Podstawy matematyki

Wykład 2 - Język logika pierwszego rzędu, teoria zbiorów

Oskar Kędzierski

15 marca 2020

Język logiki pierwszego rzędu

Rachunek zdań, tj. system formalny, w którym występują wyłącznie zmienne zdaniowe oraz spójniki logiczne nazywa się czasem językiem logiki zerowego rzędu. Język logiki pierwszego rzędu stanowi rozszerzenie rachunku zdań o

i) kwantyfikatory,

ii) symbole funkcyjne i relacyjne,

iii) zmienne indywiduowe (lub nazwowe).

Przy ich pomocy można budować formuły, które interpretuje się nad strukturami, to jest zbiorami, przypisując symbolom funkcyjnym i relacyjnym funkcje i relacje.

Składnia języka logiki pierwszego rzędu

Definicja

Sygnaturę (lub **alfabet**) języka logiki pierwszego rzędu oznaczamy przez Σ. Jest to rodzina przeliczalnych zbiorów Σ_n^F dla $n \geq 0$ oraz rodzina przeliczalnych zbiorów Σ_n^R dla $n \geq 1$, parami rozłącznych. Elementy zbioru Σ_n^F to symbole funkcyjne $n-$argumentowe (symbole funkcyjne $0-$argumentowe traktujemy jako stałe) a elementy zbioru Σ_n^R to symbole relacyjne $n-$argumentowe.

Definicja

Niech X oznacza nieskończony, przeliczalny zbiór zmiennych indywiduowych (nazwowych). Zwykle elementy zbioru X oznacza sie przez $x, y, z, w, \ldots$.

Składnia języka logiki pierwszego rzędu

Uwaga

W formułach języka logiki pierwszego rzędu używa się też dwuargumentowego symbolu równości $=$, który nie należy do sygnatury, oraz symboli nawiasów, wskazujących na kolejności wykonywania działań.

Czasem wyklucza się symbol równości lub traktuje się go jako symbol relacyjny $2-$argumentowy.

Termy

Definicja

Termem nazywamy

i) symbol zmiennej,

ii) napis $f(t_1, \ldots, t_n)$, gdzie $t_1, \ldots, t_n$ są termami a $f \in \Sigma_n^F$ jest symbolem funkcyjnym dla $n \geq 0$.

Zbiór wszystkich termów nad sygnaturą Σ oraz zbiorem zmiennych indywiduowych X oznaczamy $\mathcal{T}_\Sigma(X)$.

Zmienne występujące

Definicja

Dla każdego termu $t \in \mathcal{T}_\Sigma(X)$ definiujemy zbiór $FV(t) \subset X$ **zmiennych występujących** w termie t w sposób rekurencyjny

i) $FV(x) = \{x\}$,

ii) $FV(f(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} FV(t_i)$.

W szczególności, gdy $n = 0$ suma pustej rodziny jest zbiorem pustym, tj. w zbiór zmiennych występujących w termie będącym stałą, to zbiór pusty.

Przykład

Niech f będzie symbolem funkcyjnym 2−argumentowym a g symbolem funkcyjnym 3−argumentowym. Wtedy

$$FV(g(x, f(y, z), z)) = \{x\} \cup FV(f(y, z)) \cup \{z\} = \{x, y, z\}.$$

Formuły atomowe

Definicja

Dla ustalonej sygnatury Σ i zmiennych indywiduowych X, **formułą atomowa** nazywamy

i) symbol fałszu $\bot$,

ii) napis $r(t_1, \ldots, t_n)$, gdzie $t_1, \ldots, t_n \in \mathcal{T}_\Sigma(X)$ są termami a $r \in \Sigma_n^R$ dla $n \geq 1$ jest symbolem relacyjnym,

iii) napis $(t_1 = t_2)$, gdzie $t_1, t_2 \in \mathcal{T}_\Sigma(X)$ są termami.

Uwaga

Niektóre symbole funkcyjne i relacyjne są pisane pomiędzy argumentami zamiast przed argumentami (notacja prefiksowa, także notacja polska). Na przykład, symbol funkcyjny dodawania $+$ zapisuje się zwykle jako $x + y$, a nie $+(x, y)$, a symbol funkcyjny „mniejszy lub równy” $\leq$ zapisuje się zwykle jako $x \leq y$, a nie $\leq (x, y)$.

Notacja infiksowa i prefiksowa

Notację

$$x + y,\ x \leq y$$

nazywamy **notacją infiksową** (binarny symbol funkcyjny lub relacyjny stawiamy **pomiędzy** argumentami) a notację

$$+(x, y), \leq (x, y)$$

nazywamy **notacją prefiksową** lub **notacją polską** (binarny symbol funkcyjny lub relacyjny stawiamy **przed** argumentami).

W przeciwieństwie do infiksowej, notacja prefiksowa nie wymaga stosowania nawiasów ale uważa się ją za mniej przejrzystą.

Formuły

Definicja

Formułą języka logiki pierwszego rzędu (nad ustaloną sygnaturą Σ i zbiorem zmiennych indywiduowych X) nazywamy:

i) dowolną formułę atomową,

ii) napis $(\varphi \to \psi)$, gdzie φ, ψ są formułami,

iii) napis $\forall x\, \varphi$, gdzie $x \in X$ jest zmienną indywiduową a φ formułą.

Uwaga

Ponieważ każdy z klasycznych logicznych spójników logicznych $\neg, \vee, \wedge, \leftrightarrow$ można zapisać przy pomocy spójnika $\to$ oraz symbolu fałszu $\bot$, w praktyce stosuje się je także w formułach. Używa się też symbolu kwantyfikatora szczegółowego $\exists x$ zamiast napisu $\neg \forall x \neg$.

Przykład

Niech sygnatura Σ będzie zadana warunkami $\Sigma_0^F = \{0, 1\}, \Sigma_2^F = \{+, \cdot\}, \Sigma_2^R = \{\leq\}$ będzie sygnaturą ciała uporządkowanego. Wtedy, na przykład, termami są następujące napisy

i) 0,

ii) x,

iii) $x + 0$,

iv) $(1 \cdot (x + 0)) + y$.

Przykładowe formuły atomowe to,

i) $\bot$,

ii) $x \leq 0$,

iii) $(x + 1) \leq (1 + (1 + y)) \cdot z$,

iv) $(x = 1)$,

v) $((x \cdot 0) = (y + 1))$.

Przykład cd.

Przykładowe formuły, to

i) $\bot$,

ii) $x \leq 0$,

iii) $(x \leq 0) \to \bot$,

iv) $\forall x\, (x \leq 0) \to \bot$,

v) $(x \leq 1) \to (y \leq 0)$,

vi) $(x \leq 1) \to (\forall y\, (y \leq 0))$.

Zmienne wolne

Definicję zmiennych występujących w termach można rozszerzyć na zmienne wolne w formułach.

Definicja

Dla dowolnej formuły φ definiujemy zbiór **zmiennych wolnych** występujących w φ w następujący sposób

i) $FV(\bot) = \emptyset$,

ii) $FV(r(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} FV(t_i)$, gdzie $t_1, \ldots, t_n \in \mathcal{T}_\Sigma(X)$ są termami a $r \in \Sigma_n^R$ jest $n-$agrumentowym symbolem relacyjnym,

iii) $FV(t_1 = t_2) = FV(t_1) \cup FV(t_2)$, gdzie $t_1, t_2 \in \mathcal{T}_\Sigma(X)$ są termami,

iv) $FV(\varphi \to \psi) = FV(\varphi) \cup FV(\psi)$, gdzie φ, ψ są formułami,

v) $FV(\forall x\, \varphi) = FV(\varphi) \setminus \{x\}$, gdzie φ jest formułą.

Zmienne wolne – przykłady

Niech sygnatura Σ będzie zadana warunkami $\Sigma_0^F = \{0, 1\}, \Sigma_2^F = \{+, \cdot\}, \Sigma_2^R = \{\leq\}$ będzie sygnaturą ciała uporządkowanego. Wtedy, na przykład,

i) $FV(x \leq 0) = \{x\}$,

ii) $FV((x \leq 0) \to \bot) = \{x\}$,

iii) $FV(\forall x\, (x \leq 0) \to \bot) = \emptyset$,

iv) $FV(\forall x\, (x \leq y)) = \{y\}$,

v) $FV((\forall x\, (x \leq y)) \to (x \leq z)) = \{x, y, z\}$.

Uwaga

Uwaga, w ostatnim przykładzie zmienna x jest związana w poprzedniku implikacji, ale jest wolna w następniku. Zgodnie z definicją, jest to zmienna wolna w powyższej formule.

Formuły otwarte i zamknięte

Definicja

Jeśli $FV(\varphi) = \emptyset$, to formułę nazywamy **zamkniętą** (lub **zdaniem**).

Jeśli w formule φ nie występują kwantyfikatory, to nazywamy ją formułą **otwartą**.

Siła wiązania spójników logicznych a kwantyfikatory

Największy priorytet w formułach języka logiki pierwszego rzędu (po dopuszczeniu klasycznych spójników logicznych i kwantyfikatora $\exists$) mają

i) negacja $\neg$,

ii) koniunkcja $\wedge$ i alternatywa $\vee$,

iii) kwantyfikatory $\forall, \exists$,

iv) implikacja $\rightarrow$ i równoważność $\leftrightarrow$.

Przykład

Formułę logiczną $\forall x \, \neg r(x) \rightarrow r(x) \wedge s(x, y)$ należy interpretować jako $(\forall x \, (\neg r(x))) \rightarrow (r(x) \wedge s(x, y))$.

Semantyka języka logiki pierwszego rzędu

Formuły języka logiki pierwszego rzędu mogą być interpretowane nad strukturą, to jest zbiorem, którego elementy przypisuje się zmiennym indywiduowym.

Definicja

Niech Σ będzie sygnaturą. **Strukturą** $\mathfrak{A}$ nad sygnaturą Σ nazywamy niepusty zbiór A wraz z przypisaniem

i) każdemu symbolowi relacyjnemu $r \in \Sigma_n^R$ dla $n \geq 1$ relacji $r^{\mathfrak{A}} \subset A^n$,

ii) każdemu symbolowi funkcyjnemu $f \in \Sigma_n^R$ dla $n \geq 0$ funkcji $f^{\mathfrak{A}} \colon A^n \to A$ (w szczególności, dla $n = 0$, przypisanie stałym elementów ze zbioru A).

Uwaga

Gdy jasne jest o jaką strukturę chodzi opuszcza się jej nazwę i zamiast $r^{\mathfrak{A}}, f^{\mathfrak{A}}$ pisze się r, f.

Wartościowanie w strukturze

Definicja

Wartościowaniem w strukturze $\mathfrak{A}$ nad sygnaturą Σ nazywamy dowolną funkcję

$$\rho\colon X \to A,$$

tj. przypisanie zmiennym indywiduowym ze zbioru X elementów ze zbioru A. Dla dowolnego wartościowania ρ, zmiennej $x \in X$ oraz elementu $a \in A$ definiujemy wartościowanie ρ_x^a wzorem

$$\rho_x^a(y) = \begin{cases} \rho(y) & x \neq y, \\ a & x = y. \end{cases}$$

Każde wartościowanie w strukturze pozwala przypisać termom elementy zbioru A a formułom wartości logiczne.

Wartość termu

Definicja

Dla struktury $\mathfrak{A}$ nad sygnaturą Σ z ustalonym wartościowaniem $\rho\colon X \to A$ wartością termu $t \in \mathcal{T}_\Sigma(X)$ nazywamy element $[\![t]\!]^{\mathfrak{A}}_\rho \in A$ zdefiniowany rekurencyjne w następujący sposób

i) $[\![x]\!]^{\mathfrak{A}}_\rho = \rho(x)$ dla $x \in X$,

ii) $[\![f(t_1, \ldots, t_n)]\!]^{\mathfrak{A}}_\rho = f^{\mathfrak{A}}([\![t_1]\!]^{\mathfrak{A}}_\rho, \ldots, [\![t_n]\!]^{\mathfrak{A}}_\rho)$ dla termów $t_1, \ldots, t_n \in \mathcal{T}_\Sigma(X)$ oraz symbolu funkcyjnego $f \in \Sigma^F_n$.

Spełnianie formuł

Definicja

Mówimy, że formuła φ jest **spełniona** dla ustalonego wartościowania ρ w strukturze $\mathfrak{A}$, i piszemy

$$(\mathfrak{A}, \rho) \models \varphi,$$

jeśli

i) nie zachodzi $(\mathfrak{A}, \rho) \models \bot$,

ii) $(\mathfrak{A}, \rho) \models r(t_1, \ldots, t_n)$ wtedy i tylko wtedy, gdy $([\![t_1]\!]^{\mathfrak{A}}_{\rho}, \ldots, [\![t_n]\!]^{\mathfrak{A}}_{\rho}) \in r^{\mathfrak{A}}$ (tj. elementy $[\![t_1]\!]^{\mathfrak{A}}_{\rho}, \ldots, [\![t_n]\!]^{\mathfrak{A}}_{\rho}$ są ze sobą w relacji $r^{\mathfrak{A}}$) dla dowolnego symbolu relacyjnego $r \in \Sigma^F_n, n \geq 1$ i dowolnych termów $t_1, \ldots, t_n \in \mathcal{T}_{\Sigma}(X)$,

iii) $(\mathfrak{A}, \rho) \models (t_1 = t_2)$ wtedy i tylko wtedy, gdy $[\![t_1]\!]^{\mathfrak{A}}_{\rho} = [\![t_2]\!]^{\mathfrak{A}}_{\rho}$ dla dowolnych termów $t_1, t_2 \in \mathcal{T}_{\Sigma}(X)$,

Spełnianie formuł cd.

iv) $(\mathfrak{A}, \rho) \models (\varphi \to \psi)$ wtedy i tylko wtedy, gdy nie zachodzi $(\mathfrak{A}, \rho) \models \varphi$ lub zachodzi $(\mathfrak{A}, \rho) \models \psi$,

v) $(\mathfrak{A}, \rho) \models (\forall x\, \varphi)$ wtedy i tylko wtedy, gdy dla dowolnego $a \in A$ zachodzi $(\mathfrak{A}, \rho^a_x) \models \varphi$.

Stwierdzenie

Niech $\mathfrak{A}$ będzie strukturą nad sygnaturą Σ. Niech ρ, ρ' będą dwoma wartościowaniami w tej strukturze. Wtedy dla dowolnej formuły φ, jeśli $\rho|_{FV(\varphi)} = \rho'|_{FV(\varphi)}$, to

$$(\mathfrak{A}, \rho) \models \varphi \text{ wtedy i tylko wtedy, gdy } (\mathfrak{A}, \rho') \models \varphi,$$

tzn. spełnianie formuły zależy jedynie od wartościowania jej zmiennych wolnych.

Spełnialność

Definicja

Mówimy, że formuła φ jest **spełnialna w strukturze** $\mathfrak{A}$, jeśli istnieje wartościowanie ρ, takie, że

$$(\mathfrak{A}, \rho) \models \varphi,$$

(czyli jeśli jest **spełniona** dla pewnego wartościowania w $\mathfrak{A}$).

Definicja

Mówimy, że formuła φ nad sygnaturą Σ jest **spełnialna** jeśli istnieje struktura $\mathfrak{A}$, nad sygnaturą Σ, w której formuła φ jest spełnialna.

Spełnialność – przykłady

Formuła

$$(x + y = x + z) \rightarrow (y = z),$$

jest spełnialna w strukturze $\mathbb{R}$ nad sygnaturą ciał uporządkowanych. W szczególności jest spełnialna.

Formuła

$$(x + y = x + z) \wedge \neg(x + y = x + z),$$

nie jest spełnialna nad sygnaturą ciał uporządkowanych.

Prawdziwość

Definicja

Formuła φ jest **prawdziwa** w strukturze $\mathfrak{A}$, jeśli dla każdego wartościowania ρ zachodzi

$$(\mathfrak{A}, \rho) \models \varphi,$$

(czyli formuła jest spełniona przez wszystkie wartościowania w tej strukturze). W takim przypadku, strukturę $\mathfrak{A}$ nazywa się **modelem** dla formuły φ, co zapisujemy

$$\mathfrak{A} \models \varphi.$$

Jeśli Γ jest zbiorem formuł nad sygnaturą Σ, to piszemy

$$\mathfrak{A} \models \Gamma,$$

jeśli dla każdej formuły $\varphi \in \Gamma$ zachodzi $\mathfrak{A} \models \varphi$ (wszystkie formuły z Γ są prawdziwe w strukturze $\mathfrak{A}$).

Tautologie

Definicja

Formułę φ nad sygnaturą Σ nazywa się **tautologią**, jeśli dla dowolnej struktury $\mathfrak{A}$ nad sygnaturą Σ zachodzi

$$\mathfrak{A} \models \varphi,$$

(formuła φ jest prawdziwa w każdej strukturze nad Σ). Piszemy wtedy

$$\models \varphi.$$

Stwierdzenie

Podstawienie dowolnych formuł za zmienne zdaniowe tautologii języka logiki zerowego rzędu daje tautologię języka logiki pierwszego rzędu.

Tautologie cd.

Aby dowieść, że dana formuła jest tautologią, należy wykazać jej prawdziwość w dowolnej strukturze.

Aby dowieść, że dana formuła jest nie tautologią, należy wskazać strukturę, w której nie jest prawdziwa (tzn. wskazać wartościowanie ρ w tej strukturze, takie, że formuła φ nie jest spełniona).

Tautologie cd.

Stwierdzenie

Następujące formuły są tautologiami języka logiki pierwszego rzędu

i) $\forall x\,(\varphi \to \psi) \to (\forall x\,\varphi \to \forall x\,\psi)$,

ii) $\varphi \to \forall x\,\varphi$ o ile $x \notin FV(\varphi)$,

iii) $\forall x\,\varphi \to \varphi$,

iv) $\exists x\,\varphi \to \varphi$ o ile $x \notin FV(\varphi)$,

v) $x = x$,

vi) $(x_1 = y_1) \to ((x_2 = y_2) \to \ldots \to ((x_n = y_n) \to (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)))\ldots)$, gdzie $f \in \Sigma_n^F, n \geq 0$,

vii) $(x_1 = y_1) \to ((x_2 = y_2) \to \ldots \to ((x_n = y_n) \to (r(x_1, \ldots, x_n) \to r(y_1, \ldots, y_n)))\ldots)$, gdzie $f \in \Sigma_n^R, n \geq 1$,

viii) $\forall x\,(\varphi \vee \psi) \leftrightarrow \varphi \vee \forall x\,\psi$ o ile $x \notin FV(\varphi)$,

ix) $\exists x\,(\varphi \wedge \psi) \leftrightarrow \varphi \wedge \exists x\,\psi$ o ile $x \notin FV(\varphi)$,

Tautologie cd.

x) $\forall x\,(\varphi \wedge \psi) \leftrightarrow \forall x\,\varphi \wedge \forall x\,\psi$,

xi) $\exists x\,(\varphi \vee \psi) \leftrightarrow \exists x\,\varphi \vee \exists x\,\psi$,

xii) $\neg\exists x\,\varphi \leftrightarrow \forall x\,\neg\varphi$,

xiii) $\neg\forall x\,\varphi \leftrightarrow \exists x\,\neg\varphi$,

xiv) $\forall x \forall y\,\varphi \leftrightarrow \forall y \forall x\,\varphi$,

xv) $\exists x \exists y\,\varphi \leftrightarrow \exists y \exists x\,\varphi$,

xvi) $\forall x\,\varphi \rightarrow \exists x\,\varphi$,

xvii) $\exists y \forall x\,\varphi \rightarrow \forall x \exists y\,\varphi$,

gdzie φ, ψ są dowolnymi formułami.

Tautologie cd.

Dowód.

Dla przykładu udowodnimy iii). Ustalmy strukturę $\mathfrak{A}$ oraz wartościowanie ρ. Jeśli $(\mathfrak{A}, \rho) \not\models \forall x\, \varphi$, to $(\mathfrak{A}, \rho) \models \forall x\, \varphi \to \varphi$. Jeśli $(\mathfrak{A}, \rho) \models \forall x\, \varphi$, to dla dowolnego $a \in A$

$$(\mathfrak{A}, \rho_x^a) \models \varphi.$$

Wtedy dla dowolnego $a \in A$

$$(\mathfrak{A}, \rho_x^a) \models \forall x\, \varphi \to \varphi,$$

skąd, z dowolności $a \in A$,

$$(\mathfrak{A}, \rho) \models \forall x\, \varphi \to \varphi.$$

Równoważność formuł

Definicja

Mówimy, że dwie formuły φ, ψ są **logicznie równoważne**, jeśli

$$\models \varphi \leftrightarrow \psi,$$

tzn. w dowolnym modelu, przy dowolnym wartościowaniu obie są spełnione lub obie nie są spełnione. Piszemy wtedy

$$\varphi \equiv \psi.$$

Preneksowa postać normalna

Definicja

Formuła φ jest w **preneksowej postaci normalnej**, jeśli

$$\varphi = Q_1 x_1 Q_2 x_2 \dots Q_n x_n \psi,$$

gdzie Q_i jest równy $\forall$ lub $\exists$ dla $i = 1, \dots, n$ a formuła ψ jest otwarta.

Stwierdzenie

Dla dowolnej formuły φ istnieje równoważna do niej formuła w **preneksowej postaci normalnej.**

Preneksowa postać normalna

Przykład

$$\forall x\ p(x) \rightarrow \exists y\ q(y) \equiv \exists x\ \neg p(x) \vee \exists y\ q(y) \equiv \exists x \exists y \neg p(x) \vee q(y).$$

Przykład

$$\forall x\ (p(x) \rightarrow \exists y\ q(x,y)) \equiv \forall x\ (\neg p(x) \vee \exists y\ q(x,y)) \equiv$$
$$\equiv \forall x \exists y (\neg p(x) \vee q(x,y)).$$

Nierozstrzygalność

Twierdzenie

Istnieje *algorytm sprawdzający, czy formuła w języku logiki* **zerowego** *rzędu jest tautologią.*

Dowód.

Jeśli w formule występuje n parami różnych zmiennych, należy sprawdzić 2^n wartościowań.

Twierdzenie (A. Church, A. Turing)

Nie istnieje *algorytm sprawdzający, dla dowolnej sygnatury* Σ*, czy formuła w języku logiki* **pierwszego** *rzędu nad* Σ *jest tautologią.*

Dowód.

Gdyby istniał taki algorytm, to można pokazać, że istnieje także algorytm sprawdzający czy dowolna maszyna Turinga skończy działanie. Taki algorytm nie istnieje.

Entscheidungsproblem

Mówimy, że **nierozstrzygalny** jest problem decyzyjny:

Czy dana formuła języka pierwszego rzędu jest tautologią?

System Hilberta dla języka logiki pierwszego rzędu

Definicja

Generalizacją formuły $\varphi \in \mathcal{F}_\Sigma$ nazywamy każdą formułę postaci $\forall x_1 \ldots \forall x_n \varphi$, gdzie $x_1, \ldots, x_n$ są dowolnymi zmiennymi.

Definicja

Systemem Hilberta dla języka logiki pierwszego rzędu nazywamy system dowodzenia formuł nad przeliczalną sygnaturą Σ, w których występują jedynie spójniki $\neg, \rightarrow$, stała $\bot$, kwantyfikator $\forall$ oraz symbole z sygnatury Σ wraz z aksjomatami (oraz ich dowolnymi generalizacjami)

A1) $\varphi \rightarrow (\psi \rightarrow \varphi)$,

A2) $(\varphi \rightarrow (\psi \rightarrow \vartheta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \vartheta))$,

A3) $\neg\neg\varphi \rightarrow \varphi$,

A4) $\forall x(\varphi \rightarrow \psi) \rightarrow (\forall x\varphi \rightarrow \forall x\psi)$,

A5) $\varphi \rightarrow \forall x\varphi$, jeśli $x \notin FV(\varphi)$,

A6) $\forall x\varphi \rightarrow \varphi(t/x)$, jeśli term t jest dopuszczalny w φ,

System Hilberta dla języka logiki pierwszego rzędu cd.

Definicja

A7) $(x_1 = y_1) \to ((x_2 = y_2) \to \ldots \to ((x_n = y_n) \to (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))) \ldots)$, gdzie $f \in \Sigma_n^F, n \geq 0$,

A8) $(x_1 = y_1) \to ((x_2 = y_2) \to \ldots \to ((x_n = y_n) \to (r(x_1, \ldots, x_n) \to r(y_1, \ldots, y_n))) \ldots)$, gdzie $f \in \Sigma_n^R, n \geq 1$,

gdzie φ, ψ, ϑ są dowolnym formułami nad sygnaturą Σ oraz regułą dowodzenia **modus ponens**

$$\frac{\varphi,\ \varphi \to \psi}{\psi}.$$

Uwaga

Zbiór aksjomatów jest przeliczalny.

System Hilberta dla języka logiki pierwszego rzędu cd.

Definicja

Dowodem w systemie Hilberta nazywamy skończony ciąg formuł, w którym każda formuła jest aksjomatem lub została otrzymana przez zastosowanie reguły odrywania do poprzedzających ją formuł. Formuła φ **ma dowód** (lub jest **twierdzeniem systemu Hilberta**), jeśli istnieje dowód zawierający φ, co oznaczamy przez

$$\vdash_H \varphi.$$

Formuła φ ma dowód ze zbioru hipotez (przesłanek) Δ, gdy posiada dowód w systemie Hilberta z aksjomatami rozszerzonymi o Δ

$$\Delta \vdash_H \varphi.$$

System Hilberta dla języka logiki pierwszego rzędu cd.

Twierdzenie

W systemie Hilberta dla języka logiki pierwszego rzędu zachodzi **twierdzenie o dedukcji**, *tzn. dla dowolnej formuły* $\varphi \in \mathcal{F}_\Sigma$

$$\Delta \cup \{\varphi\} \vdash_H \psi \text{ wtedy i tylko wtedy, gdy } \Delta \vdash_H (\varphi \to \psi),$$

oraz twierdzenia o poprawności i silne twierdzenie o pełności, tzn. dla dowolnej formuły $\varphi \in \mathcal{F}_\Sigma$ *oraz dowolnego zbioru formuł* $\Delta \subset \mathcal{F}_\Sigma$

$$\Delta \vdash_H \varphi \text{ wtedy i tylko wtedy, gdy } \Delta \models \varphi.$$

W szczególności, każda tautologia języka logiki pierwszego rzędu posiada dowód.

Dowód.

Pomijamy.

Efektywna przeliczalność zbioru tautologii

Wniosek

Zbiór wszystkich tautologii nad przeliczalną sygnaturą Σ jest **efektywnie przeliczalny**, tzn. w istnieje algorytm wypisujący wszystkie tautologie nad ustaloną, przeliczalną sygnaturą (w nieskończonym czasie).

Dowód.

Na podstawie twierdzenia o pełności formuła φ jest tautologią, jeśli posiada dowód w systemie Hilberta. Zbiór wszystkich dowodów jest przeliczalny, zatem przeglądając go znajdziemy dowód dla φ.

Zbiory

Intuicyjnie zbiór to kolekcja pewnych obiektów. Zbiór pusty, tj. nieposiadający żadnych elementów oznaczamy $\emptyset$. Zbiory będziemy na ogól oznaczać dużymi literami A, B, C, X, Y, Z. Jeśli x jest elementem zbioru A piszemy $x \in A$. W przeciwnym przypadku piszemy $x \notin A$. Elementy zbioru można wyliczyć, np.

$$A = \{0, 2, 4, 6, 8\}$$

(kolejność elementów i liczba ich powtórzeń nie ma znaczenia) lub też podać regułę wyróżniającą elementy zbioru (wśród elementów pewnego większego zbioru), np.

$$A = \{x \in \mathbb{N} \mid (\exists_{y \in \mathbb{N}} x = 2y) \wedge x \leq 8\}.$$

Zapis $A = \{x \in X \mid P(x)\}$, gdzie $P(x)$ jest funkcja zdaniową (predykatem) czytamy „wszystkie x należące do X takie, że $P(x)$".

$$y \in \{x \in X \mid P(x)\} \leftrightarrow P(y)$$

Zbiory cd.

Elementami zbiorów mogą być też inne zbiory, np.

$$A = \{\emptyset, 1, \{1\}, \{\{1, 2, 3\}\}.$$

Zbiór A ma 4 elementy: zbiór pusty, 1, zbiór $\{1\}$ oraz zbiór jednoelementowy $\{\{1, 2, 3\}\}$.

Zbiory jednoelementowe nazywa się czasem **singletonami**.

Zbiory, które nie mają wspólnych elementów nazywamy **rozłącznymi**.

Zbiory cd.

Mówimy, że zbiór A jest podzbiorem zbioru B, jeśli każdy element zbioru A jest elementem zbioru B. Piszemy $A \subset B$.

$$A \subset B \leftrightarrow (x \in A \rightarrow x \in B)$$

Mówimy, że dwa zbiory są równe, jeśli mają te same elementy.

$$A = B \leftrightarrow (A \subset B) \wedge (B \subset A)$$

Nie istnieje zbiór wszystkich zbiorów

Rozpatrzmy zbiór Z wszystkich zbiorów X, które nie są swoimi elementami, tj.

$$Z = \{X \mid X \notin X\}$$

Zachodzą dwie możliwości:

i) $Z \in Z$, sprzeczność, bo wtedy Z nie spełnia warunku należenia do Z,

ii) $Z \notin Z$, sprzeczność, bo wtedy Z spełnia warunek należenia do Z.

Powyższe rozumowanie nazywamy **paradoksem Russela**.

Aksjomatyka teorii mnogości

Badania nad współczesną teoria mnogości (czyli teoria zbiorów) zapoczątkowali pod koniec XIX wieku Georg Cantor i Richard Dedekind. Po odkryciu m.in. paradoksu Russela prace nad **aksjomatyzacją** teorii mnogości podjęli Ernst Zermelo i Abraham Fraenkel. Ich celem było uniknięcie paradoksów i otrzymanie teorii nie prowadzącej do sprzeczności.

Aksjomaty ZFC

Aksjomaty teorii mnogości Zermelo i Fraenkla w skrócie nazywa się aksjomatami ZF lub aksjomatami ZFC (gdy dołączy sie do nich pewnik wyboru, ang. axiom of choice).

W aksjomatyce ZFC elementy zbiorów są też zbiorami należącymi do pewnego uniwersum zbiorów. Aksjomaty są wyrażone w języku logiki pierwszego rzędu.

Aksjomat ekstensywności

$$\forall_x \forall_y (\forall_z (z \in x \leftrightarrow z \in y) \rightarrow (x = y)),$$

„dwa zbiory są równe jeśli maja takie same elementy”

Aksjomat regularności

$$\forall_x(\exists_y(y \in x) \rightarrow \exists_y(y \in x \wedge \neg(\exists_z z \in y \wedge z \in x)))$$

„każdy niepusty zbiór posiada element z nim rozłączny”

Z aksjomatu regularności wynika, że żaden zbiór nie jest swoim elementem, tzn. $\{x\} \cap x = \emptyset$ (z aksjomatu regularności zastosowanego dla jednoelementowego zbioru $\{x\}$). Aksjomat wyklucza też istnienie nieskończonej rodziny zbiorów x_n dla $n \in \mathbb{N}$ takich, że $x_{n+1} \in x_n$ (bo wtedy $x = \{x_1, x_2, \ldots\}$ nie posiada elementu z nim rozłącznego). Istnienie takiego zbioru nie wynika z poprzednich aksjomatów, ale nie jest z nimi sprzeczne.

Aksjomat wyróżniania

$$\forall_{w_1} \ldots \forall_{w_n} \forall_z \exists_y \forall_x (x \in y \leftrightarrow (x \in z \wedge \varphi))),$$

gdzie $w_1, \ldots, w_n, x, z$ są jedynymi zmiennymi, które mogą być wolne w formule φ.

„dla każdego zbioru z istnieje jego podzbiór y posiadający dokładnie elementy spełniające formułę φ”

Ten aksjomat gwarantuje istnienie zbioru pustego (wyróżniamy elementy spełniające fałszywy warunek). Z aksjomatu ekstensywności taki zbiór jest dokładnie jeden. Zmiennych $w_1, \ldots, w_n$ są parametrami formuły φ.

Aksjomat pary

$$\forall_x \forall_y \exists_z (x \in z \wedge y \in z)$$

„dla każdych dwóch zbiorów istnieje zbiór posiadający oba te zbiory”

Aksjomat sumy

$$\forall_r \exists_z \forall_x (x \in z \leftrightarrow \exists_y (y \in r \wedge x \in y))$$

„dla każdego zbioru r (rodziny zbiorów r) istnieje zbiór będący sumą zbiorów należących do r”

Aksjomat zastępowania

$$\forall_A \forall_{w_1} \ldots \forall_{w_n} (\forall_x (x \in A \rightarrow \exists!_y \varphi) \rightarrow \exists_B (\forall_x (x \in A \rightarrow \exists_y (y \in B \wedge \varphi))),$$

gdzie $x, y, w_1, \ldots, w_n, A$ mogą być jedynymi wolnymi zmiennymi w formule φ, reprezentującej funkcję f a $\exists!$ oznacza „istnieje dokładnie jeden”

„dla dowolnej funkcji określonej na zbiorze A istnieje zbiór B zawierający jej obraz”

Aksjomat nieskończoności

$$\exists_x(\emptyset \in x \wedge \forall_y(y \in x \rightarrow S(y) \in x)),$$

gdzie $S(w) = w \cup \{w\}$

„istnieje zbiór posiadający nieskończenie wiele elementów”

Aksjomat zbioru potęgowego

$$\forall_x \exists_y \forall_z (z \subset x \rightarrow z \in y)$$

„istnieje zbiór y, którego elementami są podzbiory zbioru x”

Aksjomat wyboru

$$\forall_r(\forall_x(x \in r \to \exists_y y \in x) \wedge \forall_x \forall_y((x \in r \wedge y \in r \wedge x \neq y) \to$$

$$\to \neg(\exists_z z \in x \wedge z \in y))) \to \exists_s (\forall_x(x \in r \to \exists!_y(y \in x \wedge y \in s))),$$

„dla dowolnej rodziny niepustych, parami rozłącznych zbiorów r istnieje selektor s, to jest zbiór, który ma dokładnie jeden element wspólny z każdym zbiorem z rodziny r”

Konsekwencje aksjomatu wyboru

Z aksjomatu wyboru wynika istnienie bazy (maksymalnego zbioru liniowo niezależnego) w dowolnej przestrzeni wektorowej.

Z drugiej strony, konsekwencją aksjomatu wyboru jest rozkład kuli w $\mathbb{R}^3$ na skończoną liczbę rozłącznych podzbiorów, z których można złożyć (przez translacje i obroty) dwie kule o takim samym promieniu jak wyjściowa (paradoks Banacha-Tarskiego).

Z twierdzenia Gödela o niedowoliwości niesprzeczności wynika, ze w ramach ZF(C) nie można dowieść niesprzeczności ZF(C) (jeśli system ZF(C) jest niesprzeczny). Prace Gödela i P. Cohena wykazały, że aksjomat wyboru jest niezależny od aksjomatów ZF, o ile są one niesprzeczne. Zatem, jeśli system ZF jest niesprzeczny, to niesprzeczny jest także system ZFC oraz ZF$\neg$C.

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela

W celu uniknięcia paradoksu Russela wprowadza się pojęcie **klasy**. Każdy zbiór jest klasą. Klasa nie może należeć do klasy (ale zbiór może). Istnieje klasa wszystkich zbiorów. Jest to tzw. klasa właściwa, która nie jest zbiorem.

Pozwala to na poprawne zdefiniowanie kategorii wszystkich zbiorów Set oraz kategorii Cat wszystkich małych kategorii (tj. kategorii, których zbiór wszystkich morfizmów tworzy zbiór). Przedstawione poniżej aksjomaty pochodzą od E. Mendelsona, *Introduction to Logic*, i różnią się od oryginalnych aksjomatów Bernaysa, w których istniały dwa symbole relacyjne $\in$ oraz η, które oznaczały odpowiednio „jest elementem zbioru" oraz „jest elementem klasy", zbiory oznaczano małymi literami a klasy dużymi.

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Aksjomatyka NBG stanowi **konserwatywne rozszerzenie** aksjomatów ZFC, co z definicji oznacza, że pozwala na dowiedzenie dokładnie tych samych twierdzeń o obiektach oryginalnej teorii. Twierdzenie Shoenfielda mówi, że każde twierdzenie teorii NBG, zawierające jedynie zmienne oznaczające zbiory, jest twierdzeniem teorii ZFC.

Ponieważ teoria NBG nie dopuszcza klasy wszystkich klas, wprowadza się pojęcie **konglomeratu** wszystkich klas. Istnieją alternatywne teorie zbiorów, np. teoria Morse'a–Kelley'a stanowiąca właściwe rozszerzenie teorii ZFC.

Uogólniona hipoteza continuum (tzn. dla dowolnej liczby kardynalej κ nie istnieje liczba kardynalna λ taka, że $\kappa < \lambda < 2^{\kappa}$) jest niezależna od ZFC ale implikuje pewnik wyboru. Teoria NBG jest niesprzeczna wtedy i tylko wtedy, gdy teoria ZFC jest niesprzeczna (Novak, Rosser-Wang, Shoenfield).

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Alfabet składa się ze zmiennych $X_1, X_2, \ldots,$ (oznaczanych dużymi literami dla zgodnosći z teoriami Bernaysa i Gödla) lub $X, Y, Z, \ldots$. Zmienne oznaczają klasy, czyli pewne kolekcje pewnych elementów. Teoria posiada dwa symbole relacyjny dwuargumentowe $\in$ oraz $=$. Pierwszy oznacza „bycie elementem", drugi równość spełniająca aksjomaty

i) $\forall X\ (X = X)$,

ii) $X = Y \rightarrow (\varphi(X, X) \rightarrow \varphi(X, Y))$,

gdzie $\varphi(X, X)$ jest dowolną formułą zdaniową, a $\varphi(X, Y)$ jest formułą zdaniową $\varphi(X, X)$, w której pewne wolne wystąpienia zmiennej X zastąpiono wolną zmienną Y (w celu uniknięcia np. $\forall X\ (X = X) \rightarrow \forall X\ (X = Y)$).

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Niech $X \notin Y$ będzie skrótem dla $\neg(X \in Y)$.
Niech $X \subseteq Y$ będzie skrótem dla $\forall Z\ (Z \in X \rightarrow Z \in Y)$ (X jest podklasą Y).
Niech $X \subset Y$ będzie skrótem dla $X \subseteq Y \wedge X \neq Y$ (X jest podklasą właściwą Y).
Niech $M(X)$ (niem. Menge) będzie skrótem dla $\exists Y\ (X \in Y)$ (X jest zbiorem).
Niech $Pr(X)$ (ang. proper class) będzie skrótem dla $\neg M(X)$ (X jest klasą właściwą).
Niech $\forall x\ \varphi(x)$ będzie skrótem dla $\forall X\ (M(X) \rightarrow \varphi(X))$, gdzie X jest pierwszą zmienną nie występująca w formule φ (dla każdej klasy X będącej zbiorem).
Niech $\exists x\ \varphi(x)$ będzie skrótem dla $\exists X\ (M(X) \wedge \varphi(X))$, gdzie X jest pierwszą zmienną nie występująca w formule φ (istnieje klasa X będąca zbiorem).

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Pierwsze dwa z poniższych aksjomatów są równoważne aksjomatom dla symbolu relacyjnego $=$ (ale używają skończonej liczby formuł zdaniowych).

- E $(\forall Z\ (Z \in X \leftrightarrow Z \in Y)) \rightarrow (X = Y)$ (aksjomat ekstensywności),
- T $(X = Y) \rightarrow (X \in Z \leftrightarrow Y \in Z)$ (równe klasy należą do tych samych klas),
- P $\forall x\ \forall y\ \exists z\ \forall u\ (u \in z \leftrightarrow u = x \vee u = y$, (dla dowolnych zbiorów x, y istnieje zbiór z, oznaczany $\{x, y\}$, którego elementami są jedynie x i y),
- N $\exists x\ \forall y\ (y \notin x)$ (aksjomat zbioru pustego, oznaczanego $\emptyset$, wyznaczonego jednoznacznie a aksjomatu ekstensywności),

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Jeśli X lub Y jest klasą właściwą, to $\{X, Y\} = \emptyset$. Symbol $\{X\}$ jest skrótem dla $\{X, X\}$.

Niech (X, Y) będzie skrótem dla $\{\{X\}, \{X, Y\}\}$ (gdy X, Y są zbiorami (X, Y) nazywamy parą uporządkowaną).
Niech (X) będzie skrótem dla X.
Niech $(X_1, \ldots, X_n)$ będzie skrótem dla $((X_1, \ldots, X_{n-1}), X_n)$.

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Aksjomaty istnienia klas (ang. class existence)

B-1 $\exists X\ \forall u\ \forall v\ ((u,v) \in X \leftrightarrow u \in v)$ (istnienie klasy par wszystkich zbiorów, tj. relacji $\in$),

B-2 $\forall X\ \forall Y\ \exists Z\ \forall u\ (u \in Z \leftrightarrow u \in X \wedge u \in Y)$ (istnienie klasy Z oznaczanej $X \cap Y$),

B-3 $\forall X\ \exists Z\ \forall u\ (u \in Z \leftrightarrow u \notin X)$ (istnienie klasy Z będącej dopełnieniem klasy X, oznaczanej $\overline{Z}$),

B-4 $\forall X\ \exists Z\ \forall u\ (u \in Z \leftrightarrow \exists v\ (u,v) \in X)$ (istnienie klasy Z będącej dziedziną relacji X, oznaczanej $D(X)$),

B-5 $\forall X\ \exists Z\ \forall u\ \forall v\ ((u,v) \in Z \leftrightarrow u \in X)$ (istnienie relacji (klasy) Z takiej, że każdy element (zbiór) klasy X jest w relacji z dowolnym zbiorem),

B-6 $\forall X\ \exists Z\ \forall u\ \forall v\ \forall w\ ((u,v,w) \in Z \leftrightarrow (v,w,u) \in X)$,

B-7 $\forall X\ \exists Z\ \forall u\ \forall v\ \forall w\ ((u,v,w) \in Z \leftrightarrow (u,w,v) \in X)$.

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Aksjomaty B-6 oraz B-7 pozwalają na utożsamienie iloczynów kartezjańskich $X_1 \times X_2 \times X_3$ z $X_{f(1)} \times X_{f(2)} \times X_{f(3)}$, dla dowolnej permutacji $f \in S_3$, pierwszy dotyczy cyklu, drugi transpozycji, które generują grupę S_3. Powyższe operacje pozwalają jednoznacznie zdefiniować klasę uniwersalną (dopełnienie zbioru pustego) , dopełnienie klasy, przecięcie, sumę, różnicę klas.

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

Stwierdzenie

Niech $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ będzie formułą zdaniową, w której występują co najwyżej zmienne $X_1, \ldots, X_n, Y_1, \ldots, Y_m$. Niech formuła φ będzie logicznie równoważna formule, w której jedynie zmienne oznaczające zbiory nie są wolne. Wtedy

$$\vdash \exists Z\ \forall x_1\ \ldots \forall x_n\ (x_1, \ldots, x_n) \in Z \leftrightarrow \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m).$$

Dowód.

Mendelson, *Introduction to Mathematical Logic*, Proposition 4.4. Dowód polega na indukcji ze względu na liczbę kwantyfikatorów i spójników $\rightarrow$ oraz $\neg$ w formule zdaniowej, głownie przy pomocy aksjomatów B-1, $\ldots$, B-7.

Jest to odpowiednik aksjomatu wyróżniania z aksjomatyki ZF, udowodniony na podstawie skończonej liczby aksjomatów.

Teoria zbiorów (klas) Von Neumanna–Bernaysa–Gödela cd.

U $\forall x\, \exists y\, \forall u\, (u \in y \leftrightarrow \exists v\, (u \in v \wedge v \in x)$ (istnienie zbioru y będącego sumą rodziny zbiorów x),

W $\forall x\, \exists y\, \forall u\, (u \in y \leftrightarrow u \subseteq x)$ (istnienie zbioru potęgowego y zbioru x),

S $\forall x\, \forall Y\, \exists z\, \forall u\, (u \in z \leftrightarrow u \in x \wedge u \in Y)$ (istnienie zbioru z, który zawiera elementy zbioru x i klasy Y),

R Y jest funkcją $\rightarrow \forall x\, \exists y\, \forall u\, (u \in y \leftrightarrow \exists v\, ((v, u) \in Y \wedge v \in x))$ (obraz zbioru x przez funkcję Y jest zbiorem y),

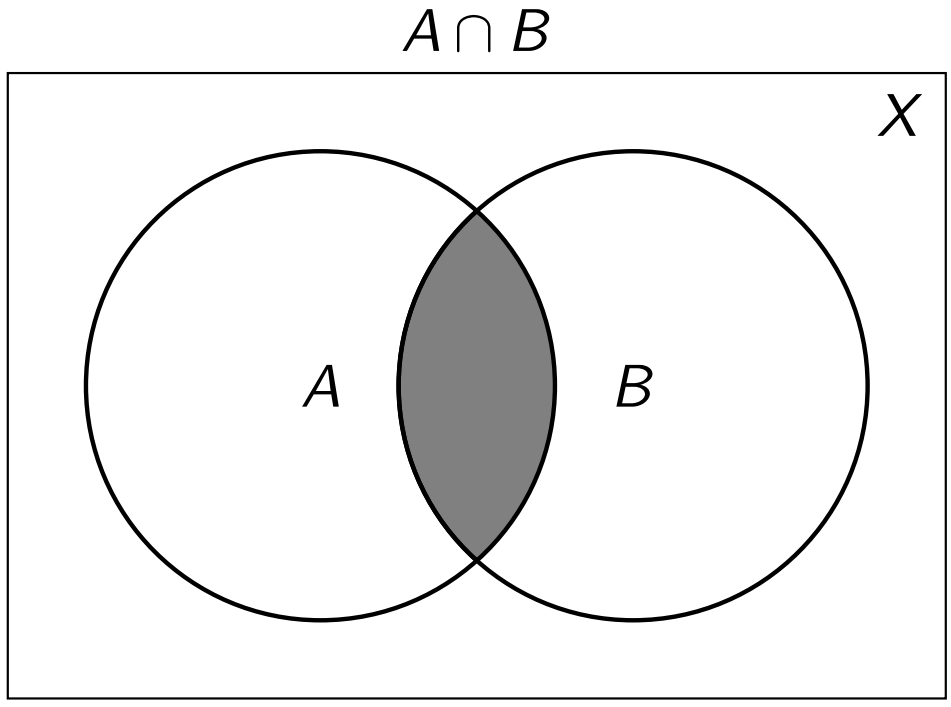
I $\exists x\, (\emptyset \in x \wedge \forall u\, (u \in x \rightarrow u \sum \{u\} \in x))$ (istnienie nieskończonego zbioru $\{x\}$),

Reg $\forall X\, (X \neq \emptyset \rightarrow \exists y; (y \in X \wedge y \cap X = \emptyset))$ (każda niepusta klasa X zawiera element (zbiór) z nią rozłączny),

C $\forall x\, \exists f (f$ jest funkcją $\wedge \forall y\, (y \neq \emptyset \wedge y \subseteq x) \rightarrow f(y) \in y)$ (pewnik wyboru)

UFC $\exists X\ f$ jest funkcją $\wedge \forall u\, (u \neq \emptyset \rightarrow X(u) \in u)$ (silny pewnik wyboru, istnienie uniwersalnej funkcji (klasy) wyboru, implikuje aksjomat C).

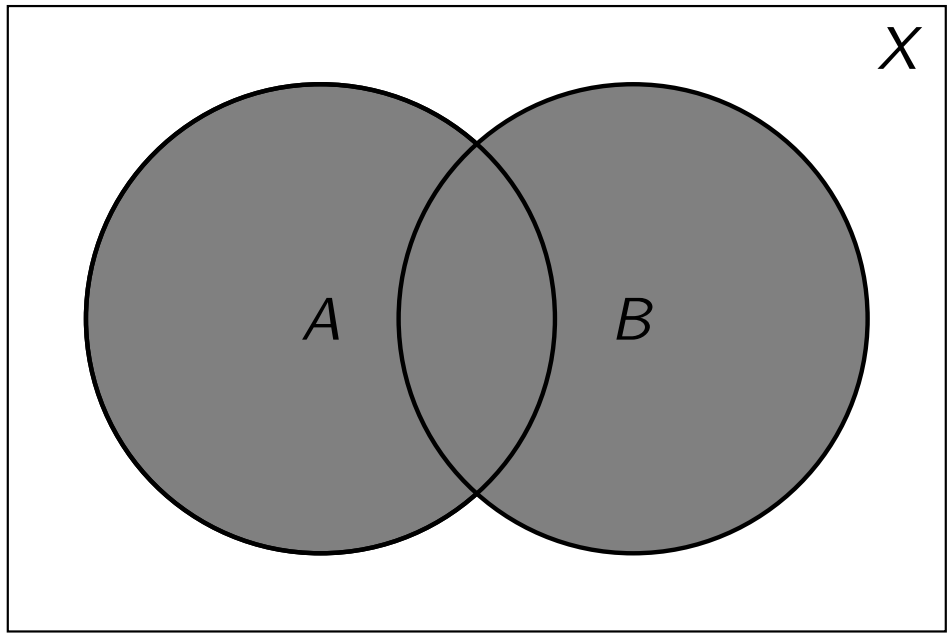
Część wspólna zbiorów A i B



$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$$

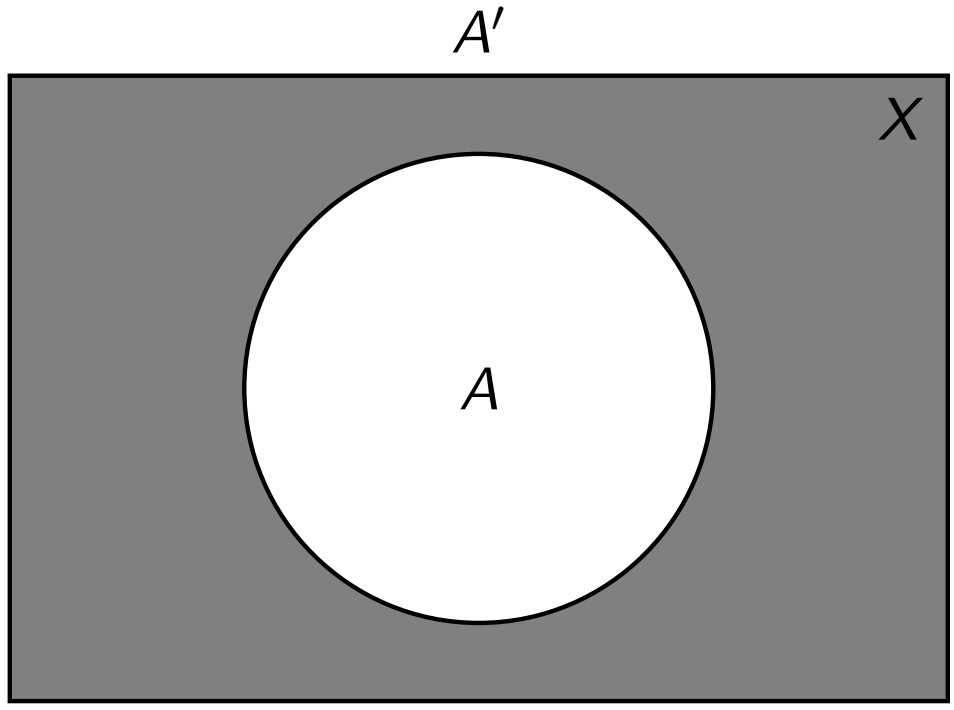
Suma zbiorów A i B

$A \cup B$



$$x \in A \cup B \leftrightarrow x \in A \vee x \in B$$

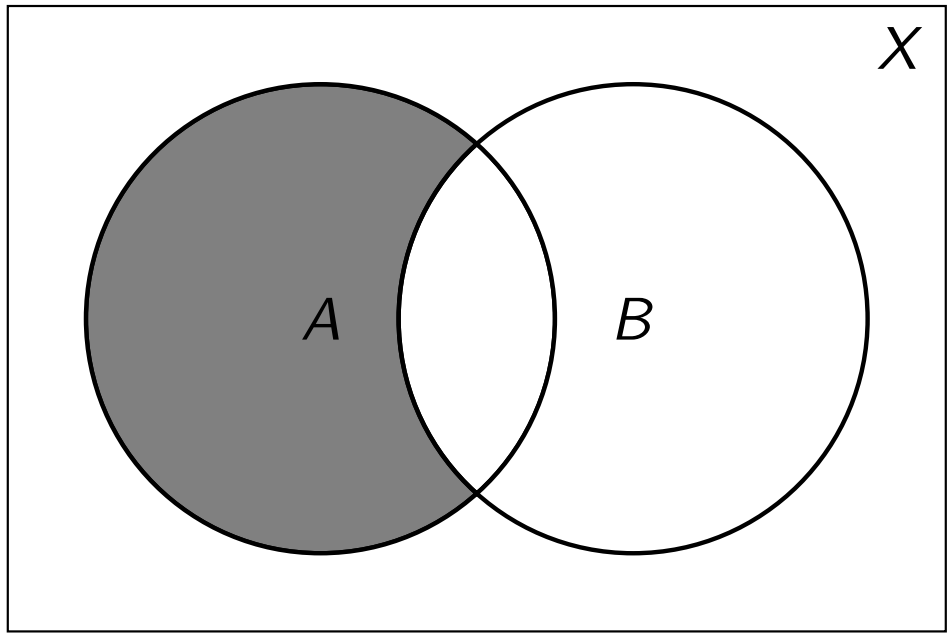
Dopełnienie zbioru A



$$x \in A' \leftrightarrow x \notin A$$

Różnica teoriomnogościowa A i B

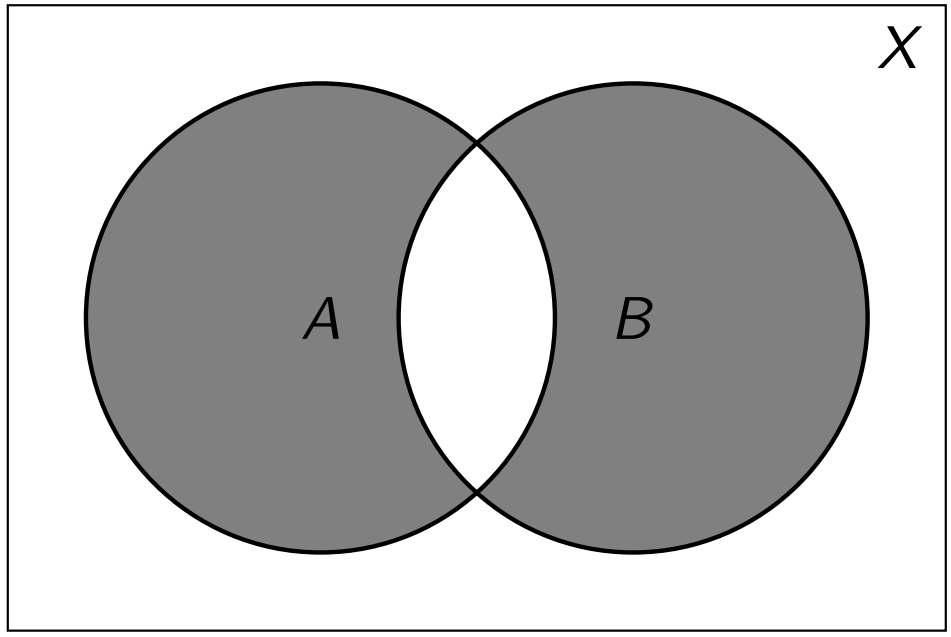
$A \setminus B$



$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B$$

Różnica symetryczna A i B

$$A \dot{-} B$$



$$x \in A \dot{-} B \leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$$

Przykłady

Niech

$A = \{1, 2, 4, 6, 8, 10\},\ B = \{2, 3, 6, 7, 9, 10\},\ X = \{1, \ldots, 10\},$

Wtedy

$$A, B \subset X,$$

$$A \cap B = \{2, 6, 10\},$$

$$A \cup B = \{1, 2, 3, 4, 6, 7, 8, 9, 10\},$$

$$A' = \{3, 5, 7, 9\},$$

$$A \setminus B = \{1, 4, 8\},$$

$$B \setminus A = \{3, 7, 9\},$$

$$A \dot{-} B = \{1, 3, 4, 7, 8, 9\}.$$

Prawa rachunku zbiorów

Ponieważ operacje na zbiorach wyrażone są w języku logiki, tautologie rachunku zdań dają tożsamości rachunku zbiorów (po podstawieniu za zmienne zdaniowe wyrażeń $x \in A, x \in B$).
Poniższe tożsamości wynikają wprost z definicji:

i) $A' = X \setminus A$,

ii) $A \setminus B = A \cap B'$,

iii) $A \dot{-} B = (A \setminus B) \cup (B \setminus A)$.

Prawa identyczności

Dla dowolnego zbioru $A \subset X$ zachodzą tożsamości

i) $A \cap \emptyset = \emptyset$,

ii) $A \cap X = A$,

iii) $A \cup \emptyset = A$,

iv) $A \cup X = X$.

Dowód.

Podstaw za p wyrażenie $x \in A$ do tautologii

i) $p \wedge \bot \leftrightarrow \bot$,

ii) $p \wedge \top \leftrightarrow p$,

iii) $p \vee \bot \leftrightarrow p$,

iv) $p \vee \top \leftrightarrow \top$.

Klasyczne własności rachunku zbiorów

i) $A \cap A = A$,

ii) $A \cup A = A$,

iii) $(A')' = A$,

iv) $A \cup A' = X$,

v) $A \cap A' = \emptyset$,

vi) $(A \subset B) \leftrightarrow (B' \subset A')$,

vii) $A \subset B \leftrightarrow A \cap B' = \emptyset$,

viii) $A \subset B \leftrightarrow A' \cup B = X$,

ix) $[(A \subset B) \wedge (B \subset A)] \leftrightarrow (A = B)$,

x) $A \cap (B \cap C) = (A \cap B) \cap C$,

xi) $A \cup (B \cup C) = (A \cup B) \cup C$,

Klasyczne własności rachunku zbiorów cd.

xii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

xiii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

xiv) $A' \subset B \wedge A' \subset B' \rightarrow A = X$,

xv) $(A \subset B \wedge B \subset C) \rightarrow (A \subset C)$.

Dowód.

Podstaw do tautologii z poprzedniego wykładu odpowiednio za p, q, r wyrażenia $x \in A, x \in B, x \in C$.

Prawa de Morgana rachunku zbiorów

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C),$$
$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C).$$

Dowód pewnej tożsamości

Udowodnimy, że $A \dot{-} B = (A \cup B) \setminus (A \cap B)$.

$$x \in A \dot{-} B \leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \leftrightarrow$$

$$\leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A) \wedge (x \notin B \vee x \in B) \wedge (x \notin B \vee x \notin A) \leftrightarrow$$

$$\leftrightarrow (x \in A \vee x \in B) \wedge \neg (x \in A \wedge x \in B) \leftrightarrow x \in (A \cup B) \setminus (A \cap B)$$