementów iloczynu kartezjańskiego $X_1 \times X_2 \times \ldots \times X_n$ wynosi $\prod_{i=1}^{n} m_i$.

Definicja 24 *Niech* $X_1, X_2, \ldots X_n$ *będą dowolnymi zbiorami. Każdy zbiór* R *będący podzbiorem iloczynu kartezjańskiego tych zbiorów, tj. taki, że*

$$R \subseteq X_1 \times X_2 \times \ldots \times X_n \tag{8}$$

nazywamy relacją n-argumentową.

Relacja n-argumentowa jest *zbiorem* ciągów n-elementowych. Ich struktura jest ustalona dla danej relacji – wszystkie ciągi będące jej elementami muszą mieć tą samą długość. Ciągi te nazywane są *krotkami* lub *n-krotkami*. Na relacjach n-argumentowych można wykonywać działania takie jak suma zbiorów, przecięcie (iloczyn zwykły), różnica zbiorów, dopełnienie, itp. Dla relacji obowiązują również pojęcia równości, zawierania, itp. Odpowiednio rozszerza się też definicje projekcji, rozszerzenia cylindrycznego, obcięcia, dopełnienia, obrazu zbioru i złożenia.

Iloczyn kartezjański $U = X_1 \times X_2 \times \ldots \times X_n$ tworzy pewne uniwersum. Relację R określoną w tym uniwersum można zadać ekstensjonalnie lub intensjonalnie, poprzez określenie pewnego warunku, który spełniają elementy należących do niej par. Warunek taki, mający zazwyczaj postać logiczną, stanowi funkcję charakterystyczną relacji. Tak więc relacja może być do pewnego stopnia utożsamiana z pewną funkcją logiczną – predykatem}; tym razem będzie to predykat o n argumentach.

Relacje n–argumentowe

Dla zapisania faktu, że pewne elementy $x_1 \in X_1$, $x_2 \in X_2$ oraz $x_n \in X_n$ tworzą ciąg należący do relacji R (jej krotkę), stosowane mogą być następujące zapisy:

- $(x_1, x_2, \ldots, x_n) \in R$ (ciąg $x_1, x_2, \ldots, x_n$) należy do relacji R),
- $R(x_1, x_2, \ldots, x_n)$ (zachodzi relacja R od $x_1, x_2, \ldots, x_n$; tzw. notacja prefiksowa).

Powyższe notacje są równoważne; notacja infiksowa nie jest stosowana w przypadku relacji n-argumentowych. Powyższe notacje są równoważne.

Ponieważ przy definiowaniu relacji R zbiory $X_1, X_2, \ldots X_n$ nie zawsze muszą być zadane jawnie, można zdefiniować *dziedzinę* relacji n-argumentowej ze względu na i-ty argument, $i = 1, 2, \ldots, n$.

Definicja 25 *Zbiór*

$$D_i(R) = \{x_i : \exists x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \ \ (x_1, x_2, \ldots, x_n) \in R\}$$

nazywany jest dziedziną relacji R ze względu na i-ty jej argument.

Dla dowolnej relacji n-argumentowej R zachodzi własność $R \subseteq D_1(R) \times D_2(R) \times \ldots \times D_n(R)$ oraz $D_i(R) \subseteq X_i$, $i = 1, 2, \ldots, n$. Jeżeli zbiory $X_1, X_2, \ldots X_n$ nie są zadane jawnie, można przyjąć, że uniwersum relacji R stanowi zbiór $D_1(R) \times D_2(R) \times \ldots \times D_n(R)$. Ma to istotne znaczenie praktyczne, np. dla zapewnienia możliwości konstruktywnego wyznaczenia dopełnienia relacji; jest ono wówczas określone jako $\overline{R}$, gdzie:

$$\overline{R} = \{(x_1, x_2, \ldots, x_n) \in D_1 \times D_2 \times \ldots \times D_n : \ \ (x_1, x_2, \ldots, x_n) \notin R\}.$$

Intensjonalnie, jeżeli relacja R jest określona w pewnym uniwersum za pomocą warunku logicznego, to dopełnienie tej relacji (w tym uniwersum) mozna określić poprzez negację tego warunku.

Funkcje

Pojęcie funkcji

Funkcją $f : X \longrightarrow Y$ będziemy nazywać przyporządkowanie każdemu elementowi zbioru X dokładnie jednego elementu zbioru Y.

Formalnie rzecz biorąc można zdefiniować funkcję jako relację w następujący sposób:

Definicja 26 *Relacja f jest nazywana funkcją wtedy gdy:*

$$\forall x, y, z : \{(x, y) \in f \wedge (x, z) \in f\} \Rightarrow y = z$$

Mówimy, że funkcja f jest określona na zbiorze X i przyjmuje wartości w zbiorze Y. Fakt $(x, y) \in f$ zapisujemy $f(x) = y$. Zbiór ten jest nazywany dziedziną funkcji i oznaczany $D(f)$, $Dom(f)$, względnie D_f, Dom_f. Zbiór wszystkich wartości funkcji f (obraz zbioru X poprzez odwzorowanie f) jest nazywany przeciwdziedziną i oznaczany $Im(f)$ względnie $D'(f)$, $D^{-1}(f)$, D_f^{-1}, $coDom(f)$.

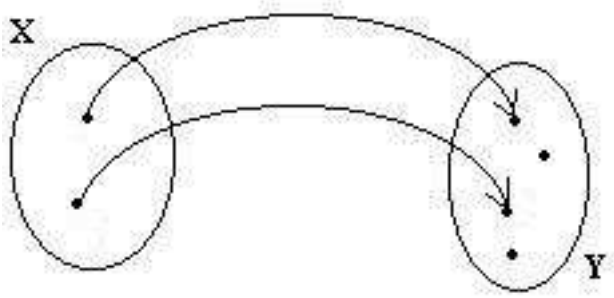
$$Im(f) = \{f(x) : x \in Dom(f)\}$$

Każda funkcja jest jednoznacznie określona poprzez swoją dziedzinę oraz sposób przyporządkowania elementom zbioru X elementów zbioru Y.

Definicja 27 *Funkcja $f : X \rightarrow Y$ jest nazywana iniekcją tj. funkcją różnowartościową wtedy gdy:*

$$\forall x_1, x_2 \in X \wedge f : X \rightarrow Y : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

Przykład iniekcji:

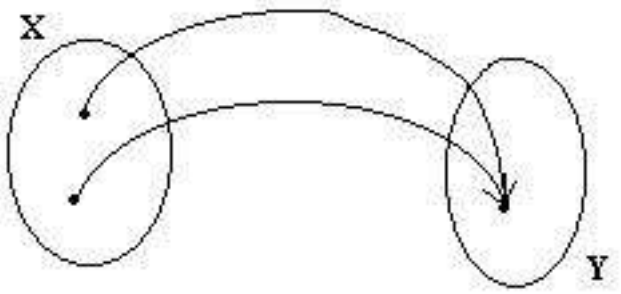


Funkcje

Definicja 28 *Funkcja $f : X \to Y$ jest nazywana* suriekcją *tj. funkcją "na" wtedy gdy:*

$$\forall y \in Y \ \wedge \ f : X \to Y \, \exists x \in X \ : f(x) = y$$

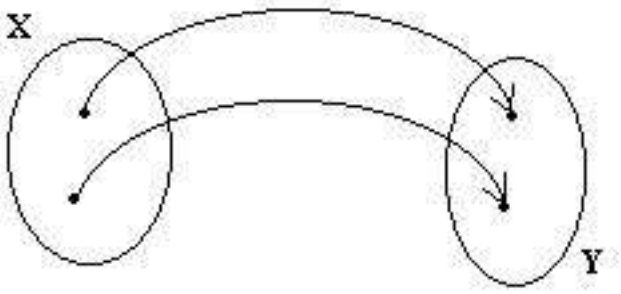
Przykład suriekcji:



Definicja 29 *Funkcja $f : X \to Y$ jest nazywana* bijekcją *tj. funkcją wzajemnie jednoznaczną wtedy gdy:*

$$\forall x \in X \, \exists! y \in Y \ : (x, \, y) \in f \ \wedge \forall y \in Y \, \exists! x \in X \ : (x, \, y) \in f$$

Przykład bijekcji:



Funkcje

Twierdzenie 2 *Funkcja $f : X \to Y$ jest równocześnie iniekcją i suriekcją wtedy i tylko wtedy gdy jest bijekcją.*

Dowód „⇒"

Chce dowieść:

(a) $\forall x \in X\, \exists! y \in Y : (x, y) \in f$

(b) $\forall y \in Y\, \exists! x \in X : (x, y) \in f$

(a) jest prawdą na mocy definicji funkcji;

(b) hipoteza: $\exists y \in Y \wedge x_1, x_2 \in X : (x_1, y) \in f \wedge (x_2, y) \in f \wedge x_1 \neq x_2$, innymi słowy $y = f(x_1) = f(x_2) \wedge x_1 \neq x_2$. Z iniektywności funkcji f mamy, że z $x_1 \neq x_2$ wynika $f(x_1) \neq f(x_2)$ co daje sprzeczność.

Dowód „⇐"

Chce dowieść:

(c) suriektywności tj.: $\forall y \in Y\, \exists x \in X : f(x) = y$

(d) iniektywności tj.: $\forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ funkcji f.

(c) Na mocy definicji bijekcji jest wszczególności prawdą,
że $\forall y \in Y\, \exists! x \in X : (x, y) \in f$ ale to tym bardziej
$\forall y \in Y\, \exists x \in X : (x, y) \in f$ tj. $\forall y \in Y\, \exists x \in X : f(x) = y$ cbdu.

(d) hipoteza: f nie jest funkcją różnowartościową tzn. $\exists x_1, x_2 \in X, : x_1 \neq x_2 \wedge f(x_1) = f(x_2)$. Oznaczmy $y = f(x_1) = f(x_2)$. Zatem $\exists y \in Y \wedge x_1, x_2 \in X : (x_1, y) \in f \wedge (x_2, y) \in f \wedge x_1 \neq x_2$ co przeczy stwierdzeniu $\forall y \in Y\, \exists! x \in X : (x, y) \in f$ cbdu.

Definicja 30 *Funkcja $f : X \to Y$ jest nazywana funkcją stałą wtedy gdy $\forall x \in X\, \exists! y \in Y : f(x) = y$.*

Funkcje

Definicja 31 *Funkcja* $\chi_A : X \to \{0, 1\}$ *jest nazywana funkcją charakterystyczną zbioru* A *wtedy gdy dla elementów zbioru* A *przyjmuje wartość* 1*, a dla pozostałych* 0*.*

$$\chi_A(x) = \begin{cases} 1 & dla\ x \in A \\ 0 & dla\ x \notin A \end{cases}$$

Definicja 32 *Funkcja* $f : X \to X$ *jest nazywana identycznościową wtedy gdy* $\forall x \in X : f(x) = x$*. Funkcję identycznościową będziemy oznaczać* 1_X*,* Id_X *lub* I_X*.*

Definicja 33 *Funkcją* $g : Y \to X$ *jest funkcją odwrotną do funkcji* $f : X \to Y$ *wtedy gdy* $g \circ f = 1_X \wedge f \circ g = 1_Y$*. Funkcję odwrotną do funkcji* f *będziemy oznaczać jako* f^{-1}*.*

Funkcja będzie nazywana odwracalną wtedy gdy będzie istniała dla niej funkcja odwrotna.

Twierdzenie 3 *Funkcja* $f : X \to Y$ *jest odwracalna wtedy i tylko wtedy gdy* f *jest bijekcją.*

(dowód twierdzenia można znaleźć w [5] rozdział 1.4. przykład 2)

Dowód „⇒"

chcę pokazać, że f *jest (a) iniekcją i (b) suriekcją, co na mocy poprzedniego twierdzenia dowodzi bijektywności* f

(a) iniektywność f

hipoteza: f nie jest różnowartościowa tzn.:$\exists x_1, x_2 \in X : x_1 \neq x_2 \wedge f(x_1) = f(x_2)$. Z odwracalności f istnieje $f^{-1} : f^{-1}(f(x)) = x$ zatem $x_1 = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = x_2$tzn.: $x_1 = x_2$ sprzeczność; cbdu.

(b) suriektywność f

Z definicji funkcji odwrotnej $f \circ f^{-1} = 1_Y$ tzn. $\forall y \in Y : f(f^{-1}(y)) = y$ przyjmijmy $x = f^{-1}(y)$ zatem $\forall y \in Y\, \exists x \in X : f(x) = y$ cbdu.

Dowód „⇐”

chcę skonstruować funkcje $g : Y \to X$ *spełniającą warunki (c)* $g \circ f = 1_X$ *oraz (d)* $f \circ g = 1_Y$.

Ponieważ f – bijekcja to na mocy definicji $\forall y \in Y \, \exists! x \, : \, f(x) = y$. Zatem dla funkcji $g : Y \to X$ przyjmiemy, iż wartością $g(y)$ będzię ów jedyny x spełniający równość $f(x) = y$. Zatem przepis na funkcję „pretendującą” do bycia funkcją odwrotną jest następujący: $g(y) = x$ gdzie $f(x) = y$.

(c) $\forall x \, : \, x = g(y) = g(f(x))$ co oznacza $g \circ f = 1_X$ cbdu.

(d) $\forall y \, : \, y = f(x) = f(g(y))$ co oznacza $f \circ g = 1_Y$ cbdu.

Liczność zbiorów

Każdemu zbiorowi przyporządkowujemy pewien obiekt zwany *liczbą kardynalną*. Liczby kardynalne ozaczamy zwykle literami alfabetu łacińskiego pisanymi gotykiem, lub literami alfabetu hebrajskiego. Jeśli zbiorowi X przyporządkowana jest liczba $\mathfrak{m}$, to piszemy $card(X) = \mathfrak{m}$.

Definicja 34 *Zbiory X i Y nazywamy równolicznymi wtedy i tylko wtedy gdy istnieje bijekcja $f : X \to Y$.*

Fakt równoliczności zbiorów oznaczać będziemy $card(X) = card(Y)$. Zbiorom równolicznym przyporządkowujemy tę samą liczbe kardynalną.

Definicja 35 *Zbiór X nazywamy zbiorem przeliczalnym wtedy gdy jest równoliczny ze zbiorem liczb naturalnych tj.:*

$$card(X) = card(\mathbb{N})$$

Liczność (moc) zbioru przeliczalnego oznaczamy symbolem $\aleph_0$ (alef–zero).

Definicja 36 *Zbiór X nazywamy zbiorem skończonym wtedy gdy:*

$$\exists n \in \mathbb{N} : card(X) = n$$

Definicja 37 *Zbiór X nazywamy zbiorem co najwyżej przeliczalnym wtedy gdy X jest zbiorem skończonym albo X jest zbiorem przeliczalnym.*

Problem z pojmowaniem zbiorów nieskończonych

- nieskończoność potencjalna
- nieskończoność aktualna

Paradoks Hilberta:

Paradoks ten znany jest też pod nazwą paradoksu Grand Hotelu lub paradoksu hotelu Hilberta. (David Hilbert 1862 – 1943).

Opisany przez Bernardo Bolzano w „Paradoksach"

Wyobraźmy sobie, że jesteśmy portierem w Grand Hotelu, w którym jest nieskończona liczba pokoi. Wszystkie pokoje są już zajęte gdy przychodzi do nas kolejny klient chcący wynająć pokój. Wydawałoby się, że sytuacja jest bez wyjścia i musimy klienta odprawić z kwitkiem. Na szczęście nasz hotel ma nieskończoną liczbę pokoi więc możemy wykonać sprytny trik: Klienta z pokoju numer 1 przekwaterujemy do pokoju nr. 2, tego z pokoju nr. 2 do pokoju nr. 3 itd. Ogólnie można powiedzieć że dokonujemy przekwaterowania klientów z pokojów n do pokojów n+1. W ten sposób wszyscy nasi wcześniejsi klienci mają gdzie mieszkać, a my mamy wolny pokój nr. 1, do którego możemy zakwaterować naszego nowego gościa. Tak więc mimo że hotel był pełen, znalazło się miejsce dla nowego klienta...

Będąc portierem w naszym nieskończonym hotelu mamy nawet jeszcze więcej możliwości. Nawet jeśli przyjedzie do nas nieskończona liczba autobusów z nieskończoną liczbą klientów w każdym z nich to nadal możemy ich wszystkich zakwaterować dokonując kolejnego, nieco bardziej złożonego triku z zamianami pokojów: Najpierw trzeba opróżnić pokoje hotelowe z nieparzystym numerem poprzez chwilowe umieszczenie ich gości w np: autobusie nr. 1. Klientów z autobusu nr. 1 umieszczamy w międzyczasie w pokojach z numerami 3^n, gdzie n to np: numery miejsc w autobusie (wszystkie te pokoje będą oczywiście nieparzyste, czyli już wcześniej opróżnione). Potem umieszczamy klientów z autobusu 2 w pokojach o numerach 5^n, Następny autobus pójdzie do pokojów 7^n. Ogólnie, będziemy umieszczali klientów kolejnych autobusów w pokojach m_i^n gdzie m_i to kolejne liczby pierwsze. Potęgi liczb pierwszych większych od 2 są nieparzyste, a że zbiory kolejnych potęg liczb pierwszych są parami rozłączne, więc nie ma ryzyka, że poślemy nowych klientów do już zajętych pokojów. Wreszcie klientów, wcześniej wykwaterowanych z pokojów nieparzystych, wysyłamy do pokojów o numerach m_{i+1}^n i wszyscy są już szczęśliwi...

Przykłady zbiorów różnej mocy:

Zbiory skończone:

- $card(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}) = 10$

- $card(\{czerwony, zielony, niebieski\}) = 3$
- zbiór wszystkich, niepustych słów Σ nad m elementowym alfabetem o długości nie większej niż k. $card(\Sigma) = m+m^2+m^3+...+m^k = \frac{m^{k+1}-m}{m-1}$.

Zbiory przeliczalne:

- dowolny nieskończony podzbiór zbioru liczb naturalnych np.: $\{1, 3, 5, 7, ...\}$, $\{1, 2, 4, 8, 16, 32, ...\}$ itd.
- zbiór liczb całkowitych $\mathbb{Z}$, wymiernych $\mathbb{Q}$, iloczyn kartezjański liczb naturalnych $\mathbb{N} \times \mathbb{N}$.

Równoliczność zbiorów oznacza się też symbolem „$\sim$”. Zamiast pisać zatem $card(X) = card(Y)$ można zapisać $X \sim Y$.

Twierdzenie 4 *Dowolny zbiór A jest przeliczalny, wtedy i tylko wtedy gdy jego elementy można ustawić w ciąg.*

Twierdzenie 5 *„Cantora – Bernsteina”*
Dla dowolnych liczb kardynalnych $\mathfrak{m}$ *i* $\mathfrak{n}$ *są prawdziwe następujące związki:*

1. $\mathfrak{m} \leqslant \mathfrak{m}$
2. $\mathfrak{m} \leqslant \mathfrak{n} \wedge \mathfrak{n} \leqslant \mathfrak{r} \Rightarrow \mathfrak{m} \leqslant \mathfrak{r}$
3. $\mathfrak{m} \leqslant \mathfrak{n} \wedge \mathfrak{n} \leqslant \mathfrak{m} \Rightarrow \mathfrak{m} = \mathfrak{n}$

Obserwacja
Jeśli pomiędzy dwoma zbiorami X i Y istnieje iniekcja $f : X \to Y$ to wtedy $card(X) \leqslant card(Y)$.

Fakt ten, w połączeniu z twierdzeniem Cantora-Bernsteina dostarcza łatwego sposobu dowodzenia równoliczności zbiorów. Zamiast bowiem często żmudnego konstruowania odwzorowania wzajemnie jednoznacznego, wystarczy wskazać odpowiedni ciąg iniekcji a następnie skorzystać z ostatniego punktu tezy twierdzenia.

Obserwacja

Odcinek obustronnie otwarty $(0,1)$ jest równoliczny z całym zbiorem $\mathbb{R}$ tj. $(0,1) \sim \mathbb{R}$. Odpowiednią bijekcję stanowi funkcja $f(x) = tan(\pi(x - \frac{1}{2}))$.

Obserwacja

Każdą liczbę rzeczywistą można zapisać w postaci nieskończonego rozwinięcia dziesiętnego.

Twierdzenie 6 ***„Przekątniowe" Cantora***

Zbiór liczb rzeczywistych nie jest przeliczalny

Dowód (niewprost)

Wystarczy pokazać, że odcinek $(0,1)$ nie jest przeliczalny. Przypuśćmy zatem, że zawiera on przeliczalną ilość punktów ω_1, ω_2, ω_3, ω_4, ... postaci:

$$\begin{array}{l} \omega_1 = 0,5142254657... \\ \omega_2 = 0,2536574783... \\ \omega_3 = 0,3464526546... \\ \omega_4 = 0,4765354253... \\ ..... \end{array}$$

Kolejność liczb ω_1, ω_2, ω_3, ω_4, ... nie ma znaczenia. Skonstruujmy liczbę $\sigma = 0.\sigma_1\sigma_2\sigma_3...$ taką, że:

$$\sigma_i = \begin{cases} 5 & \text{jeśli na i-tej pozycji } \omega_i \text{ nie posiada cyfry 5} \\ 4 & \text{jeśli na i-tej pozycji } \omega_i \text{ posiada cyfrę 5} \end{cases}$$

Widać, że σ jest różna od każdej liczby ω_i gdyż różni się od niej rozwinięciem dziesiętnym dokładnie na i-tej pozycji (na elementach przekątnej). W oczywisty sposób jest też liczbą rzeczywistą należącą do odcinka $(0,1)$, co daje porządaną sprzeczność.

Zbiór liczb rzeczywistych $\mathbb{R}$ jest nieprzeliczalny a jego moc oznaczamy symbolem $\mathfrak{c}$ (continuum).

Twierdzenie 7 *Liczność zbioru potęgowego wyraża się wzorem:*

$$card(2^X) = 2^{card(X)}$$

(Indukcyjny dowód twierdzenia można znaleźć w [5], p. 4.2. przykład 4b. Ogólny dowód można znaleźć w [3]).

Twierdzenie 8 *„Twierdzenie Cantora"*
Każdy zbiór jest mniej liczny niż jego zbiór potęgowy tj.:

$$card(X) \lneqq card(2^X)$$

Dowód twierdzenia można znaleźć w [3].

Dowód „$\leqslant$"
W przypadku gdy $X = \emptyset$ to twierdzenie jest prawdziwe:

$$0 = card(\emptyset) < card(2^{\emptyset}) = 1.$$

Przyjmijmy zatem, że $X \neq \emptyset$.
Zdefiniujmy funkcję $g : X \to 2^X$ taką, że $\forall x \in X : g(x) = \{x\} \in 2^X$. Przypisuje ona każdemu elementowi x zbiór jednoelementowy (singleton) postaci $\{x\}$ będący elementem zbioru 2^X. Funkcja g jest różnowartościowa (iniektywna) więc elementów należących do dziedziny funkcji jest nie więcej niż w przeciwdziedzinie. Dowodzi to słabej nierówności.

Dowód „$\neq$" (niewprost)
Hipoteza: załóżmy, że dla $X \neq \emptyset$ istnieje $A \subseteq X$ niepusty taki,
że $card(A) = card(2^X)$.
Zatem istnieje bijekcja $f : A \to 2^X$ $(^*)$. Ponieważ $\forall x \in A : f(x) \subset X$ (tj. obraz każdego elementu zbioru A poprzez funkcje f jest podzbiorem X) może się zdażyć, że $x \in f(x) \vee x \notin f(x)$. Niech $Z = \{x \in A : x \notin f(x)\}$. Oczywiście $Z \subseteq A \subseteq X$ oraz na mocy definicji zbioru Z prawdą jest:

$$x \in Z \Leftrightarrow x \notin f(x). \ (^{**})$$

Ponieważ na mocy hipotezy $(^*)$, f jest bijekcją to każdemu elementowi ze zbioru 2^Xprzypisuje ona jeden element zbioru A. W szczególności istnieje

$a \in A$ takie, że $Z = f(a)$ $(^{***})$. Sprawdźmy zatem czy $a \in Z$, czy też $a \notin Z$. Jeśli $a \in Z$ to z faktu $(^{**})$ $a \notin f(a)$ natomiast z faktu $(^{***})$ $a \in f(a)$ – sprzeczność; I odwrotnie: jeśli $a \notin Z$ to z faktu $(^{***})$ $a \notin f(a)$ ale tym samym spełnia definicje zbioru Z zatem $a \in Z$ – sprzeczność.

cbdu.

Wnioski z twierdzenia Cantora:

- Istnieją zbiory o mocy większej niż $\aleph_0$
  $\aleph_0 = card(\mathbb{N}) < card(2^{\mathbb{N}}) < card(2^{2^{\mathbb{N}}}) < card(2^{2^{2^{\mathbb{N}}}}) \ldots$
- nie istnieje zbiór wszystkich zbiorów.

Hipoteza continuum (pierwszy problem Hilberta):

„Czy każdy podzbiór zbioru $\mathbb{R}$ wszystkich liczb rzeczywistych jest albo conajwyżej przeliczalny albo mocy continuum".

Dowód wymaga dodatkowego aksjomatu teorii mnogości zwanego „pewnikiem wyboru".

Dyskusja wokół „pewnika wyboru":

- 1940 – Kurt Goedel (niesprzeczność z aksjomatami teori mnogości Zermelo–Fraenkla)
- 1963 – Paul Cohen (niezależność od aksjomatów teorii mnogości Zermelo–Fraenkla)

Definicja struktur grafu i drzewa. Drogi i ścieżki w grafie.

Definicja 38 *Niech N oznacza zbiór węzłów, a R będzie relacją dwuargumentową w N, tzn. $R \subseteq N \times N$. Grafem nazywamy parę postaci*

$$G = (N, R)$$

Jeżeli relacja R jest symetryczna to graf G jest grafem nieskierowanym. Jeżeli relacja jest asymetryczna to graf jest grafem skierowanym.

Definicja 39 *Niech N oznacza zbiór węzłów, a L zbiór łuków oraz niech będzie dana funkcja $\gamma : L \longrightarrow N \times N$. Grafem nazywamy trójkę postaci*

$$G = (N, L, \gamma)$$

Funkcja przypisuje krawędzi wierzchołki początkowy i końcowy.

Definicja 40 *Drogą o długości n z wierzchołka x do y nazywać będziemy ciąg krawędzi $e_1 ... e_n$ taki, że $e_i \in L$, $e_i = (x_i, x_{i+1})$,$x = x_1$, $y = x_{n+1}$.*
Droga będzie nazywana zamkniętą jeśli: $x = x_{n+1}$.

Definicja 41 *Ścieżką (drogą prostą) będzie nazywana droga, gdzie każda z krawędzi występuje conajwyżej raz.*

Definicja 42 *Cyklem będzie nazywana droga zamknięta, będąca ścieżką.*

Definicja 43 *Graf nie zawierający cykli jest nazywany grafem acyklicznym.*

Definicja 44 *Niech N oznacza zbiór węzłów. Drzewem T nazywamy graf (skierowany) spełniający następujace warunki:*

- *istnieje dokładnie jeden wezeł $n \in N$ nie bedący następnikiem żadnego wezła,*
- *każdy inny wezeł $m \in N$ jest następnikiem dla dokładnie jednego węzła,*
- *każdy węzeł $m \in N$ ma 0, 1 lub więcej następników.*

Węzeł n nazywany jest korzeniem drzewa (ang. root*). Węzły nie posiadajace następników nazywane sa liśćmi* (ang. leaf nodes*).*

Relacje częściowego porządku

Definicja 45 *Relację R określoną w zbiorze X, która jest zwrotna, antysymetryczna i przechodnia nazywamy relacją częściowego porządku w tym zbiorze.*

Relacja częściowego porządku pozwala porównywać elementy zbioru i szeregować je według pewnego kryterium; nie wszystkie elementy zbioru muszą być porównywalne.

Przykładami relacji częściowego porządku są relacje zawierania się zbiorów, wynikania logicznego (logicznej konsekwencji) wśród formuł, itp. Relację częściowego porządku oznacza się często symbolem „$\preceq$".

Jeżeli w zbiorze X określono relację częściowego porządku R, to parę (X, R) nazywamy ***zbiorem częściowo uporządkowanym***[1] (pisze się $(X, \preceq)$). Jeżeli para $(x,\ y) \in R$ to powiemy, że x poprzedza y; $(x \preceq y)$.

Element $x \in X$ nazywamy ***minimalnym***, gdy nie jest on poprzedzany przez żaden inny element zbioru X, tj.:

$$\forall y \in X\ :\ y \preceq x\ \Rightarrow y = x$$

Element $x \in X$ nazywamy ***maksymalnym***, gdy nie poprzedza on żadengo innego elementu zbioru X, tj.:

$$\forall y \in X\ :\ x \preceq y\ \Rightarrow y = x$$

Zauważmy, że w danym zbiorze częściowo uporządkowanym może być wiele elementów minimalnych (nieporównywalnych ze sobą) oraz wiele elementów maksymalnych (także nieporównywalnych ze sobą).

Jeżeli element $x \in X$ poprzedza każdy element rozważanego zbioru, to jest on nazywany ***elementem najmniejszym***, tj.:

$$\forall y \in X\ :\ x \preceq y$$

[1] ang. poset tj. partially ordered set.

Jeżeli każdy element zbioru X poprzedza $x \in X$, to x jest nazywany ***elementem największym***.

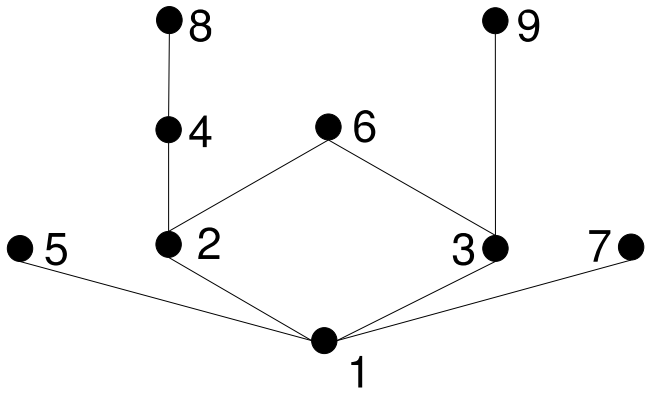
$$\forall y \in X \, : \, y \preceq x$$

W zbiorze częściowo uporządkowanym (skończonym) element najmniejszy i największy mogą nie istnieć (np. gdy jest wiele elementów minimalnych bądź maksymalnych).

Przykłady relacji „$\preceq$”: zawieranie się zbiorów ($\subseteq$), konsekwencja logiczna ($\models$), uporządkowanie hierarchiczne (drzewo), uporządkowanie ciągów, wektorów, krotek.

Definicja 46 *Diagramem Hassego relacji porządku $\preceq \subset N \times N$ nazywamy graf nieskierowany $G = (N, R)$, którego zbiorem wierzchołków jest zbiór N, a krawędzie są określone następująco: $(x, y) \in R \wedge \neg\exists\, z \, : \, x \prec z \prec y$. O parze (x, y) mówimy, że y jest bezpośrednim następnikiem x, a x bezpośrednim poprzednikiem y.*

Przykład: $N = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $R = \{(x, y) \, : \, x, y, x/y \in N\}$



Rysunek 1: Przykładowy diagram Hassego

Twierdzenie 9 *Każdy skończony zbiór częściowo uporządkowany ma diagram Hassego.*

Dowód można znaleźć w [5], str. 640.

Definicja 47 *Relację R określoną w zbiorze X, która jest przeciwzwrotna i przechodnia nazywamy quasi-porządkiem.*

Relację quasi-porządku często oznacza się symbolem „$\prec$". Każdy częściowy porządek w zbiorze X wyznacza pewien quasi-porządek i na odwrót. Jeśli „$\prec$" jest quasi-porządkiem to relacja „$\preceq$" jest zadana formułą:

$$x \preceq y \text{ wtedy i tylko wtedy, gdy } x \prec y \text{ lub } x = y$$

Relacja porządku

Definicja 48 *Relację R określoną w zbiorze X, która jest relacją częściowego porządku (jest zwrotna, antysymetryczna i przechodnia) oraz dodatkowo jest spójna nazywamy relacją porządku w tym zbiorze.*

Relację częściowego porządku nazywa się także relacją porządku; wówczas relacja porządku określana jest jako ***porządek liniowy***.

Relacja porządku w danym zbiorze pozwala na porównywanie dowolnych elementów tego zbioru i ustalenie który z nich poprzedza drugi element. Zbiór wraz z określoną na nim relacją liniowego porządku jest nazywany ***łańcuchem***. W skończonym zbiorze uporządkowanym istnieje zawsze element najmniejszy oraz element największy.

Definicja 49 *Niech $(X, \preceq)$ będzie zbiorem częściowo uporządkowanym, $X \subseteq U$. Element $u \in U$ nazywany jest ograniczeniem dolnym zbioru X, jeżeli dla każdego $x \in X$ zachodzi $u \preceq x$. Element $u \in U$ nazywany jest ograniczeniem górnym zbioru X, jeżeli dla każdego $x \in X$ zachodzi $x \preceq u$.*

W danym zbiorze może nie istnieć żaden element minimalny lub maksymalny. Pojęcia ograniczenia dolnego i ograniczenia górnego pozwalają „szacować" od dołu i od góry elementy tego zbioru. Wśród wszystkich ograniczeń dolnych (górnych) celowe jest wyodrębnienie tego największego (najmniejszego), o ile oczywiście, ono istnieje.

Definicja 50 *Niech $(X, \preceq)$ będzie zbiorem częściowo uporządkowanym, $X \subseteq U$. Największe ograniczenie dolne $i \in U$ nazywane jest kresem dolnym zbioru X (infimum). Najmniejsze ograniczenie górne $s \in U$ nazywane jest kresem górnym zbioru X (supremum).*

Jeżeli w danym zbiorze X istnieje element najmniejszy (największy), to jest on także ograniczeniem dolnym (górnym) tego zbioru. Jeżeli kres dolny (górny) istnieje, to jest on określony jednoznacznie. Kres dolny zbioru X oznacza się poprzez $\inf(X)$, a kres górny – poprzez $\sup(X)$.

Pewne szczególne porządki

Niech $(S_1, \preceq_1)$,...,$(S_n, \preceq_n)$ są zbioram częściowo uporządkowanymi.

Porządek produktowy:

Porządkiem produktowym określonym na elementach iloczynu kartezjańskiego $S_1 \times ... \times S_n$ będzie relacja „$\preceq$" zdefiniowana następująco:

$$(s_1, s_2, ..., s_n) \preceq (p_1, p_2, ..., p_n) \text{ jeśli } s_i \preceq_i p_i \text{dla wszstkich } i = 1, 2, ..., n.$$

Porządek leksykograficzny:

Dla elementów iloczynu kartezjańskiego $S_1 \times ... \times S_n$ zdefinujmy relację „$\prec$" następująco:

$(s_1, s_2, ..., s_n) \prec (p_1, p_2, ..., p_n)$ jeśli $s_1 \preceq_1 p_1$ lub jeśli istnieje $j \in \{2, ..., n\}$ takie, że $s_1 = p_1, ..., s_{j-1} = p_{j-1}$ i $s_j \preceq_j p_j$.

Porządkiem leksykograficznym określonym na elementach iloczynu kartezjańskiego $S_1 \times ... \times S_n$ będzie relacja „$\preceq$" zdefiniowana następująco:

$$(s_1, s_2, ..., s_n) \preceq (p_1, p_2, ..., p_n) \text{ wtw. } (s_1, s_2, ..., s_n) \prec (p_1, p_2, ..., p_n) \text{ lub } (s_1, s_2, ..., s_n) = (p_1, p_2, ..., p_n)$$

Elementy teorii krat

Pojęcie kraty stanowi rowinięcie pojęcia zbioru częściowo uporządkowanego $(X, \preceq)$. W kratach istnieje nie tylko możliwość porównywania niektórych elementów i ew. ich szeregowania, a także wyszukiwania elementów minimalnych i maksymalnych, ale także prowadzenia pewnych *operacji* na elementach, w szczególności operacji *sumy* i *iloczynu*.

Definicja 51 *Niech $(X, \preceq)$ będzie zbiorem częściowo uporządkowanym. Jeżeli dla dowolnych dwóch elementów $x, y \in X$ istnieje kres dolny oraz kres górny, to taki zbiór nazywamy kratą. W zbiorze X definiuje się działania sumy jako $x \vee y = \sup\{x, y\}$ oraz iloczynu jako $x \wedge y = \inf\{x, y\}$.*

Przykłady krat: zbiór wszystkich podzbiorów pewnego zbioru X wraz z relacją (słabego) zawierania się zbiorów (z działaniami sumu i iloczynu zbiorów), algebra Bool'a, zbiór krotek zoperacjami *min* oraz *max*, itp. Każdy zbiór (liniowo) uporządkowany jest kratą (z działaniami maksimum i minimum). Nie wszystkie elementy kraty można bezpośrednio porównać; zawsze jednak można dla nich określić kres górny i kres dolny.

Kraty można przedstawiać za pomocą ***grafu skierowanego***. Węzły odpowiadają elementom zbioru, a łuki relacji częściowego porządku. Dla każdych dwóch węzłów istnieją ścieżki zgodne ze skierowaniem grafu i łączące się w dokładnie jednym węźle, oraz ścieżki przeciwne do skierowania grafu i łączące się w dokładnie jednym węźle.

Kratę nazywamy ***zupełną***, jeżeli każdy podzbiór $X' \subseteq X$ ma kres dolny i kres górny.

- W dowolnej kracie każdy niepusty i skończony podzbiór ma kres górny i kres dolny.
- Każda krata skończona jest zupełna.
- Krata zupełna ma kres górny i kres dolny.

Kres górny przyjęto oznaczać jako $\top$ a kres dolny jako $\bot$. Jeżeli krata jest skończona, to elementy $\top$ oraz $\bot$ należą do tej kraty.

Struktura kraty stawia słabsze wymagania niż struktura zbioru (liniowo) uporządkowanego, a jednocześnie pozwala w sposób konstruktywny realizować operacje supremum (sumy, alternatywy, max) lub infimum (iloczynu, koniunkcji, min). Przykładem operacji sumy jest alternatywa logiczna. Przykładem operacji iloczynu jest koniunkcja logiczna.

Logika

Przedmiot logiki

Przedmiotem logiki matematycznej są następujące zagadnienia:

- formalna, symboliczna reprezentacja wiedzy; wiedza wyrażana w języku naturalnym jest zapisywana w postaci *formuł logicznych*,
- przetwarzanie wiedzy za pomocą reguł stanowiących schematy wnioskowania; w tym celu formułowane są *reguły wnioskowania*,
- badanie własności generowanych wniosków i systemów logicznych; własności te obejmuja m. in. *poprawność* i *zupełność*.

Klasyczna logika formalna bada mechanizmy rozumowań niezawodnych, w których otrzymywane wnioski są zawsze prawdziwe, o ile wychodzi się z prawdziwych przesłanek, a więc *wnioskowania dedukcyjnego*. Czasem dopuszcza się również inne schematy wnioskowania, prowadzące do użytecznych, chociaż nie zawsze prawdziwych wniosków (np. *abdukcja* oraz *indukcja*).

Alfabet rachunku zdań tworzą symbole formuł zdaniowych, łaczących je spójników (funkcji) logicznych oraz stosowane dla uporządkowania notacji nawiasy. Formuły zdaniowe symbolizują konkretne zdania; zdania te mogą być dobrze określone i wówczas można im przypisać ocenę *prawdy* albo *fałszu* lub też symbolizować pewne nieskonkretyzowane w danej chwili wypowiedzi.

W pierszym przypadku, takie skończone wypowiedzi, którym można jednoznacznie przypisać ocenę *prawdy* albo *fałszu*, nazywane będą *zdaniami*. Mogą one być zapisywane jawnie, np. "Śnieg jest biały", "W nocy jest ciemno", "Pada deszcz", itp. lub też przy użyciu pewnych symboli, np. p czy q. W drugim przypadku, formuła zdaniowa symbolizuje pewną bliżej nie sprecyzowaną wypowiedź, jednakże taką, której wartość logiczna może przyjąć wartość prawdy albo fałszu. W taki przpadku formuła zdaniowa nazywana jest *zmienną zdaniową*.

Logika

Istota wnioskowania logicznego

Chcąc przpisać konkretne znaczenie pewnej zmiennej zdaniowej można zastosować notację postaci

$$p \stackrel{\text{def}}{=} \text{“W nocy jest ciemno”},$$

co oznacza, że p staje się skrótowym zapisem podanego zdania. Ponadto, bardzo często rozważa się symbole formuł zdaniowych nie przypisując im konkretnego znaczenia, a jedynie wartość prawdy lub fałszu. Takie przypisanie nosi nazwę określenia lub nadania *interpretacji* formule zdaniowej (zmiennej zdaniowej).

Aby móc prowadzić wnioskowanie logiczne potrzebny jest zbiór formuł definiujących pewną wiedzę oraz reguły dla ich przetwarzania. Reguły przetwarzania wiedzy zazwyczaj formułowane są w postaci schematu:

$$\frac{\text{przesłanki reguły}}{\text{konkluzje}}.$$

Przykładem reguły wnioskowania jest popularna reguła *modus ponens* o następującym schemacie:

$$\frac{\alpha, \alpha \Longrightarrow \beta}{\beta}.$$

Na przykład, dysponując przesłankami $\alpha =$ *pada deszcz* oraz $\beta =$ *jeżeli pada deszcz to ulice są mokre* (logicznie: pada deszcz $\Longrightarrow$ ulice są mokre) możemy skorzystać z reguły *modeus ponens* wnioskując wg schematu:

$$\frac{\text{pada deszcz},\ \text{pada deszcz} \Longrightarrow \text{ulice są mokre}}{\text{ulice są mokre}}.$$

Otrzymujemy zatem konkluzję, że *ulice sa mokre*, która stanowi nowo wydedukowany fakt.

Logika

Spójniki i formuły logiczne

Z formuł atomowych bardziej złożone formuły budowane są przy pomocy odpowiednich *spójników logicznych*. Najczęściej stosowane są następujące spójniki logiczne:

- $\neg$ – negacja,
- $\wedge$ – koninkcja,
- $\vee$ – alternatywa,
- $\Rightarrow$ – implikacja (może być również postaci $\Leftarrow$),
- $\Leftrightarrow$ – równoważność (implikacja dwustronna).

Przy wykorzystaniu powyższych spójników logicznych i symboli formuł zdaniowych (formuł atomowych) buduje się bardziej złożone formuły logiczne rachunku zdań. Nie wszystkie jednak możliwe do utworzenia napisy będą formułami. Poniżej podano definicję poprawnie skonstruowaych formuł.

Definicja 52 ***Formuły rachunku zdań*** *Niech* $\boldsymbol{P}$ *będzie zbiorem symboli formuł atomicznych. Zbiór poprawych formuł rachunku zdań (krótko: formuł)* $\boldsymbol{FOR}$*jest zdefiniowane rekurencyjnie jak następuje:*

1. *Jeżeli* $p \in \boldsymbol{P}$ *to* $p \in \boldsymbol{FOR}$,
2. *Jeżeli* $\phi \in \boldsymbol{FOR}$ *to* $(\neg\phi) \in \boldsymbol{FOR}$,
3. *Jeżeli* $\phi, \psi \in \boldsymbol{FOR}$ *to* $(\psi \wedge \phi) \in \boldsymbol{FOR}$, $(\psi \vee \phi) \in \boldsymbol{FOR}$, $(\psi \Rightarrow \phi) \in \boldsymbol{FOR}$ *oraz* $(\psi \Leftrightarrow \phi) \in \boldsymbol{FOR}$,
4. *Wszystkie formuły muszą być generowane zgodnie z powyższymi regułami.*

Logika

Semantyka rachunku zdań

Formułom atomowym i złożonym przypisywana jest ocena prawdy lub fałszu. Aktualna ocena formuły zależy od przypisania wartości logicznych występującym w niej formułom atomowym oraz od konstrukcji samej formuły. Poniżej wprowadzono ważne pojęcie *interpretacji* formuł atomowych w rachunku zdań.

Definicja 53 *Niech* $\boldsymbol{P}$ *będzie zbiorem rozważanych symboli formuł atomowych a* $\boldsymbol{T}$ *wyróżnionym zbiorem wartości logicznych, tj.* $\boldsymbol{T} = \{true, false\}$. *Interpretacja symboli zbioru* $\boldsymbol{P}$ *nazywa się każdą funkcję postaci:*

$$I : \boldsymbol{P} \longrightarrow \boldsymbol{T}$$

przyporządkowującą każdemu symbolowi formuły atomowej wartość logiczną prawdy albo fałszu.

Interpretacja określa zatem czy dana formuła atomowa jest uznawana za prawdziwą czy też fałszywą. Przy danej interpretacji formuła może być prawdziwa lub fałszywa; w przypadku gdy interpretacja nie przypisywałaby jednoznacznie wartości logicznej prawdy albo fałszu wszystkim symbolom rozważanego zbioru, interpretację taką okresla się jako niepełną lub częściową.

Definicja 54 *Dwie formuły* ϕ *oraz* ψ *mające identyczną wartość logiczną przy każdej interpretacji* I $(I(\phi) = I(\psi))$ *nazywamy* logicznie równoważnymi.

Pojęcie interpretacji należy rozszerzyć na zbiór wszystkich formuł **FOR**. Odpowiednia definicja ma charakter rekurencyjny.

Logika

Semantyka – określanie wartości logicznej formuł

Definicja 55 *Niech* $\boldsymbol{P}$ *oznacza zbiór rozważanych symboli formuł atomowych,* $\boldsymbol{T}$ *– dwuelementowy zbiór wartości logicznych, a* I *– interpretację. Interpretacja* I *przypisuje wartości logiczne wszystkim formu@lom* ϕ, ψ *ze zbioru* $\boldsymbol{FOR}$, *tzn.:*

$$I : \boldsymbol{FOR} \longrightarrow \boldsymbol{T},$$

utworzonym wyłącznie w oparciu o symbole występujące w $\boldsymbol{P}$ *zgodnie z następującymi zasadami:*

1. $I(\neg\phi) = true$ *wtw. gdy* $I(\phi) = false$ *oraz* $I(\neg\phi) = false$ *wtw. gdy* $I(\phi) = true$,
2. $I(\phi \wedge \psi) = true$ *wtw. gdy* $I(\phi) = true$ *oraz* $I(\psi) = true$; *w pozostałych przypadkach* $I(\phi \wedge \psi) = false$,
3. $I(\phi \vee \psi) = true$ *wtw. gdy* $I(\phi) = true$ *lub* $I(\psi) = true$; *w pozosta@lym przypadku* $I(\phi \vee \psi) = false$,
4. $I(\phi \Rightarrow \psi) = true$ *wtw gdy* $I(\phi) = false$ *lub* $I(\phi) = true$ *oraz jednocześnie* $I(\psi) = true$; *w pozostałym przypadku* $I(\phi \wedge \psi) = false$,
5. $I(\phi \Leftrightarrow \psi) = true$ *wtw. gdy* $I(\phi) = I(\psi)$; *w pozostałych przypadkach* $I(\phi \Leftrightarrow \psi) = false$.

Powyższa definicja pozwala rekurencyjnie ustalić wartość logiczną dowolnie skonstruowanej i dowolnie złożonej poprawnej formuły rachunku zdań o ile tylko znane są wartości logiczne wszystkich występujących w niej formuł atomowych.

Logika

Tabele wartości logicznych

Zamiast symboli prawdy i fałszu czesto stosujemy zapis uproszczony: 1 zamiast prawdy i 0 zamiast fałszu. Tablica prawdy dla negacji przybiera postać:

p	$\neg p$
0	1
1	0

Tablica prawdy dla koninukcji przybiera postać:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Tablica prawdy dla dysjunkcji przybiera postać:

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Tablica prawdy dla implikacji przybiera postać:

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Logika

Sematyka rachunku zdań

Często podana powyżej definicja przedstawiana jest w formie jest tabeli ilustrującej podane zależności logiczne (patrz poniżej).

ϕ	ψ	$\neg\phi$	$\phi \wedge \psi$	$\phi \vee \psi$	$\phi \Rightarrow \psi$	$\phi \Leftrightarrow \psi$
true	*true*	*false*	*true*	*true*	*true*	*true*
true	*false*	*false*	*false*	*true*	*true*	*true*
false	*true*	*true*	*false*	*true*	*true*	*false*
false	*false*	*true*	*false*	*false*	*true*	*true*

Semantykę wybranych funkcji można definiować za pomocą sprowadzenia jej do równoważnej formuły zawierajacej symbole koniunkcji, dysjunkcji i negacji.

- $\phi \Rightarrow \psi \equiv \neg\phi \vee \psi$,
- $\phi \Leftrightarrow \psi \equiv (\phi \Rightarrow \psi) \wedge (\phi \Leftarrow \psi)$,
- $\phi|\psi \equiv \neg(\phi \wedge \psi)$ – funkcja (kreska) Sheffera, jest to tzw. funkcja `NAND`; inna notacja $\overline{\phi \wedge \psi}$,
- $\phi \downarrow \psi \equiv \neg(\phi \vee \psi)$ – funkcja (strzałka) Pierce'a, jest to tzw. funkcja `NOR`; inna notacja $\overline{\phi \vee \psi}$,
- $\phi \bigoplus \psi \equiv (\neg\phi \wedge \psi) \vee (\phi \wedge \neg\psi)$ – funkcja alternatywy wykluczającej, jest to tzw. funkcja `EX-OR`,
- $\neg\phi \vee \psi$ oraz $\phi \vee \neg\psi$ – funkcje zakazu lub różnice niesymetryczne.

Ogólnie dla n argumentów wejściowych można skonstruować 2^{2^n} różnych funkcji, a więc dla $n = 2$ jest 16 różnych funkcji.

Logika

Ważniejsze prawa logiczne

- $\neg\neg p \equiv p$ – prawo podwójnego przeczenia,
- $p \wedge q \equiv q \wedge p$ – prawo przemienności koninkcji,
- $p \vee q \equiv q \vee p$ – prawo przemienności alternatywy,
- $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ – prawo łączności koninkcji,
- $(p \vee q) \vee r \equiv p \vee (q \vee r)$ – prawo łączności koninkcji,
- $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$ – prawo rozdzielności koninkcji względem alternatywy,
- $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ – prawo rozdzielności alternatywy względem koninkcji,
- $p \wedge p \equiv p$ – prawo idempotentności dla koninkcji,
- $p \vee p \equiv p$ – prawo idempotentności dla alternatywy,
- $p \wedge 0 \equiv 0$, $p \wedge 1 \equiv p$ – prawo identyczności,
- $p \vee 0 \equiv p$, $p \vee 1 \equiv 1$ – prawo identyczności,
- $p \vee \neg p \equiv 1$ – prawo wyłączonego środka,
- $p \wedge \neg p \equiv 0$ – prawo sprzeczności,
- $\neg(p \wedge q) \equiv \neg(p) \vee \neg(q)$ – prawo De Morgana,
- $\neg(p \vee q) \equiv \neg(p) \wedge \neg(q)$ – prawo De Morgana,
- $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ – prawo kontrapozycji,
- $p \Rightarrow q \equiv \neg p \vee q$ – określenie implikacji za pomoca alternatywy.

Postacie specjalne formuł logicznych

Normalna postać koniunktywna

Każda formuła logiczna rachunku zdań może być sprowadzona do postaci równoważnej, w której formuły atomowe i ich negacje bedą połączone symbolem alternatywy, a tak utworzone formuły – symbolem koniunkcji; jest to tzw. *normalna postać koniuntywna, CNF* i przybiera następującą formę:

$$(p_1 \vee p_2 \vee \ldots p_k) \wedge (q_1 \vee q_2 \vee \ldots q_l) \wedge \ldots (s_1 \vee s_2 \vee \ldots s_m).$$

Normalna postać dysjunktywna

Każda formuła logiczna rachunku zdań może być sprowadzona do postaci równoważnej, w której formuły atomowe i ich negacje bedą połączone symbolem koninkcji, a tak utworzone formuły – symbolem alternatywy; jest to tzw. *normalna postać dysjunktywna, DNF* i przybiera następującą formę:

$$(p_1 \wedge p_2 \wedge \ldots p_k) \vee (q_1 \wedge q_2 \wedge \ldots q_l) \vee \ldots (s_1 \wedge s_2 \wedge \ldots s_m).$$

Normalna postać prawdy/jedynki oraz fałszu/zera

Formuła zawsze prawdziwa zawierająca n zmiennych zdaniowych może zostać przedstawiona w postaci DNF w jednoznaczny sposób i składa się ona z 2^n różnych koniunkcji, każda o n składowych, np.:

$$1 = pqr \vee pq\bar{r} \vee p\bar{q}r \vee p\bar{q}\bar{r} \vee \bar{p}qr \vee \bar{p}q\bar{r} \vee \bar{p}\bar{q}r \vee \bar{p}\bar{q}\bar{r} \qquad \text{(DNF)}$$

Formuła zawsze fałszywa zawierająca n zmiennych zdaniowych może zostać przedstawiona w postaci CNF w jednoznaczny sposób i składa się ona z 2^n różnych dysjunkcji, każda o n składowych, np.:

$$0 = pqr \wedge pq\bar{r} \wedge p\bar{q}r \wedge p\bar{q}\bar{r} \wedge \bar{p}qr \wedge \bar{p}q\bar{r} \wedge \bar{p}\bar{q}r \wedge \bar{p}\bar{q}\bar{r} \qquad \text{(CNF)}$$

Związki pomiędzy zdaniami logicznymi

Zdanie proste

$$p \Rightarrow q$$

Zdanie odwrotne

$$q \Rightarrow p$$

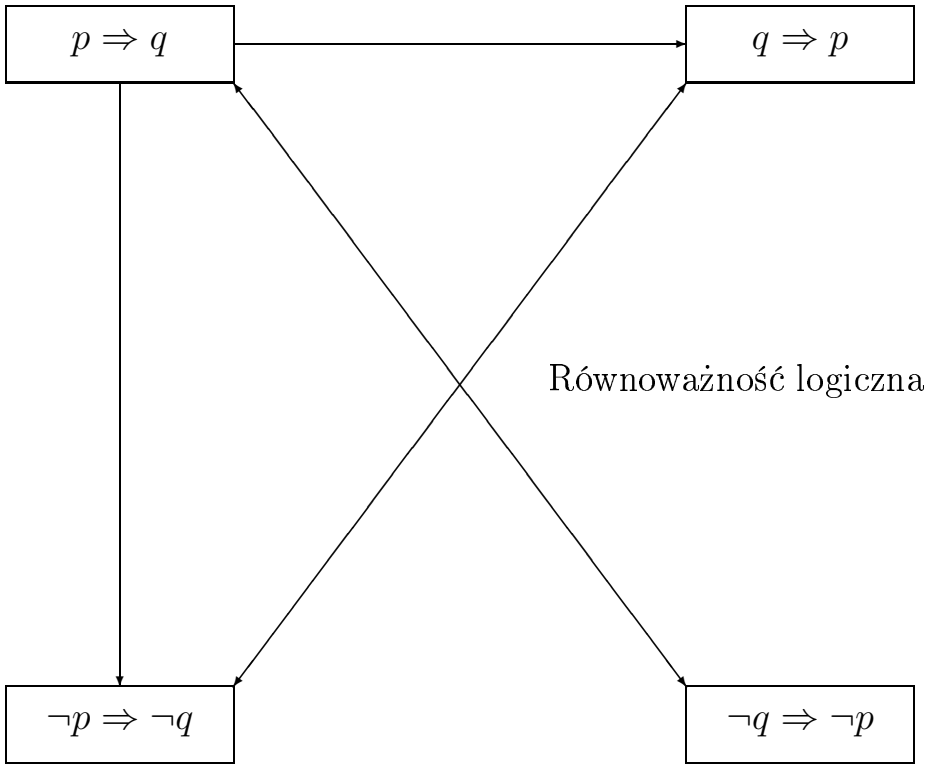
Zdanie przeciwne

$$\neg p \Rightarrow \neg q$$

Zdanie przeciwstawne

$$\neg q \Rightarrow \neg p$$

Kwadrat logiczny:



Metoda zerojedynkowa

Zastosowania metody zero-jedynkowej

Metoda zerojedynkowa polega na budowie i analizie **matrycy logicznej** formuły; może być stosowana do:

- weryfikacji tautologii (dla każdej interpretacji wartość logiczna formuły jest *true*,
- weryfikacji niespełnialności (dla każdej interpretacji wartość logiczna formuły jest *false*,
- badania równoważności formuł (dla każdej interpretacji wartości logiczne są takie same),
- weryfikacji logicznej konsekwencji (dla każdej interpretacji prawdziwość formuły musi pociągać prawdziwośc jej konsekwencji),
- wyznaczania interpretacji przy których formuła jest prawdziwa lub fałszywa.

Przykład. sprawdzimy, że formuła Φ jest tautologią.

$$\Phi = ((p \Rightarrow r) \wedge (q \Rightarrow r)) \Leftrightarrow ((p \vee q) \Rightarrow r)$$

p	q	r	$p \Rightarrow r$	$q \Rightarrow r$	$(p \Rightarrow r) \wedge (q \Rightarrow r)$	$(p \vee q) \Rightarrow r$	Φ
0	0	0	1	1	**1**	**1**	**1**
0	0	1	1	1	**1**	**1**	**1**
0	1	0	1	0	**0**	**0**	**1**
0	1	1	1	1	**1**	**1**	**1**
1	0	0	0	1	**0**	**0**	**1**
1	0	1	1	1	**1**	**1**	**1**
1	1	0	0	0	**0**	**0**	**1**
1	1	1	1	1	**1**	**1**	**1**

Wprowadzenie do logiki

Przykład zastosowania metody zero-jedynkowej

Zbadamy prawdziwość implikacji logicznej postaci:

$$\frac{(p \Rightarrow q) \wedge (r \Rightarrow s)}{(p \vee r) \Rightarrow (q \vee s)}$$

p	q	r	s	$p \Rightarrow q$	$r \Rightarrow s$	$(p \Rightarrow q) \wedge (r \Rightarrow s)$	$p \vee r$	$q \vee s$	$(p \vee r) \Rightarrow (q \vee s)$
0	0	0	0	1	1	**1**	0	0	**1**
0	0	0	1	1	1	**1**	0	1	**1**
0	0	1	0	1	0	**0**	1	0	**0**
0	0	1	1	1	1	**1**	1	1	**1**
0	1	0	0	1	1	1	0	1	1
0	1	0	1	1	1	1	0	1	1
0	1	1	0	1	0	0	1	1	1
0	1	1	1	1	1	1	1	1	1
1	0	0	0	0	1	0	1	0	0
1	0	0	1	0	1	0	1	1	1
1	0	1	0	0	0	0	1	0	0
1	0	1	1	0	1	0	1	1	1
1	1	0	0	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1	1
1	1	1	0	1	0	0	1	1	1
1	1	1	1	1	1	1	1	1	1

Z analizy kolumn 7 i 10 wynika, że implikacja jest prawdziwa. Poza wierszami 7, 10, 12 i 15 zachodzi ponadto równoważność.

Wprowadzenie do logiki

Ważniejsze reguły wnioskowania

- $\frac{p}{p \vee q}$ – reguła wprowadzania alternatywy,
- $\frac{p,\, q}{p \wedge q}$ – reguła wprowadzania koninkcji,
- $\frac{p \wedge q}{p}$ – reguła opuszczania koniunkcji,
- $\frac{p,\, p \Rightarrow q}{q}$ – reguła modus ponens (modus ponendo ponens),
- $\frac{p \Rightarrow q,\, \neg q}{\neg p}$ – reguła modus tollens (modus tollendo tollens),
- $\frac{p \vee q,\, \neg p}{q}$ – reguła ponendo tollens,
- $\frac{p \bigoplus q,\, p}{\neg q}$ – reguła ponendo tollens,
- $\frac{p \Rightarrow q,\, q \Rightarrow r}{p \Rightarrow r}$ – reguła przechodniości (reguła sylogizmu hipotetycznego),
- $\frac{p \vee r,\, \neg r \vee q}{p \vee q}$ – reguła rezolucji,
- $\frac{p \wedge r,\, \neg r \wedge q}{p \wedge q}$ – odwrotna reguła rezolucji (konkluzja logiczna jest odwrócona),
- $\frac{p \Rightarrow q,\, r \Rightarrow s}{(p \vee r) \Rightarrow (q \vee s)}$ – prawo dylematy konstrukcyjnego,
- $\frac{p \Rightarrow q,\, r \Rightarrow s}{(p \wedge r) \Rightarrow (q \wedge s)}$ – prawo dylematy konstrukcyjnego.

Sprowadzanie dowolnych formuł do postaci normalnych

Sprowadzanie do CNF/DNF

1. $\Phi \Leftrightarrow \Psi \equiv (\Phi \Rightarrow \Psi) \wedge (\Psi \Rightarrow \Phi)$ – eliminacja symboli równoważności,
2. $\Phi \Rightarrow \Psi \equiv \neg\Phi \vee \Psi$ – eliminacja symboli implikacji,
3. $\neg(\neg\Phi) \equiv \Phi$ – eliminacja zagnieżdżonych negacji,
4. $\neg(\Phi \vee \Psi) \equiv \neg\Phi \wedge \neg\Psi$ – zastosowanie prawa De Morgana do sprowadzania symbolu negacji bezpośrednio przed formułę atomową,
5. $\neg(\Phi \wedge \Psi) \equiv \neg\Phi \vee \neg\Psi$ – zastosowanie prawa De Morgana do sprowadzania symbolu negacji bezpośrednio przed formułę atomową,
6. $\Phi \vee (\Psi \wedge \Upsilon) \equiv (\Phi \vee \Psi) \wedge (\Phi \vee \Upsilon)$ – zastosowanie prawa rozdzielności alternatywy przy sprowadzaniu do CNF,
7. $\Phi \wedge (\Psi \vee \Upsilon) \equiv (\Phi \wedge \Psi) \vee (\Phi \wedge \Upsilon)$ – zastosowanie prawa rozdzielności koninkcji przy sprowadzaniu do DNF.

Przykład:

$$(p \wedge (p \Rightarrow q)) \Rightarrow q = \neg(p \wedge (p \Rightarrow q)) \vee q = \\ \neg(p \wedge \neg(p \vee q)) \vee q = (\neg p \vee \neg\neg(p \vee q)) \vee q = \\ (\neg p \vee (p \vee q)) \vee q = (\neg p \vee p \vee p \vee q) \vee q = \\ (\neg p \vee p \vee q = 1 \vee q = 1.$$

Sprowadzenie do postaci normalnej formuły zawsze prawdziwej (zawsze fałszywej) pozwala określić jej wartość logiczną.

Podstawowe definicje, określenia i twierdzenia

Definicja 56 *Formuła jest nazywana:*

- tautologią *wtw. gdy jest prawdziwa przy każdej interpretacji;*
- formułą falsyfikowalną *gdy nie jest tautologią,*
- formułą spełnialną *wtw. gdy istnieje taka interpretacja, przy której formuła ta jest prawdziwa;*
- formułą niespełnialną, formułą niespójną *lub* formułą sprzeczną *wtw. gdy przy każdej interpretacji fromuła ta jest fałszywa;*
- *fomuła* Ψ *jest* logiczną konsekwencją *formuły* Φ, *co notujemy* $\Phi \models \Psi$ *wtw. gdy dla każdej interpretacji przy której* Φ *jest prawdziwa również* Ψ *jest prawdziwa;*
- *formuła* Ψ *jest* wyprowadzalna *z formuły* Φ, *co notujemy* $\Phi \vdash \Psi$ *wtw. gdy istnieje ciąg reguł dowodzenia pozwalajacy uzyskać* Ψ *z* Φ.

Konsekwencje tych definicji:

- formuła jest tautologią wtw. gdy jej negacja jest niespełnialna (sprzeczna),
- formuła jest niespełnialna wtw. gdy jej negacja jest tautologią,
- formuła nie jest tautologią wtw. dla przynajmniej jednej inteerpretacji jest fałszywa,
- formuła jest niesprzeczna wtw. gdy dla przynajmniej jednej interpretacji jest prawdziwa,
- tautologia jest zawsze formułą spełnialną (ale nie odwrotnie),
- formuła niespełnialna jest formułą falsyfikowalną (ale nie odwrotnie).

Zasady dowodzenia

Twierdzenia o dedukcji

Twierdzenie 10 *Jeżeli* $\Delta_1, \Delta_2, \ldots \Delta_n$ *są formułami logicznymi (nazywanymi aksjomatami), formuła* Ω *(nazywana hipotezą lub konkluzją) jest ich logiczną konsekwencją wtw. gdy formuła* $\Delta_1 \wedge \Delta_2 \wedge \ldots \Delta_n \Rightarrow \Omega$ *jest tautologią.*

Twierdzenie 11 *Jeżeli* $\Delta_1, \Delta_2, \ldots \Delta_n$ *są formułami logicznymi (nazywanymi aksjomatami), formuła* Ω *(nazywana hipotezą lub konkluzją) jest ich logiczną konsekwencją wtw. gdy formuła* $\Delta_1 \wedge \Delta_2 \wedge \ldots \Delta_n \wedge \neg\Omega$ *jest sprzeczna.*

Problem dowodzenia twierdzeń ma postać: mając dane aksjomaty $\Delta_1, \Delta_2, \ldots \Delta_n$ uznane za prawdziwe wykazać prawdziwość hipotezy Ω. Tak więc należy wykazać, że:

$$\Delta_1 \wedge \Delta_2 \wedge \ldots \Delta_n \models \Omega$$

Stosowane są następujące metody:

- sprawdzanie wszystkich możliwych interpretacji (wada: duża złożoność obliczeniowa),
- *dowód wprost* – korzystając z aksjomatów i reguł dowodzenia generujemy nowe formuły aż do uzyskania formuły Ω,
- *dowodzenie tautologii* – korzystając z Tw.1 dowodzimy, że formuła $\Delta_1 \wedge \Delta_2 \wedge \ldots \Delta_n \Rightarrow \Omega$ jest tautologią,
- *dowód nie wprost* – to dowód twierdzenia przeciwstawnego, równoważnego danemu. Polega na dowodzeniu twierdzenia postaci $\neg\Omega \models \neg(\Delta_1 \wedge \Delta_2 \wedge \ldots \Delta_n)$.
- dowód przez *sprowadzenie do sprzeczności*; korzystają z Tw.2, polega na wykazaniu sprzeczności formuły: $\Delta_1 \wedge \Delta_2 \wedge \ldots \Delta_n \wedge \neg\Omega$.

Algebra Boole'a

Algebra Boole'a jest strukturą matematyczną postaci:

$$(\{0,1\}, \vee, \wedge, \neg, 0, 1),$$

gdzie dany jest zbiór dwuelementowy, działania alternatywy (sumy), koniunkcji (iloczynu) oraz negacji (dopełnienia), a także element neutralny sumy i iloczynu. Dla uproszczenia zapisu koniunkcję $p \wedge q$ zapisujemy jako $p \cdot q$ lub pq, a negację $\neg p$ jako $\bar{p}$. Działania alegbry Boole'a spełniają następujące prawa:

- element neutralny: $p \vee 0 = p$, $p \cdot 1 = p$,
- identyczność: $p \vee 1 = 1$, $p \cdot 0 = 0$,
- idempotentność: $p \vee p = p$, $p \cdot p = p$,
- dopełnianie: $p \vee \bar{p} = 1$, $p \cdot \bar{p} = 0$,
- przemienność: $p \vee q = q \vee p$, $p \wedge q = q \wedge p$,
- łączność: $(p \vee q) \vee r = p \vee (q \vee r)$, $(p \wedge q) \wedge r = p \wedge (q \wedge r)$,
- rozdzielność: $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$,
- pochłanianie: $(p \wedge q) \vee p = p$, $(p \vee q) \wedge p = p$,
- prawa De Morgana: $\overline{p \vee q} = \bar{p} \wedge \bar{q}$, $\overline{p \wedge q} = \bar{p} \vee \bar{q}$.

Przykładami algebr Boole'a są:

- Algebra zerojedynkowa: $(\{0,1\}, \vee, \wedge, \neg, 0, 1)$,
- Zbiory: $(2^S, \cap, \cup, \bar{X}, \emptyset, S)$,
- Ciągi zerojedynkowe o długości n:
  $(\{ppp\ldots p : p \in \{0,1\}\}, \vee, \wedge, \neg, 000\ldots0, 111\ldots1)$.

Funkcje Booleowskie

Niech $\mathbf{B} = \{0, 1\}$. Funkcją booleowską n-argumentową nazywamy dowolną funkcję typu:

$$f : \mathbf{B}^n \longrightarrow \mathbf{B}.$$

W ogólnym przypadku istnieje 2^{2^n} różnych funkcji booleowskich. Dla $n = 1$ mamy cztery funkcje, dla $n = 2$ jest ich 16 a dla $n = 3$ aż 256.

Przykład funkcji 3-argumentowej przedstawiono poniżej.

wartość	p	q	r	$f(p, q, r)$
0	0	0	0	0
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	1
6	1	1	0	1
7	1	1	1	1

Funkcja f dla $p = 0$ realizuje koniunkcję pozostałych argumentów, a dla $p = 1$ – ich alternatywę; można więc ją zapisać w postaci:

$$f(p, q, r) = \bar{p} \cdot (q \cdot r) \vee p \cdot (q \vee r).$$

Inna postać tej funkcji:

$$f(p, q, r) = \bar{p} \cdot q \cdot r \vee p \cdot \bar{q} \cdot r \vee p \cdot q \cdot \bar{r} \vee p \cdot q \cdot r.$$

Używany jest też inny wygodny zapis:

$$f(p, q, r) = \Sigma(3,\ 5,\ 6,\ 7)$$

Wyrażenia postaci $x \cdot y \cdot z$, lub prościej xyz, gdzie $x = p$ lub $x = \bar{p}$, $y = q$ lub $y = \bar{q}$ oraz $z = r$ lub $z = \bar{r}$ nazywamy atomami (iloczynami) w $\mathbf{B}^3$. Różnych takich atomów jest 2^n. Każdą funkcję można przedstawić jako sumę atomów.

Postać minimalna:

$$f(p, q, r) = p \cdot q \vee p \cdot r \vee \vee q \cdot r.$$

Wyrażenia booleowskie

Wyrażenia booleowskie służą do zapisu i definiowania funkcji booleowskich.

Definicja 57 *Niech będą dane symbole zmiennych booleowskich* $p_1, p_2, \ldots, p_n$. *Wyrażeniem booleowskicm jest:*

- *symbol* 0, 1 *oraz każdy z symboli* $p_1, p_2, \ldots, p_n$,
- *jeżeli* P_1 *i* P_2 *sa wyrażeniami booleowskimi, to również* $P_1 \vee P_2$, $P_1 \wedge P_2$ *oraz* $\bar{P}_1$ *(*$\bar{P}_2$*) sa wyrażeniami booleowskimi.*

Każde wyrażenie booleowskie definiuje pewna funkcje booleowską. Wartości tej funkcji dla konkretnego wyrażenia wyznaczamy stosując reguły algebry Boole'a.

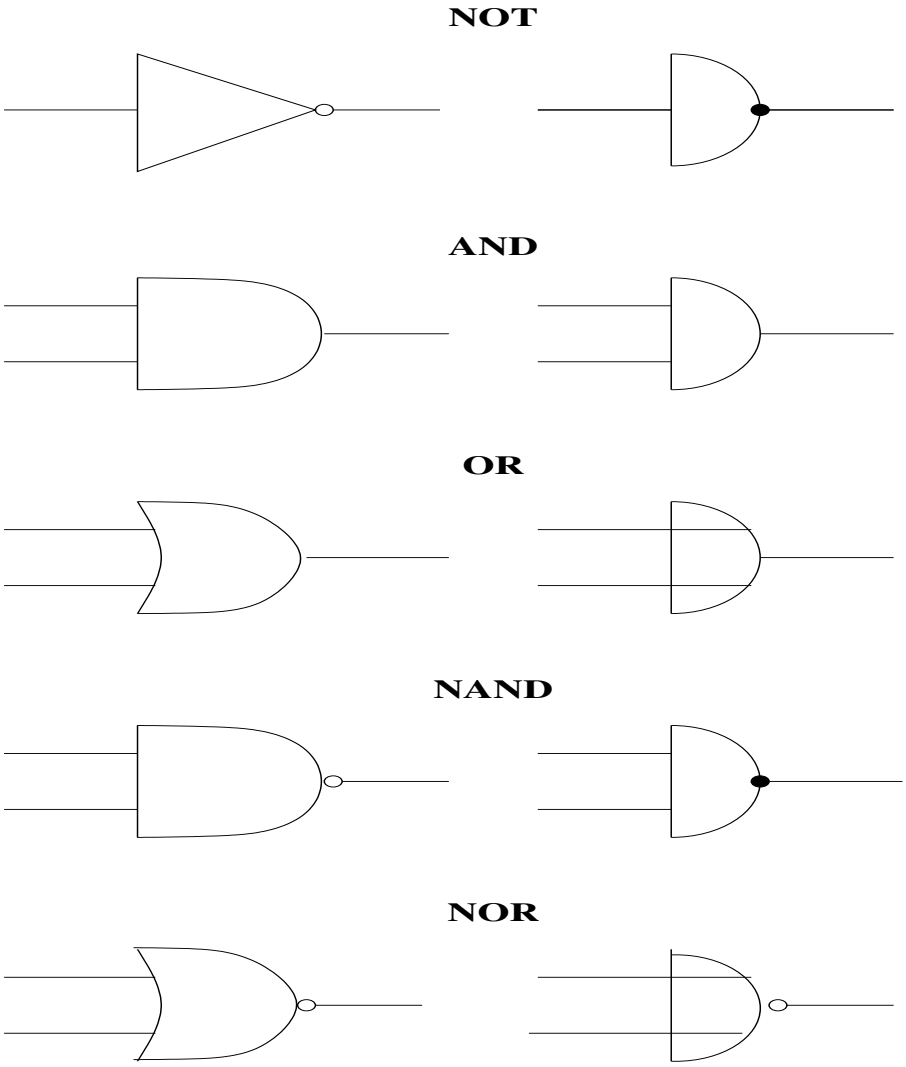
Dwa wyrażenia booleowskie nazywamy **równoważnymi** gdy definiują one identyczne funkcje.

Iloczynem minimalnym n zmiennych booleowskich nazywamy koniunkcję (atom w $\mathbf{B}^n$) n zmiennych; żadna zmienna nie może się powtarzać.

Każdą funkcję i każde wyrażenie booleowskie można przedstawić w równoważnej postaci składającej się z samych iloczynów minimalnych - jest to tzw. postać kanoniczna (postać normalna alternatywno-koniunkcyjna). Określenie postaci kanonicznej polega na wskazaniu które iloczyny minimalne wchodzą $(+)$ do definicji funkcji, a które nie wchodza $(-)$.

p	q	r	iloczyn	$f(p,q,r)$	czy wchodzi
0	0	0	$\bar{p}\bar{q}\bar{r}$	0	$-$
0	0	1	$\bar{p}\bar{q}r$	0	$-$
0	1	0	$\bar{p}q\bar{r}$	0	$-$
0	1	1	$\bar{p}qr$	1	$+$
1	0	0	$p\bar{q}\bar{r}$	0	$-$
1	0	1	$p\bar{q}r$	1	$+$
1	1	0	$pq\bar{r}$	1	$+$
1	1	1	pqr	1	$+$

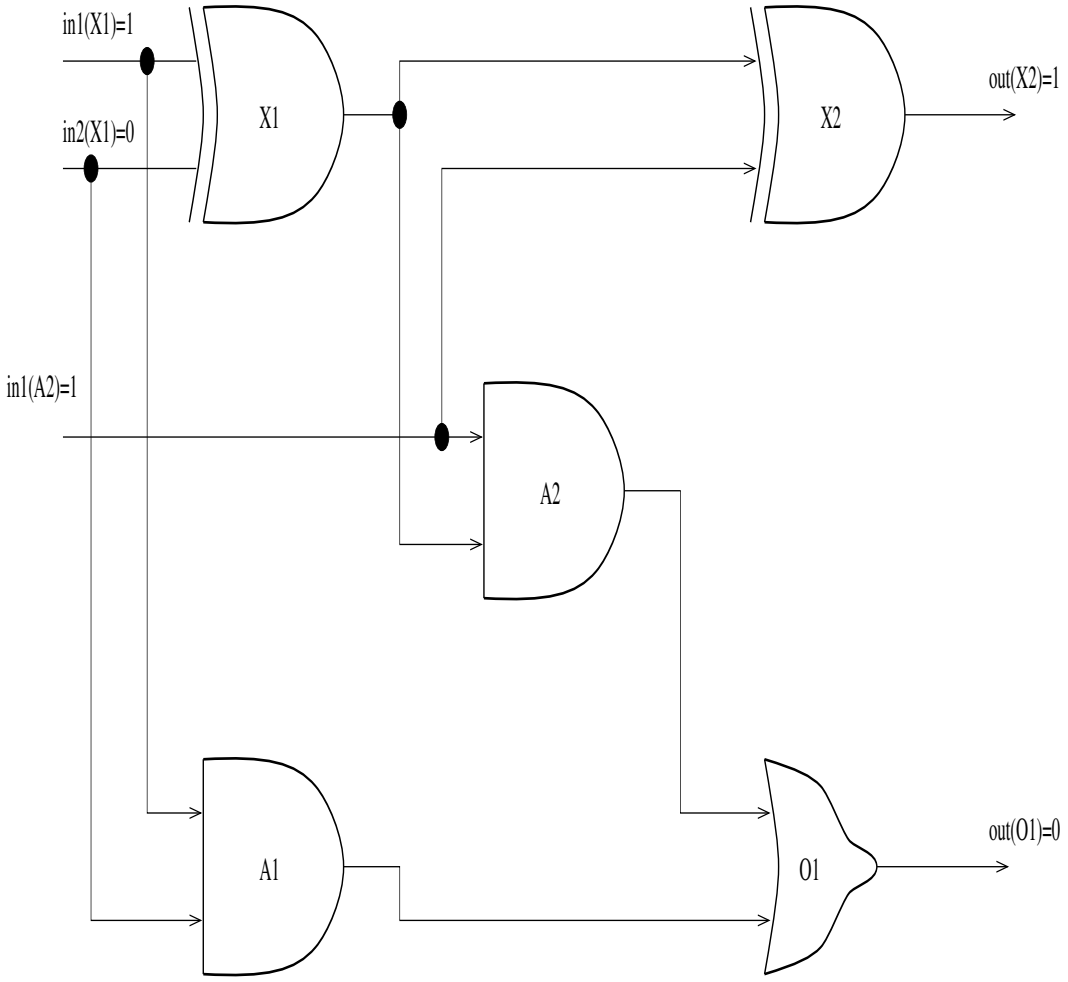
Bramki logiczne



Rysunek 2: Symbole bramek logicznych

Układy logiczne

Z bramek logicznych można budować dowolnie złożone układy logiczne.



Rysunek 3: Przykład układu logicznego – sumator.

Analiza układów logicznych

Analiza układów logicznych polega na rekonstrukcji funkcji logicznej realizowanej przez zadany układ logiczny. Można to zrobić posługując się matrycą logiczną układu. Dla układu z Rys. 2 mamy:

inp1(X1)	inp2(X1)	inp(A2)	X1	A1	A2	out(X2)	out(O1)
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	1	0	0	1	0
0	1	1	1	0	1	0	1
1	0	0	1	0	0	1	0
1	0	1	1	0	1	0	1
1	1	0	0	1	0	0	1
1	1	1	0	1	0	1	1

Na postawie powyższej tabeli można odtworzyć funkcje w postaci kanonicznej; dla uproszczenia podstawmy inp1(X1) $= p$, inp2)X1) $= q$, inp(A2) $= c$. Mamy:

$$out(X2) = \bar{p}\bar{q}c \vee \bar{p}q\bar{c} \vee p\bar{q}\bar{c} \vee pqc,$$

$$out(O1) = \bar{p}qc \vee p\bar{q}c \vee pq\bar{c} \vee pqc.$$

Można też określić postacie minimalne dla tych funkcji:

$$out(X2) = \bar{p}\bar{q}c \vee \bar{p}q\bar{c} \vee p\bar{q}\bar{c} \vee pqc,$$

$$out(O1) = pq \vee pc \vee qc.$$

Postać minimalna i kanoniczna funkcji out(X2) są identyczne.

Funkcje tego układu można też określić bezpośrednio w oparciu o schemat; jednak jest ona bardziej skomplikowana i trudna do dalszej analizy.

Synteza układów logicznych

Synteza układów logicznych polega na zaprojektowaniu struktury sieci logicznej realizującej określoną funkcję. Funkcja którą należy zrealizować może być zadana:

- ekstensjonalnie – w postaci tabeli wejścia-wyjście,
- intensjonalnie – w postaci wyrażenia logicznego (booleowskiego).

Etapy projektowania obejmują:

- specyfikację funkcji (np. werbalną, w postaci zestawu warunków),
- budowę tablicy opisującej relacje wejścia-wyjścia,
- generację funkcji,
- minimalizację i ew. faktoryzację funkcji,
- implementację z wykorzytaniem zadanych bramek logicznych.

Tablica definiująca funkcję budowana jest w oparciu o werbalną specyfikację funkcji, np.:

> *Zaprojektować układ do głosowania, o trzech wejściach, który daje na wyjściu* 1 *o ile przynajmniej na dwóch wejściach pojawią się jedynki.*

p	q	r	$f(p,q,r)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Synteza układów logicznych

Dla tabeli specyfikującej działanie funkcji można łatwo zbudować postać kanoniczną funkcji. W tym celu należy:

- uwzględnić jedynie te wiersze tabeli, w których na wyjściu układu jest 1,
- dla każdego takiego wiersza zbudować iloczyn minimalny zawierający wszystkie zmienne wejściowe,
- jeżeli w danym wierszu zmienna wejściowa przyjmuje wartość 1 to w iloczynie minimalnym występuje bez negacji,
- jeżeli w danym wierszu zmienna wejściowa przyjmuje wartość 0 to w iloczynie minimalnym występuje z negacją,
- wygenerowane iloczyny minimalne połączyć symbolem alternatywy.

Postać kanoniczna tej funkcji:

$$f(p,q,r) = \bar{p} \cdot q \cdot r \vee p \cdot \bar{q} \cdot r \vee p \cdot q \cdot \bar{r} \vee p \cdot q \cdot r.$$

Postać kanoniczna jest zwykle zbyt rozbudowana, aby wykorzystać ją bezpośrednio do syntezy układu. Należy zatem dokonać minimalizacji funkcji korzystając z praw algebry Boole'a.
Minimalizacja może przebiegać następująco:

$$\begin{aligned}
&\bar{p} \cdot q \cdot r \vee p \cdot \bar{q} \cdot r \vee p \cdot q \cdot \bar{r} \vee p \cdot q \cdot r = \\
&(\bar{p} \cdot q \cdot r \vee p \cdot q \cdot r) \vee (p \cdot \bar{q} \cdot r \vee p \cdot q \cdot r) \vee (p \cdot q \cdot \bar{r} \vee p \cdot q \cdot r) = \\
&q \cdot r \vee p \cdot r \vee p \cdot q.
\end{aligned}$$

Dla realizacji tej funkcji potrzeba 3 bramki AND i 2 bramki OR.
Dla realizacji funkcji z wykorzystaniem bramek NAND stosujemy przekształcenie: $f(p,q,r) = \overline{\overline{q \cdot r \vee p \cdot r \vee p \cdot q}} = \overline{\overline{pq} \cdot \overline{pr} \cdot \overline{qr}}$. (4 bramki NAND).

Minimalizacja i przekształcanie wyrażeń

Minimalizację i przekształcanie funkcji logicznych można prowadzić z wykorzystaniem reguł algebry Boole'a; pozwalają one zachować *równoważność* wyrażeń booleowskich (funkcji). Przy minimalizacji szczególnie użyteczne są następujące reguły:

Reguła sklejania wyrażeń iloczynowych

Niech będą dane dwa iloczyny literałów postaci $x_1x_2\ldots x_{i-1}px_{i+1}\ldots x_n$ oraz $x_1x_2\ldots x_{i-1}\bar{p}x_{i+1}\ldots x_n$, które są identyczne poza i-tą pozycją na której występują literały komplementarne. Iloczyny te można zastąpić jednym iloczynem wg następującego schematu:

$$\frac{x_1x_2\ldots x_{i-1}p\ x_{i+1}\ldots x_n,\ x_1x_2\ldots x_{i-1}\bar{p}\ x_{i+1}\ldots x_n}{x_1x_2\ldots x_{i-1}-x_{i+1}\ldots x_n}$$

Symbol $-$ oznacza *dowolną wartość* i może zostać pominięty; otrzymamy wówczas skrócony iloczyn postaci $x_1x_2\ldots x_{i-1}x_{i+1}\ldots x_n$.

Reguła pochłaniania wyrażeń iloczynowych

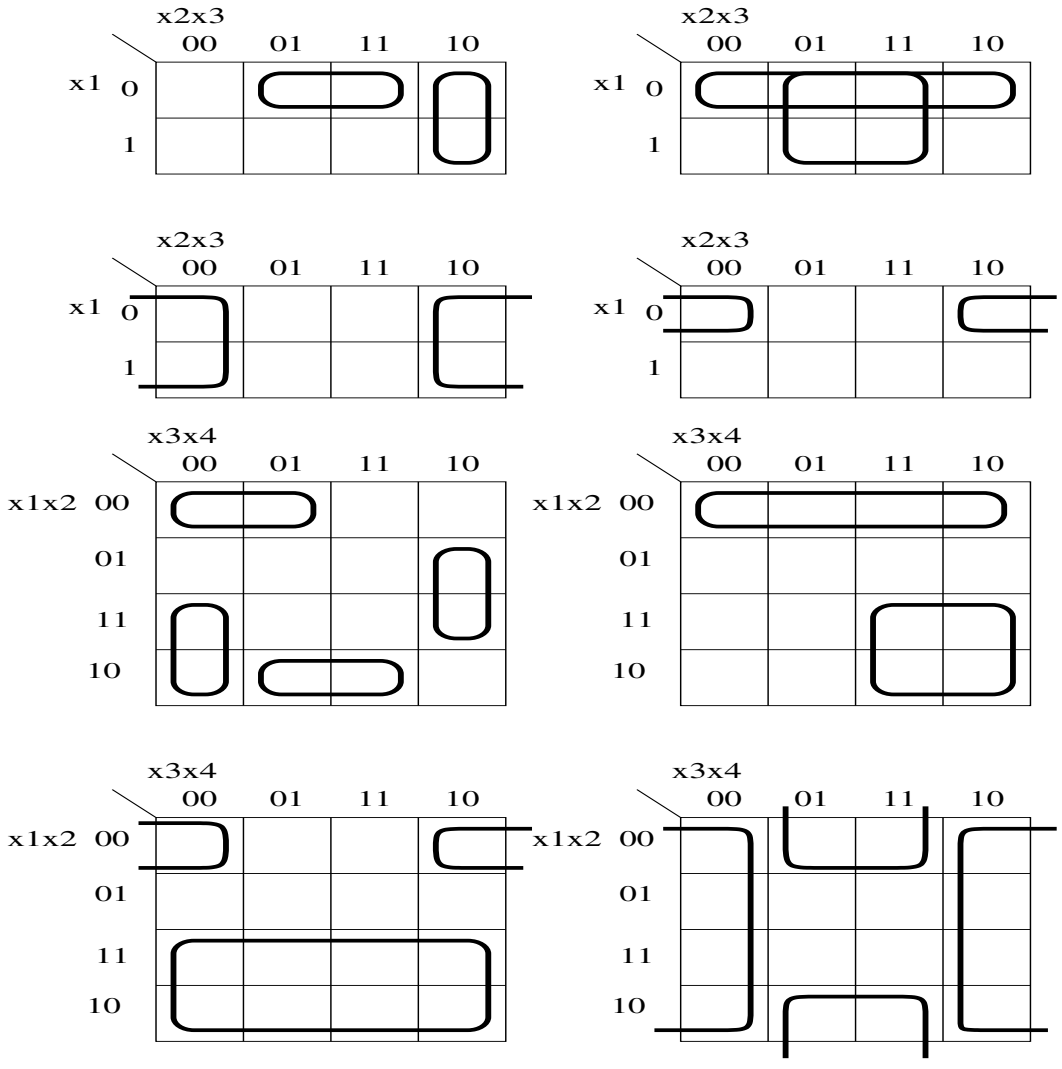
W trakcie redukcji wyrażeń booleowskich może okazać się, że pewne wyrażenia przestają być niezbędne dla zapisu funkcji – stają się one nadmiarowe i jako takie mogą być usunięte. Niech będą dane dwa iloczyny literałów postaci $x_1x_2\ldots x_n$ oraz $y_1y_2\ldots y_n$. Powiemy, że zachodzi pochłanianie:

$$x_1x_2\ldots x_n \geq y_1y_2\ldots y_n$$

wtw. gdy dla każdego i, $x_i = y_i$ lub $x_i = -$. Inaczej, wyrażenie pochłaniające przyjmuje wartość 1 zawsze gdy wyrażenie pochłaniane przyjmuje wartość 1. Wyrażenie pochłaniane $y_1y_2\ldots y_n$ można wyeliminować (bez wpływu na równoważność; pamiętajmy, że $x_1x_2\ldots x_{i-1}x_{i+1}\ldots x_n \equiv x_1x_2\ldots x_{i-1}-x_{i+1}\ldots x_n$).

Tablice Karnaugha

Tablice Karnaugha stanowią wizualne narzędzie wspomagające minimalizację wyrażeń booleowskich i funkcji logicznych. Istota tablic Karnaugha polega na uwidocznieniu wyrażeń, które mogą podlegać sklejaniu w postaci *sąsiednich pól* odpowiednio skonstruowanej tablicy.



Rysunek 4: Przykłady tablic Karnaugha

Zasady sklejania w tablicach Karnaugha

Konstrukcja tablic Karnaugha jest taka, że każde dwie sąsiednie kratki specyfikują iloczyny logiczne różniące się dokładnie na jednej pozycji; pola takie można zatem skleić, analogicznie jak iloczyny zmiennych.

Obowiązują następujące zasady sklejania:

- oznaczenia kratek:
  - $n = 2$: 00, 01, 11, 10,
  - $n = 3$: 000, 001, 011, 010, 110, 111, 101, 100.
- sklejaniu podlegają wszystkie pola zawierające 1; pola zawierające $-$ mogą, ale nie muszą być pokryte (są one uwzględniane w miarę potrzeb),
- ilość zaznaczonych kratek musi być potęgą dwójki,
- sklejane obszary muszą mieć kształt prostokąta; sklejane mogą być również "prostokąty" skonstruowane na zasadzie sąsiedztwa pól rozmieszczonych symetrycznie na krawędziach,
- należy wykorzystać prostokąty pokrywające jak największą liczbę jedynek,
- już pokryte jedynki można wykorzystać do ponownego sklejania, o ile jest taka potrzeba,
- dla danego prostokąta budowany jest iloczyn zmiennych, przy czym:
  - jeżeli wewnątrz obszaru dana zmienna przyjmuje stale wartość 1, to jest uwzględniana bez negacji,
  - jeżeli wewnątrz obszaru dana zmienna przyjmuje stale wartość 0, to jest uwzględniana z negacją,
  - jeżeli wewnątrz obszaru dana zmienna przyjmuje wartość 1 i 0, to jest pomijana.

Przykład syntezy: sumator jednobitowy

Specyfikacja zadania

Należy skonstruować układ logiczny stanowiący sumator jednobitowy, uwzględniający również przeniesienie. Na wejściu sumatora mamy dwa sumowane bity (sygnały p i q) oraz bit przeniesienia c. Na wyjściu sumatora mamy bit wyniku s oraz bit przeniesienia t. Bit wyniku s jest równy 1 wtedy i tylko wtedy gdy suma sygnałów wejściowych jest nieparzysta (jedna albo trzy jedynki). Bit przeniesienia t jest równy 1 wtedy i tylko wtedy gdy sumowane są co najmniej dwie jedynki. Odpowiednią tablicę specyfikacji funkcji s i t podano poniżej.

p	q	c	s	t
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

Postacie kanoniczne funkcji s i t mogą być odczytane bezpośrednio z tabeli; na tej podstawie można wypełnić odpowiednie tabele Karnaugha. Otrzymane postacie minimalne funkcji s i t są następujące:

$$s = \bar{p}qc \vee p\bar{q}\bar{c} \vee \bar{p}\bar{q}c \vee pqc,$$

$$t = pq \vee pc \vee qc.$$

Inna postać z wykorzystaniem EX-OR): $s = p \oplus q \oplus c$, $t = pq \vee (p \oplus q)c$.

Metoda Quine'a–McCluskeya

Metodę Quine'a–McCluskeya (zwaną też metodą implikantów) przedstawimy na przykładzie minimalizacji funkcji logicznej czterech zmiennych:

$$f(a,b,c,d) = \Sigma(5,7,8,9,10,11,13,15)$$

Proces minimalizacji rozpoczniemy od uporządkowania zbiorów iloczynów pełnych funkcji w taki sposób, aby poszczególne grupy zawierały iloczyny pełne o takiej samej liczbie jedynek.

	a	b	c	d
8	1	0	0	0
5	0	1	0	1
9	1	0	0	1
10	1	0	1	0
7	0	1	1	1
11	1	0	1	1
13	1	1	0	1
15	1	1	1	1

Następnie porównujemy każdą kombinację należącą do danej grupy z każdą kombinacją należącą do grupy następnej. Jeżeli porównywane kombinacje różnią się od siebie tylko na jednej pozycji, to łączymy je w nową kombinacje, wpisując w rozróżniające je miejsce znak „–". W omawianym przykładzie otrzymujemy następującą postać tabeli:

	a	b	c	d
8,9	1	0	0	–
8,10	1	0	–	0
5,7	0	1	–	1
5,13	–	1	0	1
9,11	1	0	–	1
9,13	1	–	0	1
10,11	1	0	1	–
7,15	–	1	1	1
11,15	1	–	1	1
13,15	1	1	–	1

Kontynuując procedurę łączenia, usuwamy powtarzające kombinacje. Procedurę łączenia kończymy, gdy nie ma możliwości dokonywania dalszych łączeń. Każda kombinacja nie podlegająca dalszemu łączeniu jest nazywana implikantem prostym. W omawianym przykładzie otrzymujemy:

	a	b	c	d
8,9,10,11	1	0	–	–
5,7,13,15	–	1	–	1
9,11,13,15	1	–	–	1

Następnie tworzymy tabelę, w której wiersze odpowiadają otrzymanym implikantom prostym, a kolumny wszystkim „prawdziwym" iloczynom pełnym, przedstawionym w defnicji funkcji. Analizując tabele stawiamy znak „x" w tych polach, które leżą na przecięciu kolumny reprezentującej dany iloczyn pełny (w postaci liczby dziesiętnej) oraz wiersza odpowiadającego implikantowi prostemu, który ów iloczyn pełny zawiera.

W naszym przykładzie wygląda to następująco:

		5	7	8	9	10	11	13	15
8,9,10,11	$a\neg b$			x	x	x	x		
5,7,13,15	bd	x	x					x	x
9,11,13,15	ad				x		x	x	x

Uproszczona funkcja, równoważna funkcji minimalizowanej, może być otrzymana w postaci sumy wybranych implikantów prostych. Wybór implikantów prostych jest przeprowadzony tak, aby pokrywały one wszystkie rozważane iloczyny pełne. W naszym przykładzie można orzymać w ten sposób dwie funkcje odpowiadające funkcji minimalizowanej:

$$f_1(a,b,c,d) = a\bar{b} + bd$$

$$f_2(a,b,c,d) = a\bar{b} + bd + ad$$

Ostatecznie najprostszą postać ma funkcja f_1 zatem:

$$f(a,b,c,d) = \Sigma(5,7,8,9,10,11,13,15) = a\bar{b} + bd$$

Rachunek predykatów pierwszego rzędu

Dotychczas prezentowane w toku wykładu elementy logiki matematycznej opierały się głównie o tzw. *rachunek zdań*.

Definicja 58 ***Rachunek zdań*** (ang. propositional calculus) *to dział logiki matematycznej badający związki między zdaniami (zmiennymi zdaniowymi) lub funkcjami zdaniowymi utworzonymi za pomocą spójników zdaniowych ze zdań lub funkcji zdaniowych prostszych. Rachunek zdań określa sposoby stosowania spójników zdaniowych w poprawnym wnioskowaniu.*

Rachunek zdań jest rozstrzygalny, tj. możemy obliczyć wartość dowolnej formuły.

Rachunek predykatów pierwszego rzędu

Jeśli chcemy opisać jakiś wycinek rzeczywistości, to często rachunek zdań okazuje sie nie wystarczający. Brakuje aparatu matematycznego umożliwiającego operowanie na abstrakcyjnych obiektach; nie pozwala to na opisywanie praw, którym te obiekty mogą podlegać. Rachunek predykatów pierwszego rzędu wprowadza tego typu mechanizmy i stanowi punkt wyjścia dla wielu systemów formalnych.

Definicja 59 *Alfabet rachunku predykatów pierwszego rzędu tworzą następujące rodzaje wyrażeń:*

- *zmienne indywiduowe:*
  $x_1, x_2, \ldots,$
- *n–argumentowe symbole funkcyjne* $(n \geq 0)$*:*
  $f_1^n, f_2^n, \ldots,$
  (symbole 0–argumentowe nazywamy stałymi indywiduowymi)
- *n–argumentowe symbole predykatowe* $(n \geq 0)$*:*
  $P_1^n, P_2^n, \ldots,$
  (symbole 0–argumentowe nazywamy stałymi zdaniowymi)

- *symbole logiczne:*
  $\neg$, $\Rightarrow$, $\forall$
  zwane odpowiednio negacją, implikacją oraz kwantyfikatorem ogólnym.

Definicja 60 ***Zbiór termów*** *jest najmniejszym zbiorem spełniającym następujące warunki:*

- *stałe indywiduowe są termami*
- *zmienne indywiduowe są termami*
- *jeśli f jest symbolem funkcji n–argumentowej, a $t_1, \ldots, t_n$ są termami, to także $f(t_1, \ldots, t_n)$ jest termem.*

Definicja 61 *Jeśli P jest symbolem relacji n–argumentowej, $t_1, \ldots, t_n$ są termami, to $P(t_1, \ldots, t_n)$ jest formułą atomową (atomem).*

Wystąpienie zmiennej nazywamy *związanym* wtedy gdy znajduje się w zasięgu działania kwantyfikatora, natomiast gdy nie jest ono związanym jest nazywane *wystąpieniem wolnym.*

Definicja 62 Zmienna *jest* wolna *w danej formule, jeśli przynajmniej jedno jej wystąpienie w tej formule jest wolne.*
Zmienna *jest* związana *w danej formule, jeśli przynajmniej jedno jej wystąpienie w tej formule jest związane.*

Definicja 63 *Formułę bez zmiennych wolnych nazywamy* formułą zamkniętą *lub* zdaniem.

Definicja 64 Zbiór formuł *jest najmniejszym zbiorem spełniającym warunki:*

- *atomy są formułami,*
- *jeśli α i β są formułami, to $(\neg\alpha)$ oraz $(\alpha \Rightarrow \beta)$, są formułami,*
- *jeśli α jest formułą, x jest zmienną wolną w α, to $(\forall x)\,\alpha$ jest formułą.*

Dla uproszczenia zapisu wprowadzamy symbole takie jak: $\wedge$, $\vee$, $\Leftrightarrow$, $\exists$ nazywane: koniunkcją, alternatywą, równoważnością, kwantyfikator szczegółowym (egzystencjalnym). Są one definiowalne za pomocą wymienionych trzech: $\neg, \Rightarrow, \forall$, w następujący sposób:

- $\alpha \vee \beta \equiv \neg\alpha \Rightarrow \beta$
- $\alpha \wedge \beta \equiv \neg(\alpha \Rightarrow \neg\beta)$
- $\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha) \equiv \neg((\alpha \Rightarrow \beta) \Rightarrow \neg(\beta \Rightarrow \alpha))$
- $(\exists x)P(x) \equiv \neg((\forall x)\neg P(x))$

Definicja 65 ***Interpretacją formuły*** *α nazywamy parę $(\mathcal{D}, m)$, gdzie $\mathcal{D}$ (dziedzina) jest niepustym zbiorem, zaś m taką funkcją przyporządkowującą wartość stałym, symbolom funkcyjnym i predykatowym występującym w α, że:*

- *każemu symbolowi stałej idywidułowej jest przyporządkowany element zbioru $\mathcal{D}$,*
- *każdemu n–argumentowemu symbolowi funkcyjnemu f^n przyporządkowane jest odwzorowanie z $\mathcal{D}^n$ w $\mathcal{D}$,*
- *każdemu n–argumentowemu symbolowi predykatowemu P^n przyporządkowane jest odwzorowanie z $\mathcal{D}^n$* w $\{0, 1\}$
- *każdemu symbolowi stałej zdaniowej jest przyporządkowany element ze zbioru $\{0, 1\}$ wartości logicznych.*

Niech $AS(\mathcal{I})$ będzie zbiorem wszystkich wartościowań zmiennych w interpretacji $\mathcal{I} = (\mathcal{D}, m)$ to znaczy wszystkich funkcji v określonych na zbiorze funkcji indywidułowych takich, że $v(x_k) \in \mathcal{D}$.

Definicja 66 ***Wartość termu*** *dla ustalonej interpretacji $\mathcal{I} = (\mathcal{D}, m)$ oraz wartościowania $v \in AS(\mathcal{I})$ określa się następująco:*

- $Wart_{\mathcal{I},v}(x_k) = v(x_k)$
- $Wart_{\mathcal{I},v}(f_k^0) = m(f_k^0)$
- $Wart_{\mathcal{I},v}(f_k^n(t_1, \ldots, t_n)) = m(f_k^n)(Wart_{\mathcal{I},v}(t_1), \ldots, Wart_{\mathcal{I},v}(t_n))$

Definicja 67 ***Wartość formuły atomowej*** *dla danej interpretacji* $\mathcal{I} = (\mathcal{D}, m)$ *oraz wartościowania* $v \in AS(\mathcal{I})$ *określa się następująco:*

- $Wart_{\mathcal{I},v}(P_k^0) = m(P_k^0)$
- $Wart_{\mathcal{I},v}(P_k^n(t_1, \ldots, t_n)) = m(P_k^n)(Wart_{\mathcal{I},v}(t_1), \ldots, Wart_{\mathcal{I},v}(t_n))$

Niech $AS_v^x(\mathcal{I})$ dla wartościowania $v \in AS(\mathcal{I})$ oraz zmiennej indywiduowej x, będzie zbiorem wszystkich wartościowań $v^{'}$ takich, że dla dowolnej zmiennej indywiduowej y różnej od x zachodzi $v^{'}(y) = v(y)$. To znaczy, wartościowania z $AS_v^x(I)$ mogą różnić się jedynie wartościami dla zmiennej x.

Definicja 68 ***Wartość formuły złożonej*** *zależy wyłącznie od wartości symboli występujących w tej formule:*

$$Wart_{\mathcal{I},v}(\neg\alpha) = \begin{cases} 1, & \textit{jeśli } Wart_{\mathcal{I},v}(\alpha) = 0 \\ 0, & \textit{w przeciwnym przypadku} \end{cases}$$

$$Wart_{\mathcal{I},v}(\alpha \Rightarrow \beta) = \begin{cases} 0, & \textit{jeśli } Wart_{\mathcal{I},v}(\alpha) = 1 \textit{ i } Wart_{I,v}(\beta) = 0 \\ 1, & \textit{w przeciwnym przypadku} \end{cases}$$

$$Wart_{\mathcal{I},v}((\forall x)\alpha) = \begin{cases} 1, & \textit{jeśli } Wart_{\mathcal{I},v'}(\alpha) = 1 \textit{ dla każdego } v^{'} \in AS_v^x(\mathcal{I}) \\ 0, & \textit{w przeciwnym przypadku} \end{cases}$$

Własności formuł

- Formuła α jest spełniona przy interpretacji $\mathcal{I}$ oraz wartościowaniu $v \in AS(\mathcal{I})$ wtedy i tylko wtedy, gdy $Wart_{\mathcal{I},v}(\alpha) = 1$.

- Formuła α jest prawdziwa przy interpretacji $\mathcal{I}$ wtedy i tylko wtedy, gdy $Wart_{\mathcal{I},v}(\alpha) = 1$ dla każdego wartościowania $v \in AS(\mathcal{I})$. Mówimy wówczas, że $\mathcal{I}$ spełnia α, tzn. $\mathcal{I}$ jest modelem dla α.
- Formuła α jest spełnialna wtedy i tylko wtedy, gdy istnieje taka interpretacja $\mathcal{I}$ oraz wartościowanie $v \in AS(\mathcal{I})$, przy których wartość formuły α wynosi 1.
- Formuła α jest prawdziwa (jest tautologią) wtedy i tylko wtedy, gdy każda interpretacja $\mathcal{I}$ spełnia α.
- Formuła α jest falsyfikowalna wtedy i tylko wtedy, gdy istnieje taka interpretacja $\mathcal{I}$ oraz wartościowanie $v \in AS(\mathcal{I})$, przy których wartość formuły α wynosi 0.
- Formuła α jest fałszywa przy interpretacji $\mathcal{I}$ wtedy i tylko wtedy, $Wart_{\mathcal{I},v}(\alpha) = 0$ dla każdego wartościowania $v \in AS(\mathcal{I})$.
- Formuła α jest fałszywa wtedy i tylko wtedy, gdy formuła α jest fałszywa przy każdej interpretacji $\mathcal{I}$.

Przykład:

Rozważmy zdanie:

$$(x_1 + 5 < x_2) \Rightarrow (2 < x_1), \text{ gdzie } x_1, x_2 \in \mathbb{N}$$

operuje ona na dwóch zmiennych indywiduowych x_1i x_2, których dziedziną $\mathcal{D}$ są liczby naturalne $\mathbb{N}$. Liczby 5 i 2 są stałymi indywiduowymi. Występująca tu operacja dodawania może zostać przedstawiona w postaci funkcji o jednym argumencie $g : \mathbb{N} \to \mathbb{N}$, a wyrażenia objęte nawiasami potraktujemy jako predykaty dwuargumentowe $P_<$. Sama formuła α odpowiadająca temu zdaniu przybiera wtedy postać:

$$\alpha(x_1, x_2) = (P_<(f_{+5}(x_1), x_2) \Rightarrow P_<(2, x_1)), \text{ gdzie } x_1, x_2 \in \mathbb{N}$$

przy czym interpretacja $\mathcal{I}$ symbolu funkcyjnego f_{+5} będzie przyporządkowywała mu odwzorowanie g:

$$m(f_{+5}) = g \text{ gdzie } g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \text{ i } g(x) = x + 5$$

a symbolowi predykatowemu $P_<$ odwzorowanie h:
$m(P_<) = h$ gdzie $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ jest zadane wzorem:

$$h(x_1, x_2) = \begin{cases} 1 & \text{gdy } x_1 < x_2 \\ 0 & \text{gdy } \neg(x_1 < x_2) \end{cases}$$

Pozostaje zatem jeszcze wyznaczyć wartościowanie dla zmiennych indywiduowych x_1, x_2. Niech zatem $v_1 \in AS(\mathcal{I})$ będzie zdefiniowane następująco: $v_1(x_1) = 3$ oraz $v_1(x_2) = 10$. Przy takim wartościowaniu zmiennych x_1, x_2 mamy;
$Wart_{\mathcal{I},v_1}(P_<(f_{+5}(x_1), x_2)) = m(P_<)(Wart_{\mathcal{I},v_1}(f_{+5}(x_1)), Wart_{I,v_1}(x_2)) =$
$= h(m(f_{+5})(Wart_{\mathcal{I},v_1}(x_1)), Wart_{I,v_1}(x_2)) = h(g(v_1(x_1)), v_1(x_2)) = h(g(3), 10) = h(8, 10) = 1$
zatem wartościowanie pierwszego użytego w formule predykatu jest równe 1 – tzn. przy takiej interpretacji oraz wartościowaniu jest on prawdziwy. Podobnie można pokazać, że $Wart_{\mathcal{I},v_1}(P_<(2, x_1)) = 1$ a w konsekwencji wartościowanie całej formuły $Wart_{\mathcal{I},v_1}(\alpha) = 1$. Oznacza to, że *formuła α jest spełniona przy interpretacji $\mathcal{I}$ oraz wartościowaniu v_1*, tym samym jest formułą *spełnialną*.

Łatwo pokazać, że nie jest formułą *prawdziwą*. Wystarczy, rozważyć wartościowanie: $v_2(x_1) = 1$, $v_2(x_2) = 10$.

Przykład:

Rozważmy dwie następujące formuły zmiennych $m, n \in \mathbb{N}$,

1. $\forall m\,(\exists n\,(n > 2^m))$
2. $\exists m\,(\forall n\,(n > 2^m))$

Obie zmienne m, n, w obu tych formułach są zmiennymi związanymi tj. znajdują się w zasięgu kwantyfikatorów. Można pokazać, że pierwsza przedstawiona formuła jest prawdziwa tj. dla dowolnej wartości m możemy tak dobrać n aby $n > 2^m$ była prawdziwa. Druga formuła natomiast jest fałszywa,

ponieważ nieprawdziwa jest formuła $\forall n(n > 2^m)$ gdzie m jest *zmienną wolną*, gdyż samo $n > 2^m$ nie jest prawdziwe, dla dowolnego wartościowania takiego, że $v(m) = v(n)$.

Z przykładu widać, iż stosowanie kwatyfikatorów ogólnego oraz szczegółowego nie jest przemienne.

Czasem przy zapisie zdania postaci „$\forall m\,(\exists n\,(n > 2^m))$" można opuścić niektóre nawiasy – „$\forall m\,\exists n\,(n > 2^m)$".

Zależności logiczne w rachunku predykatów:

- $\forall x\,\forall y\,p(x,y) \Leftrightarrow \forall y\,\forall x\,p(x,y)$
- $\exists x\,\exists y\,p(x,y) \Leftrightarrow \exists y\,\exists x\,p(x,y)$
- $\exists x\,\forall y\,p(x,y) \Leftrightarrow \forall y \exists x\,p(x,y)$
- $\forall x\,p(x) \Rightarrow \exists x\,p(x)$

Prawa De Morgana

- $\neg\forall x\,p(x) \Leftrightarrow \exists x\,(\neg p(x))$
- $\neg\exists x\,p(x) \Leftrightarrow \forall x\,(\neg p(x))$
- $\forall x\,p(x) \Leftrightarrow \neg\exists x\,(\neg p(x))$
- $\exists x\,p(x) \Leftrightarrow \neg\forall x\,(\neg p(x))$

Twierdzenie 12 *„Twierdzenie Churcha"* *Logika pierwszego rzędu nie jest rozstrzygalna, ale jest częściowo rozstrzygalna, tzn. nie istnieje algorytm, który dla danej, dowolnej formuły α rozstrzyga czy jest ona tautologią, czy nie. Istnieje jednak algorytm, który dla dowolnej formuły β, która jest tautologią potrafi to stwierdzić.*

Twierdzenie Churcha o częściowej rozstrzygalności rachunku predykatów rozwiewa marzenia o konstrukcji programu, który odpowiadałby na pytanie czy dana formuła jest twierdzeniem danej teorii czy nie. Maksimum tego, czego można oczekiwać od automatycznych systemów dowodzenia twierdzeń, jest konstrukcja dowodu dla formuły będącej twierdzeniem rozważanej teorii.