Metalogika (11)

Jerzy Pogonowski

Zakład Logiki Stosowanej UAM
www.logic.amu.edu.pl
pogon@amu.edu.pl

Uniwersytet Opolski

Plan wykładu

Słuchacze tych wykładów znają ze studiów metodę ***aksjomatyczną***. W wykładzie 3 przypomniano metodę ***dowodów założeniowych***, a w wykładzie 10 omówiono metodę ***tablic analitycznych***.

Poniżej przedstawiamy, raczej jako ilustrację niż szczegółowy wykład, trochę informacji o innych jeszcze metodach dowodowych:

- formalizmie Gentzena dla KRZ,
- formalizmie Gentzena dla KRP,
- dowodach rezolucyjnych dla KRZ.

O dowodach rezolucyjnych w KRP patrz np.:
http://www.logic.amu.edu.pl/images/f/f9/Rezkrp.pdf

Część I: Formalizm Gentzena dla KRZ

Część I:

Formalizm Gentzena dla KRZ

Formalizm Gentzena dla KRZ

Podamy podstawowe definicje dotyczące ***formalizmu Gentzena*** oraz informacje o wybranych własnościach rachunków Gentzena.

- Prezentacja opiera się na przedstawieniu tej problematyki w monografiach: Pogorzelski 1975 (dla KRZ) oraz Pogorzelski 1981 (dla KRP).
- Czytelnik zainteresowany zastosowaniami systemów Gentzena zechce zajrzeć choćby do dodatków zamieszczonej na stronie tych wykładów.

Definicje

Określimy relację $\Vdash$ między zbiorami formuł języka KRZ. Zachodzenie zależności $X \Vdash Y$ związane ma być z następującą intuicją: ze zbioru przesłanek X wyprowadzalna jest alternatywa elementów zbioru Y. Nie ograniczamy się do skończonych zbiorów formuł. Wyrażenia postaci $X \Vdash Y$ nazywamy ***sekwentami***.

Relację $\Vdash$ definiujemy indukcyjnie:

- $X \Vdash^0 Y$ wtedy i tylko wtedy, gdy $X \cap Y \neq \emptyset$
- $X \Vdash^{n+1} Y$ wtedy i tylko wtedy, gdy $X \Vdash^n Y$ lub istnieją zbiory formuł X_1, Y_1 oraz formuły α, β takie, że zachodzi jeden z warunków:

Definicje

$$\begin{array}{rl}
(+\to) & X = X_1 \cup \{\alpha \to \beta\} \text{ i } X_1 \cup \{\beta\} \Vdash^n Y \text{ i } X_1 \Vdash^n \{\alpha\} \cup Y \\
(\to+) & Y = Y_1 \cup \{\alpha \to \beta\} \text{ i } X \cup \{\alpha\} \Vdash^n \{\beta\} \cup Y_1 \\
(+\neg) & X = X_1 \cup \{\neg\alpha\} \text{ i } X_1 \Vdash^n \{\alpha\} \cup Y \\
(\neg+) & Y = Y_1 \cup \{\neg\alpha\} \text{ i } X \cup \{\alpha\} \Vdash^n Y_1 \\
(+\wedge) & X = X_1 \cup \{\alpha \wedge \beta\} \text{ i } X_1 \cup \{\alpha, \beta\} \Vdash^n Y \\
(\wedge+) & Y = Y_1 \cup \{\alpha \wedge \beta\} \text{ i } X \Vdash^n \{\alpha\} \cup Y_1 \text{ oraz } X \Vdash^n \{\beta\} \cup Y_1 \\
(+\vee) & X = X_1 \cup \{\alpha \vee \beta\} \text{ i } X_1 \cup \{\alpha\} \Vdash^n Y \text{ oraz } X_1 \cup \{\beta\} \Vdash^n Y \\
(\vee+) & Y = Y_1 \cup \{\alpha \vee \beta\} \text{ i } X \Vdash^n \{\alpha, \beta\} \cup Y_1 \\
(+\equiv) & X = X_1 \cup \{\alpha \equiv \beta\} \text{ i } X_1 \cup \{\alpha, \beta\} \Vdash^n Y \text{ oraz } X_1 \Vdash^n \{\alpha, \beta\} \cup Y \\
(\equiv+) & Y = Y_1 \cup \{\alpha \equiv \beta\} \text{ i } X \cup \{\alpha\} \Vdash^n \{\beta\} \cup Y_1 \text{ oraz } X \cup \{\beta\} \Vdash^n \{\alpha\} \cup Y_1
\end{array}$$

- $X \Vdash Y$ wtedy i tylko wtedy, gdy $X \Vdash^n Y$ dla pewnego $n \geqslant 0$.

Definicje

Powszechnie stosowaną umową notacyjną w rachunku sekwentów jest pisanie X, Y zamiast $X \cup Y$ oraz pisanie $\alpha_1, \ldots, \alpha_n$ zamiast skończonych zbiorów formuł $\{\alpha_1, \ldots, \alpha_n\}$. Dla przykładu, sekwent $X \cup \{\alpha \rightarrow \beta, \alpha\}$ zapisujemy w postaci: $X, \alpha \rightarrow \beta, \alpha$.

Zwykle posługujemy się następującymi diagramami, reprezentującymi warunki określające relację $\Vdash$ (kreskę poziomą w tych diagramach odczytujemy [metajęzykowo] jako: „jeśli …, to …", natomiast średnik oddzielający sekwenty odczytujemy [metajęzykowo] jako: „oraz"):

$$(0) \quad \frac{X \cap Y \neq \emptyset}{X \Vdash Y}.$$

$(+\rightarrow)$	$\dfrac{X,\beta \Vdash Y;\ \ X \Vdash \alpha, Y}{X,\alpha\rightarrow\beta \Vdash Y}$	$(\rightarrow +)$	$\dfrac{X,\alpha \Vdash \beta, Y}{X \Vdash \alpha\rightarrow\beta, Y}$
$(+\neg)$	$\dfrac{X \Vdash \alpha, Y}{X,\neg\alpha \Vdash Y}$	$(\neg +)$	$\dfrac{X,\alpha \Vdash Y}{X \Vdash \neg\alpha, Y}$
$(+\wedge)$	$\dfrac{X,\alpha,\beta \Vdash Y}{X,\alpha\wedge\beta \Vdash Y}$	$(\wedge +)$	$\dfrac{X \Vdash \alpha, Y;\ \ X \Vdash \beta, Y}{X \Vdash \alpha\wedge\beta, Y}$
$(+\vee)$	$\dfrac{X,\alpha \Vdash Y;\ \ X,\beta \Vdash Y}{X,\alpha\vee\beta \Vdash Y}$	$(\vee +)$	$\dfrac{X \Vdash \alpha,\beta, Y}{X \Vdash \alpha\vee\beta, Y}$
$(+\equiv)$	$\dfrac{X,\alpha,\beta \Vdash Y;\ \ X \Vdash \alpha,\beta, Y}{X,\alpha\equiv\beta \Vdash Y}$	$(\equiv +)$	$\dfrac{X,\alpha \Vdash \beta, Y;\ \ X,\beta \Vdash \alpha, Y}{X \Vdash \alpha\equiv\beta, Y}$

Definicje

- Relacja $\Vdash$ jest monotoniczna, tj. dla dowolnych X, Y, X_1, Y_1:
  - jeśli $X \Vdash Y$, to $X, X_1 \Vdash Y, Y_1$.
- Jeśli $X \Vdash Y$, to istnieją skończone zbiory X_1 oraz Y_1 takie, że: $X_1 \Vdash Y_1$.
- Dowodzi się następującego ***twierdzenia o cięciu***:
  Dla dowolnych X_1, X_2, Y_1 i Y_2 oraz formuły α: jeśli $X_1, \alpha \Vdash Y_1$ i $X_2 \Vdash \alpha, Y_2$, to $X_1, X_2 \Vdash Y_1, Y_2$.
  Tezę tego twierdzenia zapisać można również tak:

$$\frac{X_1, \alpha \Vdash Y_1; \quad X_2 \Vdash \alpha, Y_2}{X_1, X_2 \Vdash Y_1, Y_2}.$$

- Wszystkie reguły wymienione w poprzedniej tabeli są ***odwracalne***:

$(+\rightarrow)^*$	$\dfrac{X,\alpha\rightarrow\beta \Vdash Y}{X,\beta \Vdash Y;\ \ X \Vdash \alpha, Y}$	$(\rightarrow +)^*$	$\dfrac{X \Vdash \alpha\rightarrow\beta, Y}{X,\alpha \Vdash \beta, Y}$
$(+\neg)^*$	$\dfrac{X,\neg\alpha \Vdash Y}{X \Vdash \alpha, Y}$	$(\neg +)^*$	$\dfrac{X \Vdash \neg\alpha, Y}{X,\alpha \Vdash Y}$
$(+\wedge)^*$	$\dfrac{X,\alpha\wedge\beta \Vdash Y}{X,\alpha,\beta \Vdash Y}$	$(\wedge +)^*$	$\dfrac{X \Vdash \alpha\wedge\beta, Y}{X \Vdash \alpha, Y;\ \ X \Vdash \beta, Y}$
$(+\vee)^*$	$\dfrac{X,\alpha\vee\beta \Vdash Y}{X,\alpha \Vdash Y;\ \ X,\beta \Vdash Y}$	$(\vee +)^*$	$\dfrac{X \Vdash \alpha\vee\beta, Y}{X \Vdash \alpha,\beta, Y}$
$(+\equiv)^*$	$\dfrac{X,\alpha\equiv\beta \Vdash Y}{X,\alpha,\beta \Vdash Y;\ \ X \Vdash \alpha,\beta, Y}$	$(\equiv +)^*$	$\dfrac{X \Vdash \alpha\equiv\beta, Y}{X,\alpha \Vdash \beta, Y;\ \ X,\beta \Vdash \alpha, Y}$

Definicje

Zdefiniujemy operację C_{gen} ***konsekwencji w sensie Gentzena***:
$C_{gen}(X) = \{\alpha \in F_{KRZ} : X \Vdash \alpha\}$.
Tak określona operacja C_{gen} ma własności (C1)–(C4) podane na wykładzie 3, czyli jest operacją konsekwencji (w sensie Tarskiego).

Ponadto, dla dowolnego zbioru formuł X zbiór $C_{gen}(X)$ jest domknięty na odrywanie: jeśli $\alpha, \alpha \to \beta \in C_{gen}(X)$, to $\beta \in C_{gen}(X)$.

Relacja $\Vdash$ jest domknięta na podstawianie, w następującym sensie: jeśli $X \Vdash Y$, to $h^e[X] \Vdash h^e[Y]$, dla dowolnego $e : Var_{KRZ} \to F_{KRZ}$.

Sekwenty postaci $\emptyset \Vdash X$ nazywamy ***tezami*** systemu Gentzena.

Przykłady

- Zwykle dowody w rachunku sekwentów Gentzena zapisuje się jako ciągi „ułamków", w których „licznikach" występują założenia reguł, a w „mianownikach" stosowne tezy (tychże reguł).
- Postąpimy tu inaczej (głównie ze względów typograficznych, ale także dlatego, iż dowody warto śledzić „od celu do środków potrzebnych do jego osiągnięcia"). Będziemy reprezentować dowody przez drzewa. Bezpośrednie następniki danego wierzchołka to założenia reguły, dla której ów wierzchołek jest wnioskiem tej reguły. Liście drzewa dowodowego są zawsze postaci $X \Vdash Y$, gdzie $X \cap Y \neq \emptyset$. Dla sekwentu nie będącego liściem podajemy (z prawej strony, w górnej frakcji) informację o regule zastosowanej dla otrzymania tego sekwentu.

- Udowodnimy dla przykładu, że elementy jednej z aksjomatyk KRZ są tezami systemu Gentzena.

Przykłady

$$\emptyset \Vdash (\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma))\ ^{(\rightarrow +)}$$

$$\alpha \rightarrow \beta \Vdash (\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma)\ ^{(\rightarrow +)}$$

$$\alpha \rightarrow \beta, \beta \rightarrow \gamma \Vdash \alpha \rightarrow \gamma\ ^{(\rightarrow +)}$$

$$\alpha, \alpha \rightarrow \beta, \beta \rightarrow \gamma \Vdash \gamma\ ^{(+\rightarrow)}$$

$$\alpha, \beta, \beta \rightarrow \gamma \Vdash \gamma\ ^{(+\rightarrow)} \qquad \alpha, \beta \rightarrow \gamma \Vdash \alpha, \gamma$$

$$\alpha, \beta, \gamma \Vdash \gamma \qquad \alpha, \beta \Vdash \beta, \gamma$$

1. Dowód formuły: $(\alpha \rightarrow \beta) \rightarrow ((\beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma))$.

Przykłady

$$\emptyset \Vdash \alpha \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta)\ ^{(\rightarrow +)}$$

$$\alpha \rightarrow (\alpha \rightarrow \beta) \Vdash \alpha \rightarrow \beta\ ^{(\rightarrow +)}$$

$$\alpha, \alpha \rightarrow (\alpha \rightarrow \beta) \Vdash \beta\ ^{(+\rightarrow)}$$

$$\alpha, \alpha \rightarrow \beta \Vdash \beta\ ^{(+\rightarrow)} \qquad \alpha \Vdash \alpha, \beta$$

$$\alpha, \beta \Vdash \beta \qquad \alpha \Vdash \alpha, \beta$$

2. Dowód formuły: $\alpha \rightarrow (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta)$.

Przykłady

$$\emptyset \Vdash \alpha \to (\beta \to \alpha)^{\,(\to +)}$$

$$|$$

$$\alpha \Vdash \beta \to \alpha^{\,(\to +)}$$

$$|$$

$$\alpha, \beta \Vdash \alpha$$

3. Dowód formuły: $\alpha \to (\beta \to \alpha)$.

Przykłady

$$
\begin{array}{c}
\emptyset \Vdash (\alpha \wedge \beta) \rightarrow \alpha \;^{(\rightarrow +)} \\
| \\
\alpha \wedge \beta \Vdash \alpha \;^{(+\wedge)} \\
| \\
\alpha, \beta \Vdash \alpha
\end{array}
$$

4. Dowód formuły: $(\alpha \wedge \beta) \rightarrow \alpha$.

Przykłady

$$\emptyset \Vdash (\alpha \wedge \beta) \rightarrow \beta^{\,(\rightarrow +)}$$

$$|$$

$$\alpha \wedge \beta \Vdash \alpha^{\,(+\wedge)}$$

$$|$$

$$\alpha, \beta \Vdash \beta$$

5. Dowód formuły: $(\alpha \wedge \beta) \rightarrow \beta$.

Przykłady

$$\emptyset \Vdash (\alpha \to \beta) \to ((\alpha \to \gamma) \to (\alpha \to (\beta \wedge \gamma)))\ ^{(\to +)}$$

$$\alpha \to \beta \Vdash (\alpha \to \gamma) \to (\alpha \to (\beta \wedge \gamma))\ ^{(\to +)}$$

$$\alpha \to \beta, \alpha \to \gamma \Vdash \alpha \to (\beta \wedge \gamma)\ ^{(\to +)}$$

$$\alpha, \alpha \to \beta, \alpha \to \gamma \Vdash \beta \wedge \gamma\ ^{(\wedge +)}$$

$$\alpha, \alpha \to \beta, \beta \to \gamma \Vdash\ ^{(+ \to)} \qquad \alpha, \alpha \to \beta, \alpha \to \gamma \Vdash \gamma\ ^{(+ \to)}$$

$$\alpha, \beta, \alpha \to \gamma \Vdash \beta \qquad \alpha, \alpha \to \gamma \Vdash \alpha, \beta \qquad \alpha, \alpha \to \beta, \gamma \Vdash \gamma \qquad \alpha, \alpha \to \beta \Vdash \alpha, \gamma$$

6. Dowód formuły: $(\alpha \to \beta) \to ((\alpha \to \gamma) \to (\alpha \to (\beta \wedge \gamma)))$.

Przykłady

$$\begin{array}{c} \emptyset \Vdash \alpha \to (\alpha \vee \beta)\ ^{(\to +)} \\ | \\ \alpha \Vdash \alpha \vee \beta\ ^{(\vee +)} \\ | \\ \alpha \Vdash \alpha, \beta \end{array}$$

7. Dowód formuły: $\alpha \to (\alpha \vee \beta)$.

Przykłady

$$\emptyset \Vdash \alpha \rightarrow (\beta \vee \alpha)\ ^{(\rightarrow +)}$$

$$|$$

$$\alpha \Vdash \beta \vee \alpha\ ^{(\vee +)}$$

$$|$$

$$\alpha \Vdash \beta, \alpha$$

8. Dowód formuły: $\alpha \rightarrow (\beta \vee \alpha)$.

Przykłady

$$\emptyset \Vdash (\alpha \to \gamma) \to ((\beta \to \gamma) \to ((\alpha \vee \beta) \to \gamma))\ ^{(\to +)}$$

$$\alpha \to \gamma \Vdash (\beta \to \gamma) \to ((\alpha \vee \beta) \to \gamma)\ ^{(\to +)}$$

$$\alpha \to \gamma, \beta \to \gamma \Vdash (\alpha \vee \beta) \to \gamma\ ^{(\to +)}$$

$$\alpha \vee \beta, \alpha \to \gamma, \beta \to \gamma \Vdash \gamma\ ^{(+\vee)}$$

$$\alpha, \alpha \to \gamma, \beta \to \gamma \Vdash \gamma \qquad \beta, \beta \to \gamma, \alpha \to \gamma \Vdash \gamma$$

9. Dowód formuły: $(\alpha \to \gamma) \to ((\beta \to \gamma) \to ((\alpha \vee \beta) \to \gamma))$.

Przykłady

$$\emptyset \Vdash (\alpha \equiv \beta) \rightarrow (\alpha \rightarrow \beta)\ ^{(\rightarrow +)}$$

$$\alpha \equiv \beta \Vdash \alpha \rightarrow \beta\ ^{(\rightarrow +)}$$

$$\alpha, \alpha \equiv \beta \Vdash \beta\ ^{(+\equiv)}$$

$$\alpha, \alpha, \beta \Vdash \beta \qquad \alpha \Vdash \alpha, \beta, \beta$$

10. Dowód formuły: $(\alpha \equiv \beta) \rightarrow (\alpha \rightarrow \beta)$.

Przykłady

$$\emptyset \Vdash (\alpha \equiv \beta) \to (\beta \to \alpha)\ ^{(\to +)}$$

$$\alpha \equiv \beta \Vdash \beta \to \alpha\ ^{(\to +)}$$

$$\beta, \alpha \equiv \beta \Vdash \alpha\ ^{(+\equiv)}$$

$$\beta, \alpha, \beta \Vdash \alpha \qquad \beta \Vdash \alpha, \beta, \alpha$$

11. Dowód formuły: $(\alpha \equiv \beta) \to (\beta \to \alpha)$.

Trafność i pełność

Opisana wyżej konsekwencja Gentzenowska w KRZ jest zatem trafna i pełna, ponieważ:

- wszystkie aksjomaty (wybranej wyżej aksjomatyki KRZ) są tezami omawianego systemu Gentzena;
- relacja $\Vdash$ jest domknięta na odrywanie oraz podstawianie, w sensie omówionym na początku prezentacji.

Oznacza to, że:

- każda teza omawianego systemu Gentzena jest tautologią KRZ,
- każda tautologia KRZ jest tezą omawianego systemu Gentzena.

Część II: Formalizm Gentzena dla KRP

Część II:

Formalizm Gentzena dla KRP

Definicje

Popularne są dwa rachunki sekwentów, pochodzące od Gentzena. Tu omówimy tylko jeden z nich, tzw. ***wnioskowania naturalne Gentzena***. W obu formalizmach zakłada się, że wszystkie zmienne indywidualne są dwóch rodzajów:

- zmienne wolne (zmienne realne)
- zmienne związane (zmienne pozorne).

Niech $\mathcal{R} = \{u_1, u_2, \ldots\}$ będzie zbiorem zmiennych wolnych, a $\mathcal{P} = \{x_1, x_2, \ldots\}$ zbiorem zmiennych związanych. Dokonując podstawień w formułach, możemy zatem zawsze wstawiać do formuł zmienne ze zbioru $\mathcal{R}$.

Formuły w systemie Gentzena (nazywane ***formułami Gentzenowskimi***) mają więc zmienne wolne w zbiorze $\mathcal{R}$, a zmienne związane w zbiorze $\mathcal{P}$.

Definicje

Każdą parę uporządkowaną (X, Y), gdzie X i Y są skończonymi zbiorami formuł, nazywamy ***sekwentem***. Używa się także terminu: ***sekwencja***. Jeśli (X, Y) jest sekwentem, to używa się np. zapisu $X \Vdash Y$. Zamiast $X_1 \cup X_2 \Vdash Y_1 \cup Y_2$ pisze się zwykle $X_1, X_2 \Vdash Y_1, Y_2$. W szczególności, zamiast np. $X \cup \{\alpha\} \Vdash Y \cup \{\beta\}$ pisze się $X, \alpha \Vdash Y, \beta$ (i analogicznie dla $(\{\alpha\} \cup X \Vdash \{\beta\} \cup Y)$, itp.).
Niech $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ i $Y = \{\beta_1, \beta_2, \ldots \beta_m\}$. Mówimy, że sekwent $X \Vdash Y$ jest ***tautologią Gentzenowską*** wtedy i tylko wtedy, gdy tautologią KRP jest:

$$(\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n) \rightarrow (\beta_1 \vee \beta_2 \vee \ldots \vee \beta_m).$$

Tak więc, zamierzonym znaczeniem sekwentu $X \Vdash Y$ jest, iż z koniunkcji przesłanek ze zbioru X wynika logicznie co najmniej jeden wniosek ze zbioru Y.

Definicje

Zdefiniujemy teraz w sposób ścisły relację $\Vdash$, dla dowolnych skończonych zbiorów X, Y formuł Gentzenowskich. Definicja jest indukcyjna.

- 1. $X \Vdash^0 Y$ wtedy i tylko wtedy, gdy $X \cap Y \neq \emptyset$
- 2. $X \Vdash^{n+1} Y$ wtedy i tylko wtedy, gdy zachodzi jeden z warunków (A), (B) lub (C) podanych poniżej:

- (A) $X \Vdash^n Y$,

Definicje

- (B) istnieją zbiory formuł X_1, Y_1 oraz formuły α, β takie, że zachodzi jeden z warunków:

$$
\begin{array}{rl}
(+\rightarrow) & X = X_1 \cup \{\alpha \rightarrow \beta\} \text{ i } X_1 \cup \{\beta\} \Vdash^n Y \text{ i } X_1 \Vdash^n \{\alpha\} \cup Y \\
(\rightarrow +) & Y = Y_1 \cup \{\alpha \rightarrow \beta\} \text{ i } X \cup \{\alpha\} \Vdash^n \{\beta\} \cup Y_1 \\
(+\neg) & X = X_1 \cup \{\neg\alpha\} \text{ i } X_1 \Vdash^n \{\alpha\} \cup Y \\
(\neg+) & Y = Y_1 \cup \{\neg\alpha\} \text{ i } X \cup \{\alpha\} \Vdash^n Y_1 \\
(+\wedge) & X = X_1 \cup \{\alpha \wedge \beta\} \text{ i } X_1 \cup \{\alpha, \beta\} \Vdash^n Y \\
(\wedge+) & Y = Y_1 \cup \{\alpha \wedge \beta\} \text{ i } X \Vdash^n \{\alpha\} \cup Y_1 \text{ oraz } X \Vdash^n \{\beta\} \cup Y_1 \\
(+\vee) & X = X_1 \cup \{\alpha \vee \beta\} \text{ i } X_1 \cup \{\alpha\} \Vdash^n Y \text{ oraz } X_1 \cup \{\beta\} \Vdash^n Y \\
(\vee+) & Y = Y_1 \cup \{\alpha \vee \beta\} \text{ i } X \Vdash^n \{\alpha, \beta\} \cup Y_1 \\
(+\equiv) & X = X_1 \cup \{\alpha \equiv \beta\} \text{ i } X_1 \cup \{\alpha, \beta\} \Vdash^n Y \text{ oraz } X_1 \Vdash^n \{\alpha, \beta\} \cup Y \\
(\equiv +) & Y = Y_1 \cup \{\alpha \equiv \beta\} \text{ i } X \cup \{\alpha\} \Vdash^n \{\beta\} \cup Y_1 \text{ oraz } X \cup \{\beta\} \Vdash^n \{\alpha\} \cup Y_1,
\end{array}
$$

Definicje

- (C): istnieją liczba naturalna k, term t (z ewentualnymi zmiennymi jedynie z $\mathcal{R}$), formuła α, w której x_k jest zmienną z $\mathcal{P}$ oraz zbiory X_1, Y_1 formuł bez zmiennych z $\mathcal{P}$ takie, że zachodzi jeden z warunków (tu $S(t, x_k, \alpha)$ oznacza wynik podstawienia termu t za zmienną x_k w formule α):

(+∀) $X = X_1 \cup \{\forall x_k \alpha\}$ i $\{S(t, x_k, \alpha)\} \Vdash^n Y$

(∀+) $Y = Y_1 \cup \{\forall x_k \alpha\}$ i przy pewnym m, zmienna u_m nie występuje jako wolna ani w α, ani w formułach z $X \cup Y_1$ i $X \Vdash^n \{S(u_m, x_k, \alpha)\} \cup Y_1$

(+∃) $X = X_1 \cup \{\exists x_k \alpha\}$ i przy pewnym m, zmienna u_m nie występuje jako wolna ani w α, ani w formułach z $X_1 \cup Y$ i $X_1 \cup \{S(u_m, x_k, \alpha)\} \Vdash^n Y$

(∃+) $Y = Y_1 \cup \{\exists x_k \alpha\}$ i $X \Vdash^n \{S(t, x_k, \alpha)\} \cup Y_1$.

- 3. $X \Vdash Y$ wtedy i tylko wtedy, gdy $X \Vdash^n Y$ dla pewnej $n \geqslant 0$.

Definicje

Określona w ten sposób relacja $\Vdash$ ma własności przysługujące ogólnym relacjom konsekwencji. Zachodzą dla niej także twierdzenia o trafności i pełności.

- Reguły wnioskowania będziemy (tradycyjnie, odmiennie niż w pierwszej części tej prezentacji) zapisywali w postaci „ułamków”, w których nad kreską zapisujemy sekwenty, będące przesłankami, a pod kreską wniosek. Gdy mamy więcej niż jedną przesłankę, to oddzielamy je separatorem w postaci średnika: ; .
- (0) $\dfrac{X \cap Y \neq \emptyset}{X \Vdash Y}$.
- Reguły dotyczące spójników zdaniowych są oczywiście takie same, jak w rachunku sekwentów dla KRZ (zobacz początek tej prezentacji).

Definicje

Dochodzą jeszcze cztery reguły dotyczące kwantyfikatorów:

$(+\forall)$	$\dfrac{X, S(t, x_k, \alpha) \Vdash Y}{X, \forall x_k \alpha \Vdash Y}$	$(\forall +)$	$\dfrac{X \Vdash S(u_m, x_k, \alpha), Y}{X \Vdash \forall x_k \alpha, Y}$
$(+\exists)$	$\dfrac{X, S(u_m, x_k, \alpha) \Vdash Y}{X, \exists x_k \alpha \Vdash Y}$	$(\exists +)$	$\dfrac{X \Vdash S(t, x_k, \alpha), Y}{X \Vdash \exists x_k \alpha, Y}$

Reguły $(\forall +)$ oraz $(+\exists)$ są obwarowane dodatkowymi zastrzeżeniami. Mogą one mianowicie być stosowane, o ile:

- $(\forall +)$ zmienna u_m nie jest zmienną wolną w α ani w żadnej z formuł występujących w X lub w Y,
- $(+\exists)$ zmienna u_m nie jest zmienną wolną w żadnej z formuł występujących w X lub w Y.

Definicje

Operację $\mathbf{G}_{krp}$ ***konsekwencji Gentzenowskiej*** w KRP określamy następująco dla dowolnego zbioru formuł Gentzena X:

$\mathbf{G}_{krp}(X) = \{\alpha : \alpha$ jest formułą Gentzena oraz
$Y \Vdash \alpha$ dla pewnego skończonego zbioru $Y \subseteq X\}$.

Tak określona operacja $\mathbf{G}_{krp}$ ma własności (C1)–(C4) z definicji ogólnej operacji konsekwencji.

Zbiór $\mathbf{G}_{krp}(\emptyset)$, czyli ogół wszystkich $\Vdash$-konsekwencji zbioru pustego, to zbiór wszystkich ***tez*** systemu Gentzena dla KRP. Jeśli więc, stosując podane wyżej reguły, otrzymamy sekwent $\emptyset \Vdash \alpha$, to α jest tezą systemu Gentzena. Zamiast $\emptyset \Vdash X$ piszemy $\Vdash X$, a zamiast $\emptyset \Vdash \alpha$ piszemy $\Vdash \alpha$.

Przykłady

Oto cztery proste przykłady dowodów w rozważanym systemie, zaczerpnięte z monografii Pogorzelski 1981. W ostatniej z prawej kolumnie podawany jest symbol reguły, na mocy której formuła z rozważanego wiersza została otrzymana jako wniosek z formuły z wiersza poprzedzającego.

$$\begin{array}{cc}
S(t, x_k, \alpha) \Vdash S(t, x_k, \alpha) & \\
\hline
\forall x_k \alpha \Vdash S(t, x_k \alpha) & (+\forall) \\
\hline
\Vdash \forall x_k \alpha \rightarrow S(t, x_k, \alpha) & (\rightarrow +).
\end{array}$$

Dowód sekwentu: $\Vdash \forall x_k \alpha \rightarrow S(t, x_k, \alpha)$.

Przykłady

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{S(u,x_k,\alpha), S(u,x_k,\alpha\rightarrow\beta) \Vdash S(u,x_k,\beta)}{\forall x_k\alpha, S(u,x_k,\alpha\rightarrow\beta) \Vdash S(u,x_k,\beta)}\ (+\forall)}{\forall x_k\alpha, \forall x_k(\alpha\rightarrow\beta) \Vdash S(u,x_k,\beta)}\ (+\forall)}{\forall x_k\alpha, \forall x_k(\alpha\rightarrow\beta) \Vdash \forall x_k\beta}\ (\forall+)}{\forall x_k(\alpha\rightarrow\beta) \Vdash \forall x_k\alpha \rightarrow \forall x_k\beta}\ (\rightarrow+)}{\Vdash \forall x_k(\alpha\rightarrow\beta) \rightarrow (\forall x_k\alpha \rightarrow \forall x_k\beta)}\ (\rightarrow+).
$$

Dowód sekwentu: $\Vdash \forall x_k(\alpha \rightarrow \beta) \rightarrow (\forall x_k\alpha \rightarrow \forall x_k\beta)$. Zakładamy, że u nie jest zmienną wolną ani w α, ani w β.

Przykłady

$$\cfrac{\cfrac{\alpha \Vdash S(u, x_k, \alpha)}{\alpha \Vdash \forall x_k \alpha} \quad (\forall +)}{\Vdash \alpha \rightarrow \forall x_k \alpha} \quad (\rightarrow +).$$

Dowód sekwentu: $\Vdash \alpha \rightarrow \forall x_k \alpha$.

Przykłady

$$\dfrac{\dfrac{\dfrac{\dfrac{S(u,x_k,\alpha),\neg S(u,x_k,\alpha)\Vdash\emptyset}{S(u,x_k,\alpha),\forall x_k\neg\alpha\Vdash\emptyset}\,(+\forall)}{S(u,x_k,\alpha)\Vdash\neg\forall x_k\neg\alpha}\,(\neg+)}{\exists x_k\alpha\Vdash\neg\forall x_k\neg\alpha}\,(+\exists)\qquad\dfrac{\dfrac{\dfrac{\Vdash S(u,x_k,\alpha),\neg S(u,x_k,\alpha)}{\Vdash\exists x_k\alpha,\neg S(u,x_k,\alpha)}\,(\exists+)}{\Vdash\exists x_k\alpha,\forall x_k\neg\alpha}\,(\forall+)}{\neg\forall x_k\neg\alpha\Vdash\exists x_k\alpha}\,(+\neg)}{\Vdash\exists x_k\alpha\equiv\neg\forall x_k\neg\alpha}\ (\exists+).$$

Dowód sekwentu: $\Vdash \exists x_k\alpha \equiv \neg\forall x_k\neg\alpha$. Zakładamy, że u nie jest zmienną wolną w formule α.

Wykorzystywana literatura (części I i II)

- Gallier, J.H. 1986. *Logic for Computer Science.* Harper and Row, New York.
- Gentzen, G. 1935. Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift* **39**, 176–210, 405–431.
- Indrzejczak, A. 2006. *Hybrydowe systemy dedukcyjne w logikach modalnych.* Wydawnictwo Uniwersytetu Łódzkiego, Łodź.
- Jaśkowski, S. 1934. On the Rules of Suppositions in Formal Logic. *Studia Logica* **I**, 5–32.
- Lyndon, R.C. 1978. *O logice matematycznej*. PWN, Warszawa.
- Ławrow, I.A., Maksimowa, L.L. 2004. *Zadania z teorii mnogości, logiki matematycznej i teorii algorytmów*. Wydawnictwo Naukowe PWN, Warszawa.

Wykorzystywana literatura (części I i II)

- Pogorzelski, W.A. 1975. *Klasyczny rachunek zdań. Zarys teorii*. PWN, Warszawa.
- Pogorzelski, W.A. 1981. *Klasyczny rachunek kwantyfikatorów. Zarys teorii.* Państwowe Wydawnictwo Naukowe, Warszawa.
- Pogorzelski, W.A. 1992. *Elementarny słownik logiki formalnej*. Uniwersytet Warszawski, Filia w Białymstoku, Białystok.
- Rasiowa, H., Sikorski, R. 1963. *The Mathematics of Metamathematics.* Państwowe Wydawnictwo Naukowe, Warszawa.
- Smullyan, R. 1968. *First-Order Logic.* Springer Verlag, Berlin.

Część III: Rezolucja w KRZ

Część III:

Rezolucja w KRZ

Rezolucja w KRZ

Kolejna z omawianych operacji konsekwencji w KRZ wykorzystuje ***metodę rezolucji***.

- Postać klauzulowa formuł.
- Reguła rezolucji.
- Dowody rezolucyjne.
- Trafność i pełność metody rezolucyjnej.

Uwaga. Dowody oparte na metodzie rezolucji mają istotne zastosowania np. w automatycznym dowodzeniu twierdzeń.

Postać klauzulowa formuł

Klauzulą nazwiemy dowolny skończony zbiór literałów.

Klauzule odpowiadają alternatywom elementarnym. Tak więc, jeśli $\ell_1 \vee \ell_2 \vee \ldots \vee \ell_n$ jest alternatywą elementarną, to odpowiadająca jej klauzula jest zbiorem $\{\ell_1, \ell_2, \ldots, \ell_n\}$.
Umawiamy się, że literały, które (ewentualnie) występują więcej niż raz w danej alternatywie elementarnej zapisujemy tylko raz w odpowiadającej jej klauzuli. Ponieważ $(\alpha \vee \alpha) \equiv \alpha$ jest tezą KRZ, umowa ta niczego nie „psuje".

Klauzulę pustą (nie zawierającą żadnych elementów) oznaczamy przez $\Box$.

Postać klauzulowa formuł

Zbiory klauzul są więc rodzinami zbiorów literałów. Każdej formule w kpn odpowiada pewien zbiór klauzul. Jeśli α jest kpn, to jest postaci: $\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n$, gdzie każda formuła α_i jest alternatywą elementarną postaci:

$$\ell_1^i \vee \ell_2^i \vee \ldots \vee \ell_{m_i}^i,$$

gdzie z kolei każda formuła ℓ_j^i jest literałem. Formule α odpowiada wtedy zbiór klauzul:

$$\{\{\ell_1^1, \ell_2^1, \ldots, \ell_{m_1}^1\}, \{\ell_1^2, \ell_2^2, \ldots, \ell_{m_2}^2\}, \ldots, \{\ell_1^n, \ell_2^n, \ldots, \ell_{m_n}^n\}\}.$$

Umawiamy się, że alternatywy elementarne, które (ewentualnie) występują więcej niż raz w danej koniunkcyjnej postaci normalnej zapisujemy tylko raz w odpowiadającej jej rodzinie zbiorów. Również ta umowa jest poprawna.

Postać klauzulowa formuł

Dla przykładu, formule w koniunkcyjnej postaci normalnej:

$$(p_1 \vee p_2 \vee \neg p_3) \wedge (p_3 \vee p_4) \wedge \neg p_1 \wedge (\neg p_2 \vee \neg p_4)$$

odpowiada następujący zbiór klauzul:

$$\{\{p_1, p_2, \neg p_3\}, \{p_3, p_4\}, \{\neg p_1\}, \{\neg p_2, \neg p_4\}\}.$$

Można wprowadzić jakiś symbol relacyjny, powiedzmy $\rightleftharpoons$, pozwalający na skrótowe zapisywanie wypowiedzi:

- $\alpha \rightleftharpoons S$ czytamy: „formule α w kpn odpowiada zbiór klauzul S" ***lub, równoznacznie***
- $\alpha \rightleftharpoons S$ czytamy: „zbiór klauzul S reprezentuje formułę α w kpn".

Symbol $\rightleftharpoons$ należy oczywiście do metajęzyka.

Postać klauzulowa formuł

Pamiętamy, że algorytm ustalania, czy dana formuła języka KRZ jest tautologią ma złożoność wykładniczą: aby sprawdzić, czy formuła o n zmiennych zdaniowych jest tautologią KRZ trzeba sprawdzić, jaka jest jej wartość dla 2^n wzz.

Na mocy Twierdzenia o Pełności KRZ, jeśli formuła α ***nie jest*** spełnialna, to możemy to wykazać na drodze dedukcyjnej,

- pokazując, że: $\emptyset \vdash_{krz} \neg\alpha$ ***lub***
- pokazując, że: $\vdash_{jas} \neg\alpha$.

Nie możemy jednak, ani używając konsekwencji $\vdash_{krz}$, ani używając konsekwencji $\vdash_{jas}$ pokazać, że jakaś formuła ***jest*** spełnialna.

Postać klauzulowa formuł

Podobnie, jeśli α wynika logicznie z X (czyli jeśli zachodzi $X \models_{KRZ} \alpha$), to możemy to wykazać,

- pokazując, że: $X \vdash_{krz} \alpha$ ***lub***
- pokazując, że: $X \vdash_{jas} \alpha$.

Jeśli jednak $X \not\models \alpha$, (czyli gdy przy ***co najmniej jednym*** wartościowaniu h, $h[X] \subseteq \{1\}$ oraz $h(\alpha) = 0$), to nie mamy możliwości przedstawienia dowodu (w terminach konsekwencji $\vdash_{krz}$ lub $\vdash_{jas}$), że ***istnieje*** wartościowanie h takie, że $h[X] \subseteq \{1\}$ oraz $h(\alpha) = 0$.

Reguła rezolucji, którą omówimy za chwilę, dostarcza możliwości wykazywania środkami czysto syntaktycznymi, że dana formuła nie jest spełnialna.

Reguła rezolucji: definicja

Niech C_1 i C_2 będą klauzulami i niech literał ℓ występuje w C_1, a literał $\overline{\ell}$ występuje w C_2. Wtedy każdą klauzulę postaci:

$$(C_1 - \{\ell\}) \cup (C_2 - \{\overline{\ell}\})$$

nazywamy ***rezolwentą*** klauzul C_1 i C_2.

Zamiast ***rezolwenta*** używa się też terminu: ***rezolwent***. Logice jest oczywiście obojętny rodzaj gramatyczny. Jeśli C_1 i C_2 są powyższej postaci, to mówimy też, że C_1 i C_2 ***kolidują*** ze względu na literały ℓ oraz $\overline{\ell}$.

Reguła rezolucji: przykład

Niech:

- $C_1 = \{p_1, \neg p_2, p_3\}$
- $C_2 = \{p_2, \neg p_3, p_4\}$.

Widać, że C_1 i C_2 kolidują ze względu na następujące pary literałów komplementarnych:

- (a) $(\neg p_2, p_2)$,
- (b) $(p_3, \neg p_3)$.

Wtedy rezolwentami C_1 i C_2 są klauzule:

- (a) $\{p_1, p_3, \neg p_3, p_4\}$
- (b) $\{p_1, p_2, \neg p_2, p_4\}$.

Dowody rezolucyjne: definicje

(i) ***Dowodem rezolucyjnym*** klauzuli C ze zbioru klauzul S nazywamy każdy skończony ciąg klauzul $C_1, \ldots, C_n$ taki, że:

- C jest identyczna z C_n
- każda klauzula C_i $(1 \leqslant i \leqslant n)$ jest albo elementem zbioru S albo rezolwentą pewnych klauzul C_j oraz C_k dla $j, k < i$.

(ii) Jeśli istnieje dowód rezolucyjny C z S, to mówimy, że C jest ***rezolucyjnie dowodliwa*** (lub: ***rezolucyjnie wyprowadzalna***) z S i oznaczamy ten fakt przez $S \vdash_{res} C$.
(iii) Każdy dowód rezolucyjny klauzuli pustej $\Box$ ze zbioru S nazywamy ***rezolucyjną refutacją*** S. Jeżeli istnieje rezolucyjna refutacja S, to mówimy, że S jest ***rezolucyjnie odrzucalny*** i oznaczamy ten fakt przez $S \vdash_{res} \Box$.

Dowody rezolucyjne: definicje

(iv) Dla dowolnego zbioru klauzul S niech $res(S)$ będzie zbiorem wszystkich rezolwent wszystkich par elementów S. Zdefiniujmy:

- $res_0(S) = S$
- $res_n = res_{n-1}(S) \cup res(res_{n-1}(S))$ dla $n > 0$
- $\mathcal{R}(S) = \bigcup\{res_n(S) : n \in \mathcal{N}\}$.

Zbiór $\mathcal{R}(S)$ nazywamy ***domknięciem rezolucyjnym*** zbioru S.
(v) ***Rezolucyjnym drzewem dowodowym*** klauzuli C ze zbioru klauzul S nazywamy każde drzewo binarne T o następujących własnościach:

- korzeniem T jest C
- liśćmi T są pewne elementy zbioru S
- bezpośrednimi następnikami wierzchołka D nie będącego liściem są klauzule D_1 oraz D_2, których rezolwentą jest D.

Uwaga. Często mówi się o dowodach rezolucyjnych ***formuł*** ze ***zbiorów formuł***. Rozumiemy przez to, że wszystkie brane pod uwagę formuły:

- (1) zostały przekształcone do równoważnych im inferencyjnie kpn;
- (2) zostały zastąpione (przy uwzględnieniu (1)) odpowiadającymi im zbiorami klauzul.

Wtedy oczywiście należy powiedzieć, co rozumiemy przez dowód rezolucyjny ***zbioru klauzul*** ze ***zbiorów zbiorów*** klauzul. Jeśli piszemy skrótowo $S \vdash_{res} \alpha$, gdzie S jest zbiorem ***formuł***, a α jest ***formułą*** to rozumiemy przez to, że:

- α została zastąpiona przez swoją kpn, a ta z kolei przez odpowiedni zbiór klauzul,
- każda formuła $\beta \in S$ została zastąpiona przez swoją kpn, a ta z kolei przez odpowiedni zbiór klauzul,
- $S \vdash_{res} \alpha$ oznacza, że ***każda*** klauzula występująca w zbiorze klauzul odpowiadającym kpn formuły α ma dowód rezolucyjny ze zbioru klauzul odpowiadającemu ***koniunkcji*** pewnych formuł z S.

Dowody rezolucyjne: komentarze

Uwaga. Możemy rozważać ***dowolne*** zbiory klauzul jako poprzedniki relacji $\vdash_{res}$. Z Twierdzenia o Zwartości oraz z Twierdzeń o Trafności i Pełności metody rezolucyjnej (które udowodnimy za chwilę) wynika, że jeśli $S \vdash_{res} \alpha$, to istnieje ***skończony*** zbiór $S' \subseteq S$ taki, że $S' \vdash_{res} \alpha$.

Uwaga. Nietrudno sprawdzić (korzystając z indukcji po długości dowodu rezolucyjnego), że zachodzi następująca równoważność:

- Istnieje rezolucyjne drzewo dowodowe dla C z S wtedy i tylko wtedy, gdy C jest rezolucyjnie dowodliwa z S, czyli gdy $S \vdash_{res} C$.

Uwaga. Rozważamy drzewa, których wierzchołki są znakowane ***zbiorami*** literałów.

Dowody rezolucyjne: przykład 1

Niech $S = \{p_1 \rightarrow p_2, p_2 \rightarrow p_3, p_1, \neg p_3\}$ i niech $\bigwedge S$ będzie koniunkcją wszystkich formuł ze zbioru S. Pokażemy, że $\bigwedge S \vdash_{res} \Box$. Formuła $\bigwedge S$ ma następującą kpn: $(\neg p_1 \vee p_2) \wedge (\neg p_2 \vee p_3) \wedge p_1 \wedge \neg p_3$. Odpowiada jej zatem zbiór klauzul:

$$\{\{\neg p_1, p_2\}, \{\neg p_2, p_3\}, \{p_1\}, \{\neg p_3\}\}.$$

A oto zapowiadany dowód rezolucyjny:

1.	$\{\neg p_1, p_2\}$	przesłanka
2.	$\{\neg p_2, p_3\}$	przesłanka
3.	$\{p_1\}$	przesłanka
4.	$\{\neg p_3\}$	przesłanka
5.	$\{\neg p_1, p_3\}$	rezolwenta (1) i (2)
6.	$\{p_3\}$	rezolwenta (3) i (5)
7.	$\Box$	rezolwenta (4) i (6).

Dowody rezolucyjne: przykład 1

Zwykle takie dowody rezolucyjne zapisuje się w poniższej postaci:

1.	$\neg p_1 \vee p_2$	przesłanka
2.	$\neg p_2 \vee p_3$	przesłanka
3.	p_1	przesłanka
4.	$\neg p_3$	przesłanka
5.	$\neg p_1 \vee p_3$	rezolwenta (1) i (2)
6.	p_3	rezolwenta (3) i (5)
7.	$\square$	rezolwenta (4) i (6).

Informatycy stosują inne jeszcze skróty notacyjne, czym nie będziemy się tutaj przejmować.

Dowody rezolucyjne: przykład 1

Zauważmy, że $\{p_1 \rightarrow p_2, p_2 \rightarrow p_3, p_1\} \models_{KRZ} p_3$, co oznacza, że zbiór

$$\{p_1 \rightarrow p_2, p_2 \rightarrow p_3, p_1, \neg p_3\}$$

nie jest spełnialny (nie istnieje wartościowanie, przy którym wszystkie elementy tego zbioru mają wartość 1).

Pokażemy za chwilę, że zbiór klauzul S jest rezolucyjnie odrzucalny dokładnie wtedy, gdy nie jest spełnialna formuła, której kpn odpowiada (skończonemu podzbiorowi) S.

Dowody rezolucyjne: przykład 2

Pokażemy, że zbiór formuł

$$S = \{p_1 \rightarrow (\neg p_2 \vee (p_3 \wedge p_4)), p_1, p_2, \neg p_4\}$$

jest rezolucyjnie odrzucalny. Tworzymy koniunkcję $\bigwedge S$ wszystkich formuł z S:

$$(p_1 \rightarrow (\neg p_2 \vee (p_3 \wedge p_4))) \wedge p_1 \wedge p_2 \wedge \neg p_4,$$

a po przekształceniu tej formuły do kpn tworzymy odpowiadający jej zbiór klauzul:

$$\{\{\neg p_1, \neg p_2, p_3\}, \{\neg p_1, \neg p_2, p_4\}, \{p_1\}, \{p_2\}, \{\neg p_4\}\}.$$

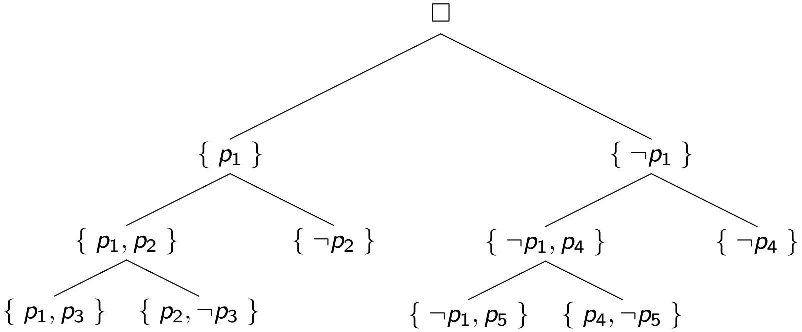
Dowody rezolucyjne: przykład 2

Dowód rezolucyjny zapiszemy korzystając z uproszczenia notacji zastosowanego w poprzednim przykładzie:

1.	$\neg p_1 \vee \neg p_2 \vee p_3$	przesłanka
2.	$\neg p_1 \vee \neg p_2 \vee p_4$	przesłanka
3.	p_1	przesłanka
4.	p_2	przesłanka
5.	$\neg p_4$	przesłanka
6.	$\neg p_1 \vee \neg p_2$	rezolwenta 2 i 5
7.	$\neg p_1$	rezolwenta 4 i 6
8.	$\Box$	rezolwenta 3 i 7.

Dowody rezolucyjne: przykład 3

Niech $S = \{\{p_1, p_3\}, \{p_2, \neg p_3\}, \{\neg p_2\}, \{\neg p_1, p_5\}, \{\neg p_4\}, \{p_4, \neg p_5\}\}$ będzie zbiorem klauzul. Poniższe drzewo jest rezolucyjnym drzewem dowodowym klauzuli $\Box$ ze zbioru S (co oznacza, że S jest rezolucyjnie odrzucalny):



Dowody rezolucyjne: przykład 4

Pokażemy, że ze zbioru:

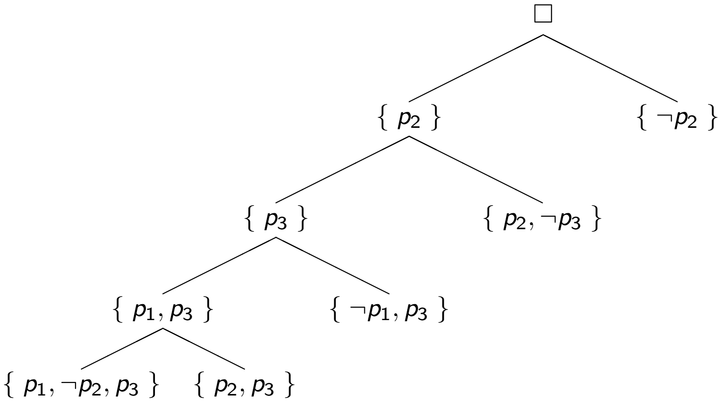
$$\{\{p_1, \neg p_2, p_3\}, \{p_2, p_3\}, \{\neg p_1, p_3\}, \{p_2, \neg p_3\}, \{\neg p_2\}\}$$

wyprowadzić można klauzulę pustą $\Box$.

1.	$\{p_1, \neg p_2, p_3\}$	przesłanka
2.	$\{p_2, p_3\}$	przesłanka
3.	$\{\neg p_1, p_3\}$	przesłanka
4.	$\{p_2, \neg p_3\}$	przesłanka
5.	$\{\neg p_2\}$	przesłanka
6.	$\{p_1, p_3\}$	rezolwenta 1 i 2
7.	$\{p_3\}$	rezolwenta 6 i 3
8.	$\{p_2\}$	rezolwenta 7 i 4
9.	$\Box$	rezolwenta 8 i 5.

Dowody rezolucyjne: przykład 4

Powyższe wyprowadzenie reprezentowane jest przez następujące rezolucyjne drzewo dowodowe:



Banalność metody rezolucji?

Powyższe przykłady pokazują, że stosowanie reguły rezolucji jest banalnie proste. Mogą więc skłaniać do (pochopnej!) konkluzji, że reguła rezolucji może zastąpić wszelkie skomplikowane techniki dowodowe (metodę aksjomatyczną, dedukcję naturalną, itd.). Rzecz ma się następująco. Owszem, reguła rezolucji nie jest skomplikowana i — jak pokażemy za chwilę — jest trafna i pełna. Jednak owa prostota ma też swoją cenę: zbiory klauzul odpowiadają formułom w koniunkcyjnych postaciach normalnych, i choć istnieje algorytm znajdowania dla każdej formuły równoważnej jej inferencyjnie formuły w kpn, to postępowanie wedle jego zaleceń jest dla Człowieka wielce czasochłonne. Inaczej rzecz się ma z Maszynami liczącymi, które stosunkowo szybko znajdują kpn, a potem przeprowadzają dowody rezolucyjne.

Tak więc, nie ma ucieczki (przed Myśleniem): choć bezmyślną pracę można powierzyć Maszynom, to praca twórcza (np. znajdowanie dowodów) stale należy do Człowieka.

Trafność metody rezolucji

Twierdzenie. (*Trafność metody rezolucji w KRZ*)

Niech S będzie zbiorem klauzul. Jeśli $\Box \in \mathcal{R}(S)$, to S nie jest spełnialny w KRZ.

Twierdzenie o trafności rezolucji w KRZ mówi zatem, że: jeżeli istnieje rezolucyjna refutacja S, to S nie jest spełnialny w KRZ.

Dowód twierdzenia o trafności rezolucji w pliku: **rezolkrz.pdf**.

Pełność metody rezolucji

Twierdzenie. (***Pełność metody rezolucji w KRZ***).

Jeżeli S nie jest spełnialny w KRZ, to $\Box \in \mathcal{R}(S)$.

Twierdzenie o pełności rezolucji w KRZ mówi zatem, że: jeżeli S nie jest spełnialny w KRZ, to istnieje rezolucyjna refutacja S.

Dowód twierdzenia o pełności rezolucji w pliku: **rezolkrz.pdf**.

Dowody rezolucyjne: dalsze przykłady

Skoro metoda rezolucji jest trafna i pełna, to można jej używać np. dla ustalania, czy:

- formuła języka KRZ jest tautologią KRZ
- formuła języka KRZ jest spełnialna
- formuła języka KRZ nie jest spełnialna
- formuła α wynika logicznie ze zbioru formuł X
- zbiór formuł X jest spełnialny
- zbiór formuł X nie jest spełnialny, itd.

Rozważmy kilka przykładów.

Dowody rezolucyjne: przykład 5

Rozważmy zbiór klauzul: $S = \{\{p_1, p_2, \neg p_3\}, \{p_3\}, \{p_1, \neg p_2, p_3\}, \{\neg p_3\}\}$. Zauważmy, że w zależności od kolejności doboru klauzul, do których stosujemy regułę rezolucji, możemy otrzymać różne wyniki końcowe:

1.	$\{p_1, p_2, \neg p_3\}$	przesł.
2.	$\{p_3\}$	przesłanka
3.	$\{p_1, \neg p_2, p_3\}$	przesł.
4.	$\{\neg p_3\}$	przesł.
5.	$\square$	rezolw. 2 i 4.

1.	$\{p_1, p_2, \neg p_3\}$	przesł.
2.	$\{p_3\}$	przesł.
3.	$\{p_1, \neg p_2, p_3\}$	przesł.
4.	$\{\neg p_3\}$	przesł.
5.	$\{p_1, p_2\}$	rezolw. 1 i 2.
6.	$\{p_1, \neg p_2\}$	rezolw. 3 i 4
7.	$\{p_1\}$	rezolw. 5 i 6.

Tak więc, zbiór S ***nie jest*** spełnialny, ponieważ istnieje ***co najmniej jedno*** wyprowadzenie $\square$ ze zbioru S.

Dowody rezolucyjne: przykład 6

Pokażemy, że

$$((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma) \wedge (\gamma \rightarrow \alpha) \wedge (\alpha \vee \beta \vee \gamma)) \rightarrow (\alpha \wedge \beta \wedge \gamma)$$

jest tautologią KRZ.

Jest tak dokładnie wtedy, gdy zbiór:

$$\{\alpha \rightarrow \beta, \beta \rightarrow \gamma, \gamma \rightarrow \alpha, \alpha \vee \beta \vee \gamma, \neg(\alpha \wedge \beta \wedge \gamma)\}$$

jest semantycznie sprzeczny (nie jest spełnialny).

To z kolei jest równoważne temu, że zbiór:

$$\{\neg\alpha \vee \beta, \neg\beta \vee \gamma, \neg\gamma \vee \alpha, \alpha \vee \beta \vee \gamma, \neg\alpha \vee \neg\beta \vee \neg\gamma\}$$

nie jest spełnialny.

Dowody rezolucyjne: przykład 6

Każda z formuł tego zbioru jest podstawieniem jakiejś alternatywy elementarnej: otrzymujemy je, gdy dokonamy np. podstawień p_1/α, p_2/β, p_3/γ.
W takich przypadkach usprawiedliwione jest pisanie dowodów rezolucyjnych z użyciem *metazmiennych* reprezentujących dowolne formuły języka KRZ i traktowanie pojedynczych metazmiennych jak literałów.
Na mocy pełności metody rezolucji wystarczy pokazać, że ze zbioru

$$\{\neg\alpha \vee \beta, \neg\beta \vee \gamma, \neg\gamma \vee \alpha, \alpha \vee \beta \vee \gamma, \neg\alpha \vee \neg\beta \vee \neg\gamma\}$$

można wyprowadzić klauzulę $\Box$:

Dowody rezolucyjne: przykład 6

1.	$\neg\alpha \vee \beta$	przesłanka
2.	$\neg\beta \vee \gamma$	przesłanka
3.	$\neg\gamma \vee \alpha$	przesłanka
4.	$\alpha \vee \beta \vee \gamma$	przesłanka
5.	$\neg\alpha \vee \neg\beta \vee \neg\gamma$	przesłanka
6.	$\alpha \vee \beta$	rezolwenta 4 i 3
7.	β	rezolwenta 6 i 1
8.	γ	rezolwenta 7 i 2
9.	α	rezolwenta 8 i 3
10.	$\neg\beta \vee \neg\gamma$	rezolwenta 9 i 5
11.	$\neg\gamma$	rezolwenta 7 i 10
12.	$\Box$	rezolwenta 8 i 11.

Dowody rezolucyjne: przykład 7

Pokażemy, że formuła:

$$(\bigstar)\quad \neg((\alpha \to \beta) \to ((\alpha \vee \gamma) \to (\beta \vee \gamma)))$$

nie jest spełnialna. Oznacza to, że formuła:

$$(\bigstar\bigstar)\quad (\alpha \to \beta) \to ((\alpha \vee \gamma) \to (\beta \vee \gamma))$$

jest tautologią KRZ.

W tym celu wystarczy pokazać, że ze zbioru klauzul otrzymanego z kpn formuły $(\bigstar)$ można wyprowadzić $\Box$. Koniunkcyjną postacią normalną formuły $(\bigstar)$ jest:

$$(\neg\alpha \vee \beta) \wedge (\alpha \vee \gamma) \wedge (\neg\beta) \wedge (\neg\gamma).$$

Dowody rezolucyjne: przykład 7

Przeprowadzamy dowód rezolucyjny:

1.	$\neg\alpha \vee \beta$	przesłanka
2.	$\alpha \vee \gamma$	przesłanka
3.	$\neg\beta$	przesłanka
4.	$\neg\gamma$	przesłanka
5.	α	rezolwenta 2 i 4
6.	β	rezolwenta 1 i 5
9.	$\square$	rezolwenta 3 i 6.

Dowody rezolucyjne: przykład 8

Pokażemy, że formuła γ wynika logicznie ze zbioru formuł:

$$S = \{\alpha, (\alpha \wedge \beta) \rightarrow \gamma, \tau \rightarrow \beta, \tau\}.$$

W tym celu wystarczy pokazać, że zbiór

$$\{\alpha, (\alpha \wedge \beta) \rightarrow \gamma, \tau \rightarrow \beta, \tau, \neg\gamma\}$$

nie jest spełnialny.

Każda formuła ze zbioru S jest równoważna alternatywie elementarnej:

1. α
2. $\neg\alpha \vee \neg\beta \vee \gamma$
3. $\neg\tau \vee \beta$
4. τ.

Dowody rezolucyjne: przykład 8

Pokazujemy, że z powyższych klauzul można wyprowadzić $\Box$:

1.	α	przesłanka
2.	$\neg\alpha \vee \neg\beta \vee \gamma$	przesłanka
3.	$\neg\tau \vee \beta$	przesłanka
4.	τ	przesłanka
5.	$\neg\gamma$	przesłanka
6.	$\neg\alpha \vee \neg\beta$	rezolwenta 2 i 5
7.	$\neg\beta$	rezolwenta 6 i 1
8.	$\neg\tau$	rezolwenta 3 i 7
9.	$\Box$	rezolwenta 4 i 8.

Skoro $S \cup \{\neg\gamma\} \vdash_{res} \Box$, to $S \models_{KRZ} \gamma$.

Dowody rezolucyjne: przykład 9

Pokażemy, że formuła β wynika logicznie z następującego zbioru formuł:

$$S = \{\alpha \rightarrow \beta, (\gamma \wedge \delta) \rightarrow \alpha, (\tau \wedge \gamma) \rightarrow \delta, (\theta \wedge \alpha) \rightarrow \gamma, (\theta \wedge \tau) \rightarrow \gamma, \theta, \tau\}.$$

Każda formuła ze zbioru S jest równoważna alternatywie elementarnej:

1. $\neg\alpha \vee \beta$
2. $\neg\gamma \vee \neg\delta \vee \alpha$
3. $\neg\tau \vee \neg\gamma \vee \delta$
4. $\neg\theta \vee \neg\alpha \vee \gamma$
5. $\neg\theta \vee \neg\tau \vee \gamma$
6. θ
7. τ.

Dowody rezolucyjne: przykład 9

1.	$\neg\alpha \vee \beta$	przesłanka
2.	$\neg\gamma \vee \neg\delta \vee \alpha$	przesłanka
3.	$\neg\tau \vee \neg\gamma \vee \delta$	przesłanka
4.	$\neg\theta \vee \neg\alpha \vee \gamma$	przesłanka
5.	$\neg\theta \vee \neg\tau \vee \gamma$	przesłanka
6.	θ	przesłanka
7.	τ	przesłanka
8.	$\neg\tau \vee \gamma$	rezolwenta 5 i 6
9.	γ	rezolwenta 7 i 8
10.	$\neg\delta \vee \alpha$	rezolwenta 2 i 9
11.	$\neg\gamma \vee \delta$	rezolwenta 3 i 7
12.	$\neg\gamma \vee \alpha$	rezolwenta 2 i 11
13.	α	rezolwenta 9 i 12
14.	β	rezolwenta 1 i 13.

Ponieważ uzyskaliśmy rezolucyjne wyprowadzenie β z S, więc na mocy twierdzenia o pełności metody rezolucyjnej otrzymujemy, że $S \models_{KRZ} \beta$.

Dowody rezolucyjne: przykład 9

Dla porównania, przytoczmy jeszcze dowód założeniowy, że $S \vdash_{jas} \beta$:

1.	$\alpha \rightarrow \beta$	założenie
2.	$(\gamma \wedge \delta) \rightarrow \alpha$	założenie
3.	$(\tau \wedge \gamma) \rightarrow \delta$	założenie
4.	$(\theta \wedge \alpha) \rightarrow \gamma$	założenie
5.	$(\theta \wedge \tau) \rightarrow \gamma$	założenie
6.	θ	założenie
7.	τ	założenie
8.	$\theta \wedge \tau$	DK: 6,7
9.	γ	RO: 5,8
10.	$\tau \wedge \gamma$	DK: 7,9
11.	δ	RO: 3,10
12.	$\gamma \wedge \delta$	DK: 9,11
13.	α	RO: 2,12
14.	β	RO: 1,13.

Dowody rezolucyjne: refleksja

Powyższe przykłady mogą osobie nieufnej nasunąć pytanie, po co właściwie zajmować się metodą rezolucji, skoro mamy inne, dobre metody dowodzenia tez.
Podkreślamy, że metoda rezolucji znajduje zastosowanie przede wszystkim w automatycznym dowodzeniu twierdzeń. Przekształcenie nawet bardzo skomplikowanych formuł na równoważne im inferencyjnie kpn nie jest problemem dla szybkich maszyn liczących. Drugi krok w metodzie rezolucyjnej dowodzenia twierdzeń, czyli stosowanie samej reguły rezolucji, jest oczywiście także bardzo prostym zadaniem dla maszyn liczących.

Warto zatem wyobrazić sobie np. zbiór liczący **tysiące** skomplikowanych przesłanek i odetchnąć z ulgą, że możemy w takiej sytuacji powierzyć robotę dedukcyjną Maszynom.

Konsekwencja rezolucyjna

Jest jasne, jak zdefiniować ***operację C_{res} konsekwencji rezolucyjnej*** wyznaczoną przez metodę rezolucji:

$$C_{res}(X) = \{\alpha \in F_{KRZ} : \ X \vdash_{res} \alpha\}.$$

Tak zdefiniowana operacja konsekwencji ma własności (C1)–(C4) ogólnej operacji konsekwencji.

Jest wiele różnych, bardziej subtelnych od powyższego — całkowicie ogólnego — rodzajów rezolucji. Problematyka ta jest intensywnie badana, przede wszystkim w związku z zastosowaniami metody rezolucji w automatycznym dowodzeniu twierdzeń.

Koniec

W pliku rezolkrz.pdf znajdują się dowody twierdzeń o trafności i pełności metody rezolucji w KRZ, a także wszystkie przedstawione tu definicje i przykłady:

http://www.logic.amu.edu.pl/images/e/e3/Rezolkrz.pdf

Zainteresowany czytelnik zechce zajrzeć również do odnośników zamieszczonych na stronie tych wykładów.

Wykorzystywana literatura (część III)

- Baader, F., Snyder, W. 2001. Unification theory. W: *Handbook of Automated Reasoning.*, 446–533.
- Bachmair, L., Ganzinger, H. 2001. Resolution theorem proving. W: *Handbook of Automated Reasoning.*, 19–99.
- Bartley, W.W., III. 1977. *Lewis Carroll's Symbolic Logic.* Clarkson N. Potter, New York.
- Ben-Ari, M. 2005. *Logika matematyczna w informatyce.* Wydawnictwa Naukowo Techniczne.
- Fitting, M. 1990. *First-Order Logic and Automated Theorem Proving.* Springer Verlag, New York Berlin Heidelberg London Paris Tokyo Hong Kong.

Wykorzystywana literatura (część III)

- *Handbook of Automated Reasoning.* 2001. A. Robinson, A. Voronkov (eds.), Elsevier, Amsterdam London New York Oxford Paris Shannon Tokyo, The MIT Press, Cambridge, Massachusetts.
- *Handbook of Tableau Methods*. 1999. Edited by: D'Agostino, M., Gabbay, D.M., Hähnle, R., Posegga, J., Kluwer Academic Publishers, Dordrecht Boston London.
- Hedman, S. 2004. *A first course in logic.* Oxford University Press.
- Letz, R. 1990. First-order tableau methods. W: *Handbook of Tableau Methods*, 125–196.
- Marciszewski, W., Murawski, R. 1995. *Mechanization of Reasoning in a Historical Perspective.* Rodopi, Amsterdam – Atlanta.
- Nerode, A., Shore, R.A. 1997. *Logic for applications.* Springer.