Metod Dowodzenia Twierdzeń I Automatyzacja Rozumowań

Wykład 8: Rachunki Sekwentów

III rok kognitywistyki UAM, 2016–2017

1 Wstęp

Rachunki sekwentów biorą swój początek z prac Gentzena. Zaproponowane przez niego systemy: LK (dla logiki klasycznej pierwszego rzędu) oraz LJ (dla logiki intuicjonistycznej pierwszego rzędu) miały początkowo pełnić rolę pomocniczą w rozważaniach metalogicznych dotyczących opracowanych także przez niego systemów dedukcji naturalnej: NK (dla logiki klasycznej) oraz NJ (dla logiki intuicjonistycznej). Obecnie różne odmiany rachunku sekwentów (dla wielu systemów logiki) są coraz bardziej popularnymi metodami dowodowymi, zarówno w dowodzeniu „ręcznym", jak i w automatycznym dowodzeniu twierdzeń.

Celem Gentzena było także wykazanie niesprzeczności ważnych teorii matematycznych (arytmetyki, analizy). Przypomnijmy, że w 1931 roku Kurt Gödel udowodnił dwa ważne twierdzenia metalogiczne dotyczące teorii wystarczająco bogatych, aby zawrzeć w nich arytmetykę liczb naturalnych (o tych wynikach opowiemy na wykładach w styczniu):

1. Jeśli arytmetyka (pierwszego rzędu) jest ω-niesprzeczna, to jest niezupełna oraz istotnie nierozstrzygalna.
2. Jeśli arytmetyka (pierwszego rzędu) jest niesprzeczna, to nie istnieje dowód jej niesprzeczności w niej samej.

Wykluczona została zatem możliwość udowodnienia niesprzeczności arytmetyki metodami ściśle finitystycznymi, zalecanymi w Programie Hilberta. Gentzen uzyskał dowód niesprzeczności arytmetyki, posługując się szczególnym rodzajem indukcji (tzw. indukcja pozaskończona do ϵ_0).

Rachunek sekwentów, który tu przedstawimy opiera się na *aksjomatach* oraz zestawie reguł *logicznych*, dotyczących wprowadzania stałych logicznych, a także reguł *strukturalnych*.

Język formalny, w którym mówimy o sekwentach ma formalizować zależność między zbiorami formuł polegającą na wyprowadzalności jednego zbioru formuł (w szczególności: zbioru jednoelementowego, czyli jednej formuły) z innego zbioru formuł. Reguły rachunku sekwentów charakteryzują tę zależność poprzez ustalanie, że jeśli owa relacja zachodzi między pewnymi zbiorami formuł, to zachodzi także między innymi takimi zbiorami.

2 Sekwenty

Sekwentem jest dowolna para (Γ, Δ) skończonych zbiorów formuł. Sekwenty zapisujemy, korzystając z jakiejś przyjętej konwencji. Często używane zapisy to:

1. $\Gamma \Longrightarrow \Delta$
2. $\Gamma \Rightarrow \Delta$
3. $\Gamma \vdash \Delta$.

Wybieramy tutaj trzecią z tych notacji. Ponadto, zwykło się dokonywać pewnych uproszczeń notacji, np.:

1. Zamiast $\{\varphi_1, \ldots, \varphi_n\} \vdash \{\psi_1, \ldots, \psi_m\}$ piszemy $\varphi_1, \ldots, \varphi_n \vdash \psi_1, \ldots, \psi_m$.
2. Zamiast $\Gamma \cup \{\psi\} \vdash \Delta$ piszemy $\Gamma, \psi \vdash \Delta$, a zamiast $\Gamma \vdash \Delta \cup \{\psi\}$ piszemy $\Gamma \vdash \Delta, \psi$.
3. Zamiast $\Gamma \vdash \emptyset$ piszemy $\Gamma \vdash$, a zamiast $\emptyset \vdash \Delta$ piszemy $\vdash \Delta$.

Można nadawać różne interpretacje (semantyczne) sekwentom. Za najbardziej naturalną uważa się dość powszechnie interpretację, wedle której sekwent $\Gamma \vdash \Delta$ stwierdza, że jeśli wszystkie formuły z Γ są prawdziwe, to co najmniej jedna formuła z Δ jest prawdziwa.

Formalnie interpretację taką określamy rozszerzając wartościowania boolowskie z formuł na sekwenty. Jeśli v jest wartościowaniem, to piszemy $v(\Gamma \vdash \Delta) = 1$ wtedy i tylko wtedy, gdy $v(\varphi) = 0$ dla pewnej formuły $\varphi \in \Gamma$ lub $v(\psi) = 1$ dla pewnej formuły $\psi \in \Delta$. Innymi słowy, $v(\Gamma \vdash \Delta) = 1$ wtedy i tylko wtedy, gdy: jeśli $v(\varphi) = 1$ dla wszystkich $\varphi \in \Gamma$, to $v(\psi) = 1$ dla co najmniej jednej $\psi \in \Delta$.

Jeśli zatem $\Gamma = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ oraz $\Delta = \{\psi_1, \psi_2, \ldots, \psi_m\}$, to następujące warunki są równoważne:

1. $v(\Gamma \vdash \Delta) = 1$

2. $v((\varphi_1 \wedge \varphi_2 \wedge \ldots \wedge \varphi_n) \to (\psi_1 \vee \psi_2 \vee \ldots \vee \psi_m)) = 1$

3. $v(\neg\varphi_1 \vee \neg\varphi_2 \vee \ldots \vee \neg\varphi_n \psi_1 \vee \psi_2 \vee \ldots \vee \psi_m) = 1.$

Zauważmy, że: $v(\emptyset \vdash \emptyset) = 0$ oraz $v(\vdash \psi) = v(\psi)$, dla dowolnej formuły ψ.
Uwaga. Czasami konieczne bywa rozumienie sekwentów nie jako par *zbiorów* formuł, ale jako par *ciągów* formuł. W niektórych stylizacjach rachunku sekwentów rozważa się także *multizbiory*, czyli zbiory, w których pewne elementy mogą się powtarzać.

3 Reguły

Rachunek ma następujące aksjomaty:

1. $\varphi \vdash \varphi$

2. $\bot \vdash$

3. $\vdash \top$

Reguły logiczne dotyczą poszczególnych spójników prawdziwościowych (tu podamy je dla: negacji, koniunkcji, alternatywy oraz implikacji) i związane są z wprowadzaniem tych spójników w poprzedniku lub następniku sekwentu (najpierw reguły logiczne dla funktorów prawdziwościowych w jednej tabeli, potem po kolei wszystkie reguły systemu):

$(L_\neg)$	$\frac{\Gamma\vdash\Delta,\varphi}{\Gamma,\neg\varphi\vdash\Delta}$	$\frac{\Gamma,\varphi\vdash\Delta}{\Gamma\vdash\Delta,\neg\varphi}$	$(R_\neg)$
$(L_\wedge)$	$\frac{\Gamma,\varphi,\psi\vdash\Delta}{\Gamma,\varphi\wedge\psi\vdash\Delta}$	$\frac{\Gamma\vdash\Delta,\varphi \quad \Gamma\vdash\Delta,\psi}{\Gamma\vdash\Delta,\varphi\wedge\psi}$	$(R_\wedge)$
$(L_\vee)$	$\frac{\Gamma,\varphi\vdash\Delta \quad \Gamma,\psi\vdash\Delta}{\Gamma,\varphi\vee\psi\vdash\Delta}$	$\frac{\Gamma\vdash\Delta,\varphi,\psi}{\Gamma\vdash\Delta,\varphi\vee\psi}$	$(R_\vee)$
$(L_\to)$	$\frac{\Gamma\vdash\Delta,\varphi \quad \Gamma,\psi\vdash\Delta}{\Gamma,\varphi\to\psi\vdash\Delta}$	$\frac{\Gamma,\varphi\vdash\Delta,\psi}{\Gamma\vdash\Delta,\varphi\to\psi}$	$(R_\to)$

Reguły dla negacji:

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma, \neg\varphi \vdash \Delta}\ (L_{\neg}) \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}\ (R_{\neg})$$

Reguły dla koniunkcji:

$$\frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \wedge \psi \vdash \Delta}\ (L_{\wedge}) \qquad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}\ (R_{\wedge})$$

Reguły dla alternatywy:

$$\frac{\Gamma, \varphi \vdash \Delta \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \vee \psi \vdash \Delta}\ (L_{\vee}) \qquad \frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}\ (R_{\vee})$$

Reguły dla implikacji:

$$\frac{\Gamma \vdash \Delta, \varphi \quad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \to \psi \vdash \Delta}\ (L_{\to}) \qquad \frac{\Gamma, \varphi \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \to \psi}\ (R_{\to})$$

Zauważmy, że niektóre reguły wymagają dwóch sekwentów w przesłankach.

Niech uciechą na konwersatorium będzie ustalenie, jak powinny wyglądać reguły dla pozostałych funktorów prawdziwościowych.

Reguły dla formuł zawierających kwantyfikatory:

$$\frac{\varphi(x/t), \Gamma \vdash \Delta}{\forall x\varphi, \Gamma \vdash \Delta}\ (L\forall) \qquad \frac{\Gamma \vdash \Delta, \varphi(x/a)}{\Gamma \vdash \Delta, \forall x\varphi}\ (R\forall)$$

$$\frac{\varphi(x/a), \Gamma \vdash \Delta}{\exists x\varphi, \Gamma \vdash \Delta}\ (L\exists) \qquad \frac{\Gamma \vdash \Delta, \varphi(x/t)}{\Gamma \vdash \Delta, \exists x\varphi}\ (R\exists)$$

Zastrzeżenia:

1. W regułach dla formuł z kwantyfikatorami sekwenty rozumiane są jako pary *ciągów*.

2. W regułach: $(L\exists)$ oraz $(R\forall)$ symbol a jest parametrem, który nie może wystąpić we wniosku reguły.

3. W regułach: $(R\exists)$ oraz $(L\forall)$ symbol t jest termem domkniętym.

Reguły strukturalne:
Osłabienie (weakening):

$$\frac{\Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta}\ (LW) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi}\ (RW)$$

Skrócenie (contraction):

$$\frac{\varphi, \varphi, \Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta}\ (LC) \qquad\qquad \frac{\Gamma \vdash \Delta, \varphi, \varphi}{\Gamma \vdash \Delta, \varphi}\ (RC)$$

Przestawienie (exchange):

$$\frac{\Gamma_1, \varphi, \psi, \Gamma_2 \vdash \Delta}{\Gamma_1, \psi, \varphi, \Gamma_2 \vdash \Delta}\ (LE) \qquad\qquad \frac{\Gamma \vdash \Delta_1, \varphi, \psi, \Delta_2}{\Gamma \vdash \Delta_1, \psi, \varphi, \Delta_2}\ (RE)$$

System o tych regułach oraz aksjomatach będziemy oznaczali przez RS (rachunek sekwentów dla logiki klasycznej).

Rachunek sekwentów dla logiki intuicjonistycznej otrzymujemy z podanego wyżej zestawu aksjomatów oraz reguł poprzez dodanie warunku, że po prawej stronie sekwentów występować może jedynie pojedyncza formuła (a nie skończony zbiór formuł).

Opatrzmy jeszcze komentarzami przedstawione wyżej reguły:

1. Rozważamy tylko reguły *wprowadzania* stałych logicznych (a nie, jak w systemach dedukcji naturalnej, także reguły *eliminacji* stałych logicznych).

2. We wniosku każdej reguły mamy *formułę główną*, czyli tę, która jest wprowadzana na mocy przesłanek. Pozostałe formuły tworzą *kontekst*.

3. *Formułami aktywnymi* nazywamy te formuły w przesłankach reguły, z których otrzymujemy formułę główną tej reguły.

4. Jak zobaczymy pod koniec wykładu, wszystkie reguły systemu RS są *odwracalne*.

5. Zauważmy wreszcie, że każda reguła dotyczy tylko jednej stałej logicznej oraz że we wniosku każdej reguły formuła główna jest tylko jedna.

4 Dowody

W rachunku RS, jak nazwa wskazuje, rachujemy na sekwentach, w tym sensie, że wyprowadzamy jedne sekwenty z innych. Takie wyprowadzenia mają postać drzew.

Definicja. *Dowodem* sekwentu $\Gamma \vdash \Delta$ w systemie RS nazywamy skończone drzewo dwójkowe spełniające następujące warunki:

1. W korzeniu drzewa znajduje się sekwent $\Gamma \vdash \Delta$.

2. W liściach drzewa znajdują się aksjomaty systemu RS.

3. Dla każdego wierzchołka w drzewa, który nie jest liściem:

   (a) Jeśli rząd w jest równy jeden (czyli w ma dokładnie jednego bezpośredniego potomka), to istnieje reguła systemu RS taka, że w wierzchołku w znajduje się wniosek tej reguły, a w bezpośrednim potomku wierzchołka w znajduje się przesłanka tej reguły.

   (b) Jeśli rząd w jest równy dwa (czyli w ma dokładnie dwóch bezpośrednich potomków), to istnieje reguła systemu RS taka, że w wierzchołku w znajduje się wniosek tej reguły, a w bezpośrednich potomkach w znajdują się przesłanki tej reguły.

Jeśli sekwent $\Gamma \vdash \Delta$ ma dowód w systemie RS, to piszemy $\vdash_{RS} \Gamma \vdash \Delta$.

Możemy również mówić, że w rachunku RS dowodzimy formuł (języka KRZ lub języka KRP). Powiemy mianowicie, że formuła φ jest tezą systemu RS, gdy sekwent $\emptyset \vdash \varphi$ ma dowód w systemie RS.

5 Przykłady dowodów

Tradycja każe pisać dowody w systemie RS w postaci drzew, których korzeń znajduje się na dole, a liście na górze. Praktyka znajdowania takich dowodów polega jednak zwykle na przechodzeniu od dowodzonego sekwentu do sekwentów, z których jest on wyprowadzany, aż do zakończenia dowodu poprzez dotarcie do liści drzewa, będących aksjomatami systemu. Oczywiście nie ma zakazu, aby zaczynać budowę dowodu od aksjomatów systemu, docierając do uzasadnianej tezy. Tak jest np. w przykładzie podanym w Fitting 1990, 84:

Przykład 1: $\vdash \neg(p \wedge q) \rightarrow (\neg p \vee \neg q)$

$$
\begin{array}{c}
1.\ p \vdash p \qquad\qquad\qquad 2.\ q \vdash q \\
| \qquad\qquad\qquad\qquad | \\
3.\ p, q \vdash p \ \ LW : 1 \quad 4.\ p, q \vdash q \ \ LW : 2 \\
5.\ p, q \vdash p \wedge q \ \ R_{\wedge} : 3, 4 \\
| \\
6.\ q \vdash p \wedge q, \neg p \ \ R_{\neg} : 5 \\
| \\
7.\ \vdash p \wedge q, \neg p, \neg q \ \ R_{\neg} : 6 \\
| \\
8.\ \neg(p \wedge q) \vdash \neg p, \neg q \ \ L_{\neg} : 7 \\
| \\
9.\ \neg(p \wedge q) \vdash \neg p \vee \neg q \ \ R_{\vee} : 8 \\
| \\
10.\ \vdash \neg(p \wedge q) \rightarrow (\neg p \vee \neg q) \ \ R_{\rightarrow} : 9
\end{array}
$$

Chuck Norris potrafi każdy dowód w rachunku sekwentów RS przeprowadzić właśnie w ten sposób: raz, dwa znajduje aksjomaty potrzebne w dowodzie, a potem (z półobrotu) wdzięcznie korzysta z dostępnych reguł. Większość osób, które znam prowadzi jednak dowody w RS metodą *backward proof search*: zaczynamy od dowodzonego segmentu (w korzeniu drzewa) i dla każdego kolejnego wierzchołka w budowanym dowodzie wybieramy w nim formułę główną oraz tworzymy bezpośredniego potomka lub dwóch bezpośrednich potomków, z odpowiednimi formułami aktywnymi. Kontynuujemy to postępowanie tak długo, aż na każdej gałęzi tworzonego drzewa znajdzie się aksjomat rachunku RS. Oczywiście, jeśli w korzeniu drzewa znajduje się sekwent, który nie posiada dowodu, to w drzewie znajdzie się co najmniej jedna gałąź, której nie uda się zakończyć aksjomatem systemu RS.

Kilka dalszych prostych przykładów (z użyciem powyższego sposobu zapisywania dowodów):

Przykład 2: $\vdash p \rightarrow (q \rightarrow p)$

1.	$p \vdash p$	aksjomat
2.	$q, p \vdash p$	$LW : 1$
3.	$p \vdash q \rightarrow p$	$R_{\rightarrow} : 2$
4.	$\vdash p \rightarrow (q \rightarrow p)$	$R_{\rightarrow} : 3$

Przykład 3: $\vdash (p \wedge q) \rightarrow p$

1.	$p \vdash p$	aksjomat
2.	$p, q \vdash p$	$LW : 1$
3.	$p \wedge q \vdash p$	$L_{\wedge} : 2$
4.	$\vdash (p \wedge q) \rightarrow p$	$R_{\rightarrow} : 3$

Przykład 4: $\vdash p \rightarrow (p \vee q)$

1.	$p \vdash p$	aksjomat
2.	$p \vdash p, q$	$RW : 1$
3.	$p \vdash p \vee q$	$R_{\vee} : 2$
4.	$\vdash p \rightarrow (p \vee q)$	$R_{\rightarrow} : 3$

Przykład 5: $\vdash \neg\neg p \rightarrow p$

1.	$p \vdash p$	aksjomat
2.	$\vdash p, \neg p$	$R_{\neg} : 1$
3.	$\neg\neg p \vdash p$	$L_{\neg} : 2$
4.	$\vdash \neg\neg p \rightarrow p$	$R_{\rightarrow} : 3$

Kilka bardziej złożonych przykładów (aksjomat, jaki jest, każdy widzi, więc opuszczamy komentarze dotyczące aksjomatów):

Przykład 6

1. $p \vdash p$	2. $q \vdash q$
3. $p, \neg q \vdash p$ $LW1$	4. $q \vdash \neg p, q$ $RW2$
5. $\neg q \vdash \neg p, p$ $R_{\neg}3$	6. $q, \neg q \vdash \neg p$ $L_{\neg}4$

7. $\neg q, p \rightarrow q \vdash \neg p$ $L_{\rightarrow}5, 6$
8. $p \rightarrow q \vdash \neg q \rightarrow \neg p$ $R_{\rightarrow}7$
9. $\vdash (p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$ $R_{\rightarrow}8$

Przykład 7

Pomijamy tym razem numery sekwentów (z lewej) oraz informację o użytych regułach (z prawej). Słuchacze zechcą dokonać stosownych uzupełnień samodzielnie. Jak pamiętamy z poprzednich wykładów, tego typu informacje nie są częścią samego dowodu, a jedynie komentarzami ułatwiającymi jego czytanie.

$$
\begin{array}{cccc}
 & & p \vdash p & q \vdash q \\
 & & | & | \\
 & p \vdash p & p \vdash q, p & q, p \vdash q \\
 & | & \diagdown & \diagup \\
 & p \vdash q, p & \multicolumn{2}{c}{p \to q, p \vdash q} \\
 & \diagdown & \diagup & \\
\multicolumn{4}{c}{p, p \to (p \to q) \vdash q} \\
\multicolumn{4}{c}{|} \\
\multicolumn{4}{c}{p \to (p \to q) \vdash p \to q} \\
\multicolumn{4}{c}{|} \\
\multicolumn{4}{c}{\vdash (p \to (p \to q)) \to (p \to q)}
\end{array}
$$

Przykład 8

Oto dowód prawa sylogizmu hipotetycznego w RS:

$$\begin{array}{cccc}
\varphi \vdash \varphi & \psi \vdash \psi & \varphi \vdash \varphi & \chi \vdash \chi \\
| & | & | & | \\
\varphi \vdash \psi, \varphi & \psi \vdash \chi, \psi & \varphi \vdash \chi, \varphi & \chi, \varphi \vdash \chi \\
| & | & | & | \\
\varphi \vdash \chi, \psi, \varphi & \psi, \varphi \vdash \chi, \psi & \chi, \varphi \vdash \chi, \varphi & \psi, \chi, \varphi \vdash \chi
\end{array}$$

$$\begin{array}{cc}
\varphi, \varphi \to \psi \vdash \chi, \psi & \chi, \varphi, \varphi \to \psi \vdash \chi
\end{array}$$

$$\begin{array}{c}
\varphi, \psi \to \chi, \varphi \to \psi \vdash \chi \\
| \\
\psi \to \chi, \varphi \to \psi \vdash \varphi \to \chi \\
| \\
\varphi \to \psi \vdash (\psi \to \chi) \to (\varphi \to \chi) \\
| \\
\vdash (\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi))
\end{array}$$

W powyższych przykładach nie zaznaczono korzystania z reguł przestawiania (zaczynają one być istotne, gdy pracujemy nie na zbiorach, lecz na ciągach formuł). Czasami stosuje się też inne jeszcze uproszczenie: jeśli w poprzedniku i następniku segmentu występuje ta sama formuła, powiedzmy φ, to uznaje się, że taki sekwent wyprowadzić można z aksjomatu $\varphi \vdash \varphi$ (poprzez, być może wielokrotne, stosowanie reguł osłabiania).

Przykład 9: $\vdash p \vee \neg p$

$$\begin{array}{c}
p \vdash p \\
| \\
\vdash p, \neg p \\
| \\
\vdash p, p \vee \neg p \\
| \\
\vdash p \vee \neg p, p \vee \neg p \\
| \\
\vdash p \vee \neg p
\end{array}$$

Przykład 10: $\vdash (p \to q) \vee (q \to p)$

$$
\begin{array}{c}
q \vdash q \\
| \\
q \vdash p, q \\
| \\
p, q \vdash p, q \\
| \\
q \vdash p \to q, p \\
| \\
\vdash p \to q, q \to p \\
| \\
\vdash p \to q, (p \to q) \lor (q \to p) \\
| \\
\vdash (p \to q) \lor (q \to p), (p \to q) \lor (q \to p) \\
| \\
\vdash (p \to q) \lor (q \to p)
\end{array}
$$

Przykład 11: $\vdash (((p \to q) \to q) \to q) \to (p \to q)$

$$
\begin{array}{c}
p \vdash p \quad q \vdash q \\
\diagdown\diagup \\
p, p \to q \vdash q \\
| \\
p \vdash (p \to q) \to q \quad q \vdash q \\
\diagdown\diagup \\
p, ((p \to q) \to q) \to q \vdash q \\
| \\
((p \to q) \to q) \to q \vdash p \to q \\
| \\
\vdash (((p \to q) \to q) \to q) \to (p \to q)
\end{array}
$$

Przykład 12: $\vdash ((\varphi \to \perp) \to \perp) \to \varphi$

$$
\begin{array}{c}
\begin{array}{cc}
\begin{array}{c} \varphi \vdash \varphi \\ | \\ \varphi \vdash \bot, \varphi \\ | \\ \vdash \varphi \to \bot, \varphi \end{array} & \bot \vdash \varphi
\end{array} \\
\diagdown \quad \diagup \\
(\varphi \to \bot) \to \bot \vdash \varphi \\
| \\
\vdash ((\varphi \to \bot) \to \bot) \to \varphi
\end{array}
$$

Przykład 13: $\exists y \forall x P(x, y) \to \forall x \exists y P(x, y)$

W tym przykładzie ponumerujemy kroki dowodowe (z lewej strony) oraz podamy (z prawej strony) komentarze dotyczące ich prawomocności:

1.	$P(a, b) \vdash P(a, b)$	aksjomat
2.	$\forall x P(x, b) \vdash P(a, b)$	$L\forall$: 1
3.	$\forall x P(x, b) \vdash \exists y P(a, y)$	$R\exists$: 2
4.	$\exists y \forall x P(x, y) \vdash \exists y P(a, y)$	$L\exists$: 3
5.	$\vdash \exists y \forall x P(x, y) \to \forall x \exists y P(x, y)$	$R\forall$: 4

Przykład 14: $\vdash \neg \exists x P(x) \to \forall x \neg P(x)$

$$
\begin{array}{c}
P(a) \vdash P(a) \\
| \\
P(a) \vdash \exists x P(x) \\
| \\
\neg \exists x P(x), P(a) \vdash \\
| \\
\neg \exists x P(x) \vdash \neg P(a) \\
| \\
\neg \exists x P(x) \vdash \forall \neg P(x) \\
| \\
\vdash \neg \exists x P(x) \to \forall x \neg P(x)
\end{array}
$$

Przykład 15: $\vdash (\exists x P(x) \vee \exists x Q(x)) \to \exists x (P(x) \vee Q(x))$

$$
\begin{array}{cc}
P(a) \vdash P(a) & Q(a) \vdash Q(a) \\
| & | \\
P(a) \vdash \exists x P(x) & Q(a) \vdash \exists x Q(x) \\
| & | \\
P(a) \vdash \exists x P(x) \vee \exists x Q(x) & Q(a) \vdash \exists x P(x) \vee \exists x Q(x)
\end{array}
$$

$$
\begin{array}{c}
P(a) \vee Q(a) \vdash \exists x P(x) \vee \exists x Q(x) \\
| \\
\exists x (P(x) \vee Q(x)) \vdash \exists x P(x) \vee \exists x Q(x) \\
| \\
\vdash \exists (P(x) \vee Q(x)) \rightarrow (\exists x P(x) \vee \exists x Q(x))
\end{array}
$$

Ćwiczenia. Podaj dowody sekwentów:

1. $\vdash (p \rightarrow q) \rightarrow ((p \rightarrow r) \rightarrow (p \rightarrow (q \wedge r)))$
2. $\vdash (p \rightarrow q) \rightarrow ((q \rightarrow r) \rightarrow ((p \vee q) \rightarrow r))$
3. $\vdash \forall x \neg P(x) \rightarrow \exists x \neg P(x)$
4. $\vdash (\exists x P(x) \vee \exists x Q(x)) \rightarrow \exists x (P(x) \vee Q(x))$

6 Fakty metalogiczne

6.1 Trafność i pełność systemu RS

Zauważmy, że reguły logiczne dla spójników prawdziwościowych mają następujące własności (semantyczne):

1. Jeśli $\Gamma \vdash \Delta$ jest aksjomatem systemu RS, to $v(\Gamma \vdash \Delta) = 1$ dla dowolnego wartościowania v.
2. Jeśli przesłanka reguły: $(L\wedge)$, $(R\vee)$, $(R \rightarrow)$, $(L\neg)$, $(R\neg)$ ma wartość 1 przy wartościowaniu v, to wniosek tej reguły także ma wartość 1 przy wartościowaniu v.
3. Jeśli obie przesłanki reguły: $(R\wedge)$, $(L\vee)$, $(L \rightarrow)$ mają wartość 1 przy wartościowaniu v, to wniosek tej reguły także ma wartość 1 przy wartościowaniu v.
4. Jeśli wniosek reguły: $(L\wedge)$, $(R\vee)$, $(R \rightarrow)$, $(L\neg)$, $(R\neg)$, ma wartość 1 przy wartościowaniu v to także przesłanka tej reguły ma wartość 1 przy wartościowaniu v.

5. Jeśli wniosek reguły: $(R\wedge)$, $(L\vee)$, $(L\to)$, ma wartość 1 przy wartościowaniu v to także obie przesłanki tej reguły mają wartość 1 przy wartościowaniu v.

Pierwsze dwie z tych własności dotyczą trafności reguł rachunku RS, pozostałe dwie mówią o odwracalności tych reguł.

Trafność systemu RS (dla KRZ) jest oczywista: aksjomaty są tautologiami KRZ (jeśli $\varphi \vdash \varphi$ jest aksjomatem systemu RS, to oczywiście $\varphi \to \varphi$ jest tautologią KRZ). Ponadto, jeśli przesłanki reguły rachunku RS są tautologiami KRZ, to i wniosek tej reguły jest tautologią KRZ.

Pełność rachunku RS udowodnić można na różne sposoby. W podręczniku Fitting 1990 zaleca się oczywiście dowód poprzez wykorzystanie Twierdzenia o Istnieniu Modelu.

Wprowadźmy użyteczny skrót: $\neg S = \{\neg\varphi \ : \ \varphi \in S\}$.

Jeśli S jest skończonym zbiorem formuł, to *sekwentem stowarzyszonym z* S nazwiemy dowolny sekwent $\Gamma \vdash \neg\Delta$, gdzie para (Γ, Δ) jest podziałem S, czyli: $\Gamma \cap \Delta = \emptyset$ oraz $\Gamma \cup \Delta = S$.

Fakt. Jeśli (dowolny) sekwent stowarzyszony z S ma dowód w systemie RS, to każdy sekwent stowarzyszony z S ma dowód w systemie RS.

Powiemy, że skończony zbiór formuł S jest *sekwentowo sprzeczny*, gdy dowolny (a w konsekwencji, każdy) sekwent stowarzyszony z S ma dowód w RS. Powiemy, że skończony zbiór formuł S jest *sekwentowo niesprzeczny*, gdy nie jest on sekwentowo sprzeczny.

Fakt. Rodzina wszystkich zbiorów sekwentowo niesprzecznych jest zdaniową własnością niesprzeczności.

Fakt. Zachodzą następujące implikacje:

1. Jeśli sekwent $\Gamma \vdash \Delta, \neg\varphi$ ma dowód w systemie RS, to sekwent $\Gamma, \varphi \vdash \Delta$ również ma dowód w systemie RS.

2. Jeśli sekwent $\Gamma, \neg\varphi \vdash \Delta$ ma dowód w systemie RS, to sekwent $\Gamma \vdash \Delta, \varphi$ również ma dowód w systemie RS.

Na mocy powyższych faktów (których dowodami można pobawić się na konwersatorium, jeśli słuchaczy najdzie na to ochota) otrzymujemy:

Twierdzenie o Pełności Systemu RS dla KRZ. Jeśli φ jest tautologią KRZ, to φ jest tezą systemu RS (czyli: $\vdash_{RS} \vdash \varphi$).

Dowód. Przypuśćmy, że φ nie jest tezą systemu RS. Wtedy sekwent $\emptyset \vdash \varphi$ nie ma dowodu w RS. Oznacza to, że zbiór $\{\neg\varphi\}$ jest sekwentowo niesprzeczny, gdyż w przeciwnym przypadku dowód posiadałby sekwent $\neg\varphi \vdash \emptyset$, a zatem dowód posiadałby również sekwent $\emptyset \vdash \varphi$. Na mocy Twierdzenia o Istnieniu Modelu zbiór $\{\neg\varphi\}$ jest spełnialny, a zatem φ nie jest tautologią KRZ.

6.2 Reguła cięcia

Regułą cięcia (*cut rule*) nazywamy regułę o następującej postaci:

$$\frac{\Gamma \vdash \Delta, \varphi \qquad \varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}$$

W szczególności, jeśli $\Delta = \{\psi\}$, to reguła cięcia przybiera postać:

$$\frac{\Gamma \vdash \psi, \varphi \qquad \varphi, \Gamma \vdash \psi}{\Gamma \vdash \psi}$$

Reguła ta odpowiada zatem następującej procedurze dowodowej:

1. Przypuśćmy, że z jakichś założeń Γ otrzymujemy lemat φ oraz tezę ψ.
2. Przypuśćmy także, że z lematu φ oraz założeń Γ otrzymać możemy tezę ψ.
3. Na mocy reguły cięcia możemy wtedy uzyskać z założeń Γ tezę ψ.

Reguła cięcia występowała w oryginalnym systemie Gentzena. Pokazał on jednak, że użycia tej reguły mogą zostać w tym systemie wyeliminowane:

Hauptsatz. Każdy dowód sekwentu $\Gamma \vdash \Delta$ (w systemie RS z regułą cięcia), w którym występuje reguła cięcia może zastać zastąpiony dowodem w systemie RS bez użycia tej reguły.

Zamiast mówić o eliminowaniu reguły cięcia, można też mówić, że reguła cięcia jest regułą dopuszczalną w systemie RS (zob. wykład drugi z materiałów na rok akademicki 2015/2016).

Słuchacze zechcą porównać regułę cięcia ze znanymi z innych technik dowodowych regułami (dla KRZ):

1. *Reguła odrywania*. $\frac{\varphi \rightarrow \psi \quad \varphi}{\psi}$
2. *Reguła rezolucji*. $\frac{\varphi \vee \psi \quad \varphi \vee \neg \psi}{\varphi}$.

Dowody, które nie zawierają użyć reguły cięcia nazywa się *analitycznymi*. Dowody analityczne zalecają się wieloma własnościami przydatnymi w automatycznym dowodzeniu twierdzeń (m.in.: odwoływanie się wyłącznie do podformuł używanych w dowodzie formuł). Jednak dowody analityczne bywają często o wiele dłuższe od dowodów, które analityczne nie są.

Zauważmy, że w przesłankach reguły cięcia występuje formuła (o dowolnej złożoności), która nie występuje we wniosku tej reguły.

Każdy dowód w systemie RS można dość łatwo przekształcić na dowód w systemie aksjomatycznym w stylu Hilberta. Aby pokazać, że jest również na odwrót, czyli że każdy dowód w systemie aksjomatycznym w stylu Hilberta można przekształcić na dowód w systemie RS, trzeba odpowiednio „zadbać" o regułę odrywania. Do tego właśnie służy dołączenie reguły cięcia do systemu RS. Następnie korzystamy oczywiście z twierdzenia o eliminacji reguły cięcia.

6.3 Konsekwencje twierdzenia o eliminacji cięcia

Twierdzenie to ma liczne zastosowania w teorii dowodu. Wymienimy, przykładowo, dwa:

1. *Dowody niesprzeczności*.
2. *Automatyczne dowodzenie twierdzeń*.

7 Wykorzystywana literatura

Fitting, M. 1996. *First-Order Logic and Automated Theorem Proving*. Springer, Berlin.

Gentzen, G. 1935. Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift* **39**, 176–210, 405–431.

Negri, S., von Plato, J. 2001. *Structural Proof Theory*. Cambridge University Press, Cambridge.

Rasiowa, H., Sikorski, R. 1963. *The Mathematics of Metamathematics.* Państwowe Wydawnictwo Naukowe, Warszawa.

Pogorzelski, W.A. 1981. *Klasyczny rachunek kwantyfikatorów. Zarys teorii.* Państwowe Wydawnictwo Naukowe, Warszawa.

Smullyan, R. 1968. *First-Order Logic.* Springer Verlag, Berlin.

Troelstra, A.S., Schwichtenberg, H. 2000. *Basic Proof Theory*. Cambridge University Press, Cambridge.

JERZY POGONOWSKI
Zakład Logiki i Kognitywistyki UAM
www.kognitywistyka.amu.edu.pl
http://logic.amu.edu.pl/index.php/Dydaktyka
pogon@amu.edu.pl