METODY DOWODZENIA TWIERDZEŃ I AUTOMATYZACJA ROZUMOWAŃ
KONWERSATORIUM 2: PRELIMINARIA LOGICZNE

V rok kognitywistyki UAM

1 Indukcja strukturalna, operacje konsekwencji

1. Proste przykłady: drzewa syntaktyczne formuł, obliczanie stopnia i rangi, przekład z notacji infiksowej na prefiksową (i na odwrót). Studenci podzieleni na grupy, nawzajem zadają sobie pytania.
2. Udowodnić, że dla dowolnej formuły ψ języka KRZ liczba wystąpień funktorów dwuargumentowych w ψ jest równa liczbie wystąpień lewych nawiasów w ψ (rozwiązanie: np. w materiałach dydaktycznych Pani dr Doroty Leszczyńskiej-Jasion).
3. Udowodnić własności 1-10 ze slajdu 20, wykład 2.

2 Zdaniowe własności niesprzeczności

Niech $\mathcal{C}$ będzie rodziną zbiorów formuł języka KRZ.Mówimy, że $\mathcal{C}$ *zdaniową własnością niesprzeczności* (*propositional consistency property*), jeśli dla każdego zbioru $S \in \mathcal{C}$:

1. Dla każdej zmiennej zdaniowej p: albo $p \notin S$ albo $\neg p \notin S$
2. $\bot \notin S$ oraz $\neg\top \notin S$
3. Jeśli $\neg\neg\psi \in S$, to $S \cup \{\psi\} \in S$
4. Jeśli $\alpha \in S$, to $S \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$
5. Jeśli $\beta \in S$, to $S \cup \{\beta_1\} \in \mathcal{C}$ lub $S \cup \{\beta_2\} \in \mathcal{C}$.

- Własność niesprzeczności $\mathcal{C}$ jest *domknięta na podzbiory*, gdy dla każdego $S \in \mathcal{C}$ oraz wszystkich $T \subseteq S$: $T \in \mathcal{C}$.

- Własność niesprzeczności $\mathcal{C}$ jest *charakteru skończonego*, gdy: $S \in \mathcal{C}$ wtedy i tylko wtedy, gdy każdy skończony podzbiór zbioru S należy do $\mathcal{C}$.

Studenci udowodnią teraz następujące twierdzenia:

1. Każda własność niesprzeczności może zostać rozszerzona do własności niesprzeczności domkniętej na podzbiory.
2. Każda własność niesprzeczności charakteru skończonego jest domknięta na podzbiory.
3. Każda własność niesprzeczności domknięta na podzbiory może zostać rozszerzona do własności niesprzeczności charakteru skończonego.

Ponadto, udowodnimy następujący (zabawny) fakt. Niech P będzie dowolną własnością zbiorów. Określamy własność $P^{\#}$ następująco: $P^{\#}(S)$ wtedy i tylko wtedy, gdy $P(T)$ dla wszystkich skończonych zbiorów $T \subseteq S$. Mamy wtedy: $P^{\#}(S)$ wtedy i tylko wtedy, gdy $P^{\#}(T)$ dla każdego skończonego zbioru $T \subseteq S$.

2.1 Dowód własności 1

Niech $\mathcal{C}$ będzie zdaniową własnością niesprzeczności. Zdefiniujmy:

$$\mathcal{C}^* = \{T : \exists S \in \mathcal{C} \ \ (T \subseteq S)\}.$$

Pokażemy, że $\mathcal{C}^*$ jest zdaniową własnością niesprzeczności.

Pierwsze dwa warunki definicji zdaniowej własności niesprzeczności są spełnione dla $\mathcal{C}^*$.

Załóżmy, że $T \in \mathcal{C}^*$ oraz $\neg\neg\psi \in T$. Wtedy istnieje $S_0 \in \mathcal{C}$ taki, że $T \subseteq S_0$. Przypuśćmy, że $T \cup \{\psi\} \notin \mathcal{C}^*$. Skoro $T \cup \{\psi\} \notin \mathcal{C}^*$, to nie istnieje $S \in \mathcal{C}$ taki, że $T \cup \{\psi\} \subseteq S$. Jednak $\neg\neg\psi \in S_0$ oraz $S_0 \in \mathcal{C}$, więc $S_0 \cup \{\psi\} \in \mathcal{C}$. Oczywiście $T \cup \{\psi\} \subseteq S_0 \cup \{\psi\}$. Otrzymujemy sprzeczność, a zatem $T \cup \{\psi\} \in \mathcal{C}^*$.

Załóżmy, że $T \in \mathcal{C}^*$ oraz $\alpha \in T$. Wtedy istnieje $S_0 \in \mathcal{C}$ taki, że $T \subseteq S_0$. Przypuśćmy, że $T \cup \{\alpha_1, \alpha_2\} \notin \mathcal{C}^*$. Oznacza to, że nie istnieje $S \in \mathcal{C}$ taki, że $T \cup \{\alpha_1, \alpha_2\} \subseteq S$. Jednak $\alpha \in S_0$ oraz $S_0 \in \mathcal{C}$, a zatem $S_0 \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$. Oczywiście $T \cup \{\alpha_1, \alpha_2\} \subseteq S_0 \cup \{\alpha_1, \alpha_2\}$. Otrzymujemy sprzeczność, a więc $T \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}^*$.

Załóżmy, że $T \in \mathcal{C}^*$ oraz $\beta \in T$. Wtedy istnieje $S_0 \in \mathcal{C}$ taki, że $T \subseteq S_0$. Przypuśćmy, że: $T \cup \{\beta_1\} \notin \mathcal{C}^*$ oraz $T \cup \{\beta_2\} \notin \mathcal{C}^*$. Oznacza to, że nie istnieją $S_1 \in \mathcal{C}$ oraz $S_2 \in \mathcal{C}$ takie, że: $T \cup \{\beta_1\} \subseteq S_1$ oraz $T \cup \{\beta_2\} \subseteq S_2$. Ponieważ $\beta \in T \subseteq S_0$, więc $\beta \in S_0$. Skoro $S_0 \in \mathcal{C}$ oraz $\beta \in S_0$, to: $S_0 \cup \{\beta_1\} \in \mathcal{C}$ lub

$S_0 \cup \{\beta_2\} \in \mathcal{C}$. Oczywiście $T \cup \{\beta_1\} \subseteq S_0 \cup \{\beta_1\}$ oraz $T \cup \{\beta_2\} \subseteq S_0 \cup \{\beta_2\}$. Otrzymujemy sprzeczność, a zatem $T \cup \{\beta_1\} \in \mathcal{C}^*$ lub $T \cup \{\beta_2\} \in \mathcal{C}^*$.

Pokazaliśmy, że $\mathcal{C}^*$ jest zdaniową własnością niesprzeczności. Z definicji, jest ona domknięta na podzbiory. Oczywiście $\mathcal{C} \subseteq \mathcal{C}^*$.

2.2 Dowód własności 2

Niech $\mathcal{C}$ będzie zdaniową własnością niesprzeczności charakteru skończonego. To oznacza, że $S \in \mathcal{C}$ wtedy i tylko wtedy, gdy $T \in \mathcal{C}$ dla wszystkich skończonych podzbiorów zbioru S. Pokażemy, że $\mathcal{C}$ jest domknięta na podzbiory.

Przeprowadzimy dowód nie wprost: przypuśćmy, że $\mathcal{C}$ nie jest domknięta na podzbiory. Wtedy istnieją: $S \in \mathcal{C}$ oraz $T \subseteq S$ takie, że $T \notin \mathcal{C}$. Oznacza to, że T nie spełnia któregoś z warunków definiujących zdaniową własność niesprzeczności. Wprost z definicji widać, że nie mogą to być warunki dotyczące: zmiennych zdaniowych, $\bot$ oraz $\neg\top$.

Rozważyć trzeba zatem pozostałe przypadki:

1. Istnieje ψ taka, że $\neg\neg\psi \in T$ oraz $T \cup \{\psi\} \notin \mathcal{C}$.
2. Istnieje α taka, że $\alpha \in T$ oraz $T \cup \{\alpha_1, \alpha_2\} \notin \mathcal{C}$
3. Istnieje β taka, że $\beta \in T$ oraz $T \cup \{\beta_1\} \notin \mathcal{C}$ i $T \cup \{\beta_2\} \notin \mathcal{C}$.

Przypadek 1. Jeśli istnieje ψ taka, że $\neg\neg\psi \in T$ oraz $T \cup \{\psi\} \notin \mathcal{C}$, to (ponieważ $\mathcal{C}$ jest charakteru skończonego) istnieje skończony zbiór $U \subseteq T \cup \{\psi\}$ taki, że $U \notin \mathcal{C}$. Jednak U jest skończonym podzbiorem $S \cup \{\psi\}$ i z założenia $S \cup \{\psi\} \in \mathcal{C}$. Na mocy definicji $\mathcal{C}$ mamy więc $U \in \mathcal{C}$, czyli sprzeczność. A zatem $T \cup \{\psi\} \in \mathcal{C}$.

Przypadek 2. Przypuśćmy, że istnieje α taka, że $\alpha \in T$ oraz $T \cup \{\alpha_1, \alpha_2\} \notin \mathcal{C}$. Z założenia $\alpha \in S$, a więc $S \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$. Skoro $T \cup \{\alpha_1, \alpha_2\} \notin \mathcal{C}$, to istnieje skończony zbiór U taki, że $U \subseteq T \cup \{\alpha_1, \alpha_2\}$ oraz $U \notin \mathcal{C}$. Jednak wtedy $U \subseteq S \cup \{\alpha_1, \alpha_2\}$ oraz $S \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$, a więc $U \in \mathcal{C}$ i otrzymujemy sprzeczność. A zatem $T \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$.

Przypadek 3. Przypuśćmy, że istnieje β taka, że $\beta \in T$ oraz: $T \cup \{\beta_1\} \notin \mathcal{C}$ i $T \cup \{\beta_2\} \notin \mathcal{C}$. Istnieją zatem skończone zbiory U_1, U_2 takie, że:

$U_1 \subseteq T \cup \{\beta_1\}$ oraz $U_1 \notin \mathcal{C}$

$U_2 \subseteq T \cup \{\beta_2\}$ oraz $U_2 \notin \mathcal{C}$.

Jednak $U_1 \subseteq S \cup \{\beta_1\}$ oraz $U_2 \subseteq S \cup \{\beta_2\}$, a ponieważ $\mathcal{C}$ jest charakteru skończonego, więc $U_1 \in \mathcal{C}$ oraz $U_2 \in \mathcal{C}$ i otrzymujemy sprzeczność. A zatem $T \cup \{\beta_1\} \in \mathcal{C}$ lub $T \cup \{\beta_2\} \in \mathcal{C}$.

2.3 Dowód własności 3

Niech $\mathcal{C}$ będzie zdaniową własnością niesprzeczności domkniętą na podzbiory. Pokażemy, że $\mathcal{C}$ może zostać rozszerzona do własności niesprzeczności charakteru skończonego. Zdefiniujmy: $\mathcal{C}^* = \{S : \forall T \subseteq S : (\text{jeśli } T \text{ skończony, to } T \in \mathcal{C})\}$.

Pokażemy, że $\mathcal{C}^*$ jest własnością niesprzeczności charakteru skończonego, czyli że $S \in \mathcal{C}^*$ wtedy i tylko wtedy, gdy $T \in \mathcal{C}^*$ dla wszystkich skończonych $T \subseteq S$. Przeprowadzimy dowód nie wprost.

Jak poprzednio, warunki dotyczące zmiennych zdaniowych oraz $\perp$ oraz $\neg\top$ nie sprawiają żadnego kłopotu. Trzeba zająć się pozostałymi warunkami.

Przypadek 1. Załóżmy, że $S \in \mathcal{C}^*$ oraz $\neg\neg\psi \in S$. Wtedy dla wszystkich skończonych $T \subseteq S$ mamy: $T \in \mathcal{C}$. Przypuśćmy, że $S \cup \{\psi\} \notin \mathcal{C}^*$. Wtedy istnieje skończony zbiór $T_0 \subseteq S \cup \{\psi\}$ taki, że $T_0 \notin \mathcal{C}$. Jeśli $\psi \in T_0$, to $T_0 \subseteq S$, a więc, na mocy definicji $\mathcal{C}^*$ mamy $T_0 \in \mathcal{C}$, sprzeczność. Jeśli $\psi \notin T_0$, to $T_0 = S$, czyli S jest skończony. Ponieważ $\neg\neg\psi \in S$, więc wynika z tego, że $T_0 \cup \{\psi\} = S \cup \{\psi\} \in \mathcal{C}$, sprzeczność. Ostatecznie, $S \cup \{\psi\} \in \mathcal{C}^*$.

Przypadek 2. Załóżmy, że $S \in \mathcal{C}^*$ oraz $\alpha \in S$. Wtedy $T \in \mathcal{C}$ dla wszystkich skończonych $T \subseteq S$. Przypuśćmy, że $S \cup \{\alpha_1, \alpha_2\} \notin \mathcal{C}^*$. Wtedy istnieje skończony $T_0 \subseteq S \cup \{\alpha_1, \alpha_2\}$ taki, że $T_0 \notin \mathcal{C}$. Jeśli jednak $\alpha \in T_0$, to $T_0 \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$, ponieważ T_0 jest skończonym podzbiorem S, zaś $S \in \mathcal{C}^*$. Jeśli natomiast $\alpha \notin T_0$, to $T_0 \cup \{\alpha\}$ jest skończonym podzbiorem S, a więc $T_0 \cup \{\alpha\} \in \mathcal{C}$. Z tego wynika, że $T_0 \cup \{\alpha, \alpha_1, \alpha_2\} \in \mathcal{C}$, a ponieważ $\mathcal{C}$ jest domknięta na podzbiory, więc $T_0 \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}$, sprzeczność. Ostatecznie, $S \cup \{\alpha_1, \alpha_2\} \in \mathcal{C}^*$.

Przypadek 3. Załóżmy, że $S \in \mathcal{C}^*$ oraz $\beta \in S$. Wtedy $T \in \mathcal{C}$ dla wszystkich skończonych $T \subseteq S$. Przypuśćmy, że $S \cup \{\beta_1\} \notin \mathcal{C}^*$ oraz $S \cup \{\beta_2\} \notin \mathcal{C}^*$. Wtedy istnieją skończone zbiory T_1 i T_2 takie, że:

$T_1 \subseteq S \cup \{\beta_1\}$ oraz $T_1 \notin \mathcal{C}$

$T_2 \subseteq S \cup \{\beta_2\}$ oraz $T_2 \notin \mathcal{C}$.

Przypominamy, że $T \in \mathcal{C}$ dla wszystkich skończonych $T \subseteq S$. Dla *dowolnego* takiego T rozważmy dwa przypadki: $\beta \in T$ oraz $\beta \notin T$. Jeśli $\beta \in T$, to: $T \cup \{\beta_1\} \in \mathcal{C}$ lub $T \cup \{\beta_2\} \in \mathcal{C}$. Sprzeczność (bo warunek taki musiałby też zachodzić dla $T = T_1$ oraz $T = T_2$). Jeśli $\beta \notin T$, to $T \cup \{\beta\}$ jest skończonym podzbiorem S, a ponieważ $S \in \mathcal{C}^*$, więc: $T \cup \{\beta_1\} \in \mathcal{C}$ lub $T \cup \{\beta_2\} \in \mathcal{C}$. Sprzeczność (bo warunek taki musiałby też zachodzić dla $T = T_1$ oraz $T = T_2$). Ostatecznie, $S \cup \{\beta_1\} \in \mathcal{C}^*$ lub $S \cup \{\beta_2\} \in \mathcal{C}^*$.

Pokazaliśmy więc, że $\mathcal{C}^*$ jest zdaniową własnością niesprzeczności. Do zakończenia dowodu własności 3 użyjemy teraz wspomnianego zabawnego faktu.

2.4 Dowód zabawnego faktu

Korzystamy z dowodu przedstawionego w książce Raymonda Smullyana *Logical Labyrinths* (rozdział 16, strona 188; tłumaczenie: JP).

> Mamy pokazać, że dla dowolnego zbioru S, S ma własność $P^{\#}$ wtedy i tylko wtedy, gdy wszystkie skończone podzbiory zbioru S mają własność $P^{\#}$.
>
> (1) Przypuśćmy, że S ma własność $P^{\#}$. Wtedy nie tylko wszystkie skończone podzbiory zbioru S mają własność $P^{\#}$, ale *wszystkie* podzbiory zbioru S muszą mieć własność $P^{\#}$. Aby to zobaczyć, niech A będzie dowolnym podzbiorem zbioru S. Wtedy każdy skończony podzbiór zbioru A jest także skończonym podzbiorem zbioru S, a więc ma własność P (ponieważ S ma własność $P^{\#}$). Tak więc, wszystkie skończone podzbiory zbioru A mają własność P, co oznacza, że A ma własność $P^{\#}$. A zatem wszystkie podzbiory zbioru S mają własność $P^{\#}$, i w szczególności, wszystkie skończone podzbiory zbioru S mają własność $P^{\#}$.
>
> (2) Na odwrót, przypuśćmy, że wszystkie skończone podzbiory zbioru S mają własność $P^{\#}$. Niech F będzie dowolnym skończonym podzbiorem zbioru S. Wtedy F ma własność $P^{\#}$, co oznacza, że wszystkie skończone podzbiory zbioru F mają własność P. Cóż, F jest skończonym podzbiorem siebie samego, a więc F ma własność P. A zatem wszystkie skończone podzbiory zbioru S mają własność P, co oznacza, że S ma własność $P^{\#}$. Tak więc, jeśli wszystkie skończone podzbiory zbioru S mają własność $P^{\#}$, to S również.
>
> Na mocy (1) i (2) S ma własność $P^{\#}$ wtedy i tylko wtedy, gdy wszystkie skończone podzbiory zbioru S mają własność $P^{\#}$, a zatem $P^{\#}$ jest *zwarta*.

Teraz zabawny fakt wykorzystać możemy w dokończeniu dowodu własności 3: wystarczy przyjąć, że $P(S)$ wtedy i tylko wtedy, gdy $S \in \mathcal{C}^*$.

3 Reguły dowodowe a pełne drzewo dwójkowe

Za monografią Kaye 2007 podamy pewną ogólną reprezentację reguł dowodowych. Pozwoli ona, jak sądzimy, oswoić się z reprezentacjami konstrukcji syntaktycznych w postaci drzew. Zacznijmy od metafory. Przypuśćmy, że D jest drzewem dwójkowym rzędu skończonego (inny termin: *skończenie generowanym*). Oglądać je można z dwóch perspektyw:

1. *Perspektywa Demona*. Widzi on całe drzewo D. Ma pełną informację o D. Uzna, że D jest *nieskończone*, gdy ma ono nieskończoną liczbę wierzchołków (lub, co na to samo wychodzi, nieskończoną liczbę krawędzi).

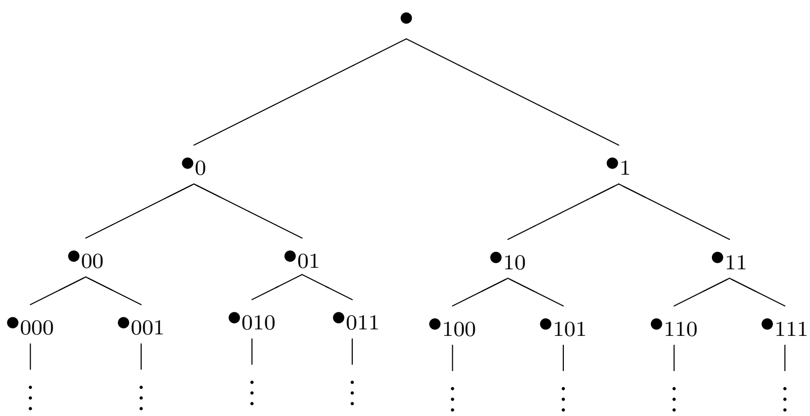
2. *Perspektywa Mrówki*. Mrówka może wędrować po drzewie D, startując z jego korzenia i dokonując wyborów (lewo-prawo) w każdym z kroków (i nie zawracając). Ma niepełną informację o D. Może osiągnąć kres swojej wędrówki, docierając do liścia. Dla Mrówki drzewo będzie *nieskończone*, jeśli da jej ono gwarancję (koszmarnej) nieśmiertelności, czyli gdy Mrówka znajdzie gałąź nieskończoną w D, po której będzie dreptać, dreptać, dreptać...

Pamiętacie Lemat Königa z pierwszego wykładu? Głosił on, że jeśli skończenie generowane (czyli rzędu skończonego) drzewo D jest nieskończone, to istnieje w nim gałąź nieskończona. Dowód nie był *konstruktywny*: dokonywaliśmy *wyboru* kolejnych elementów konstruowanej gałęzi nieskończonej, bez podania wyraźnego przepisu, który element wybieramy.

Na gruncie logiki klasycznej przez kontrapozycję Lematu Königa otrzymujemy:
TWIERDZENIE BROUWERA O WACHLARZU. Jeśli wszystkie gałęzie skończenie generowanego drzewa D są skończone, to D jest skończone.

Niektóre subtelności dotyczące Lematu Königa, Twierdzenia Brouwera o Wachlarzu, Pewnika Wyboru, Zasady Wyborów Zależnych, a nadto ich związków z metodami dowodowymi omówimy w wykładzie *Teoria rekursji a metody dowodowe*.

Przypomnijmy (początkowy fragment) pełnego drzewa dwójkowego:



Niech 2^* oznacza zbiór wszystkich *skończonych* ciągów o wyrazach 0 lub 1. Ciąg pusty oznaczmy przez $\perp$. Elementy zbioru 2^* traktować możemy jako *słowa* (lub *zdania*) w języku o alfabecie dwuelementowym. Opiszemy teraz pewien rodzaj gier, wykorzystujących formalne reguły przekształcania ciągów symboli. Później okaże się, że omawiane w dalszych wykładach metody dowodowe są właśnie tego typu grami.

Na pierwszym wykładzie podano ogólną definicję drzewa. W matematyce używamy różnych charakterystyk pojęcia *drzewa*, w zależności od potrzeb danej dyscypliny matematycznej. Dzisiaj będziemy myśleć o drzewach jako zbiorach ciągów symboli z ustalonego alfabetu. Pojęcia: *długości* ciągu oraz *konkatenacji* ciągów są słuchaczom znane z kursu *Matematycznych podstaw kognitywistyki*. Dla ciągu σ oraz liczby naturalnej n przez $\sigma \upharpoonright n$ oznaczamy ciąg o n elementach, będący podciągiem początkowym ciągu σ. Zbiór T ciągów jest *drzewem*, jeśli dla wszystkich $\sigma \in T$ o długości n, jeśli $m < n$, to $\sigma \upharpoonright m \in T$. Drzewo jest *nieskończone*, jeśli ma nieskończenie wiele elementów. Poddrzewem drzewa T jest każdy podzbiór T, który jest drzewem. *Ścieżką* w drzewie T nazywamy każdy zbiór $P \subseteq T$ taki, że dla dowolnych $\sigma, \tau \in P$, jeśli σ ma długość n, τ ma długość m oraz $n \leqslant m$, to $\sigma = \tau \upharpoonright n$. Jeśli P jest ścieżką oraz $\sigma \in p$, to mówimy, że P *przechodzi przez* σ.

UWAGA. Proszę nie lękać się podanego niżej formalizmu. W końcu zabawa zerami i jedynkami jest niegroźna, prawda? Mrówka drepcząca po (skończenie generowanym) drzewie dwójkowym robi to dzielnie, bez trwogi. Jeśli dotrze do liścia drzewa, to może spokojnie przejść do (szczęśliwego) Niebytu. Jeśli ma pecha żyć w drzewie nieskończonym i w dodatku ma Prawdziwego Pecha, ponieważ wybrała gałąź nieskończoną, to cóż – musi hardo znosić Koszmar Nieśmiertelności. Bądźcie dzielni, co najmniej tak samo, jak Mrówka.

3.1 Syntaktyczne aspekty gry dowodowej

Gra polega na tym, że: startując od jakiegoś ustalonego zbioru ciągów $\Sigma \subseteq 2^*$ i stosując pewne operacje syntaktyczne na ciągach mamy otrzymać ustalony ciąg $\tau \in 2^*$. Zabawa może też polegać na tym, żeby pokazać, iż z punktu wyjścia Σ, stosując dozwolone reguły, nie można otrzymać ciągu określonej postaci (np. ciągu pustego $\bot$).

Reguły gry (dla ustalonego Σ) mają postać następującą:

1. *Reguły Bazowe*. Możesz zapisać dowolny ciąg $\sigma \in \Sigma$.

2. *Reguły Wydłużania*. Jeśli zapisany został ciąg σ, to można zapisać jeden lub oba z ciągów: $\sigma 0$ lub $\sigma 1$.

3. *Reguły Skracania*. Dla dowolnego ciągu σ, jeśli zapisałeś ciągi $\sigma 0$ oraz $\sigma 1$, to możesz zapisać ciąg σ.

Oto podstawowe pojęcie, którym będziemy się zajmowali:

> DEFINICJA. Niech $\Sigma \subseteq 2^*$ oraz $\tau \in 2^*$. Piszemy $\Sigma \vdash \tau$ na oznaczenie tego, że można w skończonej liczbie kroków otrzymać ciąg τ, stosując reguły gry dla Σ.

Jeśli więc $\Sigma \subseteq 2^*$, to istnieje skończona lista ciągów, której elementy tworzymy wedle reguł gry i której ostatnim elementem jest τ. Zgadłaś już, prawda? Każdą taką skończoną listę nazywać będziemy *wyprowadzeniem* τ z Σ (lub *dowodem* τ z Σ).

Przykłady:

1. $\{00, 01\} \vdash 0$
2. $\{00, 01\} \vdash 00100$
3. Czy z $\{00, 01\}$ można wyprowadzić 1?

Udowodnimy, że odpowiedź na powyższe pytanie jest negatywna. Ogólniej, jeśli $\tau \in 2^*$ oraz $\{00, 01\} \vdash \tau$, to ciąg τ musi rozpoczynać się od 1. Dowód przeprowadzimy przez indukcję względem długości dowodu.

Niech $H(n)$ oznacza, że jeśli τ ma dowód z $\{00, 01\}$, to τ musi rozpoczynać się od 0.

$H(1)$ zachodzi, bo dowody o jednym kroku muszą mieć postać użycia reguły bazowej, a oba ciągi z $\{00, 01\}$ rozpoczynają się od 0.

Załóżmy, że $H(n)$ zachodzi oraz że τ ma dowód z $\{00, 01\}$ o $n + 1$ krokach. Jeśli ostatni krok jest zastosowaniem reguły bazowej, to τ musi zaczynać się od 0. Jeśli ostatnim krokiem jest użycie reguły skracania (akceptujemy τ, ponieważ $\tau = \sigma i$ i wcześniej otrzymaliśmy σ, gdzie $i \in \{0, 1\}$), to założenie indukcyjne zachodzi dla σ, co oznacza, że σ rozpoczyna się od 0, a więc także $\tau = \sigma i$ rozpoczyna się od 0. Jeśli ostatnim krokiem jest użycie reguły wydłużania (akceptujemy τ, ponieważ otrzymaliśmy wcześniej $\tau 0$ oraz $\tau 1$), to, ponieważ $\tau 0$ oraz $\tau 1$ mają dowody o co najwyżej n krokach, więc zachodzi dla nich założenie indukcyjne. Wtedy oczywiście również τ rozpoczyna się od 0.

Nieskończone zbiory Σ w naszej grze nie sprawiają kłopotu, ponieważ: jeśli $\Sigma \subseteq 2^*$ oraz $\Sigma \vdash \tau$, to istnieje skończony zbiór $\Sigma_0 \subseteq \Sigma$ taki, że $\Sigma_0 \vdash \tau$ (widzisz dlaczego tak jest?). Oczywiście ten zbiór zależy od τ.

O grach tego typu udowodnić można wiele twierdzeń, które uzyskują potem interpretacje w przypadku konkretnych metod dowodowych. Dla przykładu:

1. Załóżmy, że $\Sigma \subseteq 2^*$ jest skończony oraz $\Sigma \vdash \tau$. Wtedy istnieje dowód τ z Σ o następującej postaci:

(a) Najpierw stosowane są reguły bazowe.

(b) Potem stosowane są (wymagane w dowodzie) reguły skracania.

(c) Na koniec stosowane są (o ile są wymagane) reguły wydłużania.

2. Załóżmy, że $\Sigma \subseteq 2^*$, $\sigma, \tau \in 2^*$ i zachodzą: $\Sigma \cup \{\tau 0\} \vdash \sigma$ oraz $\Sigma \cup \{\tau 1\} \vdash \sigma$. Wtedy $\Sigma \vdash \sigma$.

3. Załóżmy, że $\Sigma \subseteq 2^*$ oraz $\Sigma \vdash \perp$. Wtedy istnieje dowód $\perp$ z Σ, który korzysta jedynie z reguł bazowych oraz reguł skracania.

4. Załóżmy, że $\Sigma \subseteq 2^*$ oraz $\Sigma \vdash \perp$. Wtedy istnieje skończony podzbiór $\Sigma_0 \subseteq \Sigma$ oraz $n \in \mathbb{N}$ takie, że dla wszystkich ciągów $\sigma \in 2^*$ o długości n, $\Sigma_0 \vdash \sigma$, przy czym w dowodzie używane są jedynie reguły bazowe oraz reguły wydłużania.

DOWÓD 1. Przez indukcję po liczbie kroków (=długości) dowodu. Jeśli dowód ma długość 1, to oznacza to, że użyto jedynie reguły bazowej.

Przypuśćmy, że τ ma dowód długości $n+1$ i że ostatnim krokiem dowodowym było otrzymanie τ z ρ przez użycie reguły wydłużania. Z założenia indukcyjnego, ρ ma dowód opisanej w twierdzeniu postaci, gdzie ciąg ρ jest otrzymany w ostatnim kroku. Wtedy dowód τ powstaje z dowodu ρ przez zastosowanie reguły wydłużania w ostatnim kroku, a więc ma postać opisaną w twierdzeniu.

Przypuśćmy, że τ otrzymano w ostatnim kroku dowodowym z $\tau 0$ oraz $\tau 1$ poprzez użycie reguły skracania. Na mocy założenia indukcyjnego, istnieje dowód $\tau 0$ z Σ, którego kroki można podzielić na trzy grupy: B_1 (tylko reguły bazowe), B_2 (tylko reguły skracania) oraz B_3 (tylko reguły wydłużania). Podobnie, istnieje dowód $\tau 1$ z Σ, którego kroki można podzielić na trzy grupy: B_1' (tylko reguły bazowe), B_2' (tylko reguły skracania) oraz B_3' (tylko reguły wydłużania). Jeśli ostatnim krokiem w którymś z tych dowodów dla $\tau 0$ oraz $\tau 1$ jest użycie reguły wydłużania, to istnieje dowód τi z samego τ, a więc istnieje dowód τ o postaci opisanej w twierdzeniu. W przeciwnym przypadku reguły wydłużania nie są używane w dowodach $\tau 0$ oraz $\tau 1$, czyli grupy B_3 i B_3' są puste. Wtedy dowodem τ w pożądanej postaci jest dowód złożony z kroków należących kolejno do: B_1, B_1', B_2, B_2'.

DOWÓD 2. Przypuśćmy, że nie zachodzi $\Sigma \vdash \sigma$ (co zapiszemy: $\Sigma \nvdash \sigma$). Możemy uważać, że kroki dowodu σ z $\Sigma \cup \{\tau 0\}$ są uporządkowane na sposób podany w poprzednim twierdzeniu. Ponieważ $\Sigma \nvdash \sigma$, więc w w dowodzie $\Sigma \cup \{\tau 0\} \vdash \sigma$ musiał zostać użyty ciąg $\tau 0$. Rozważmy *pierwsze miejsce*, w którym został on użyty. Jeśli był on założeniem w regule skracania, to $\Sigma \vdash \tau 1$, ponieważ $\tau 1$ jest wymagany jako drugie założenie takiej reguły (a wcześniej nie korzystano z $\tau 0$). Oznacza to, że $\Sigma \vdash \sigma$, ponieważ $\Sigma \cup \{\tau 1\} \vdash \sigma$. Tak więc, $\tau 0$ nie mógł zostać użyty w regule skracania, czyli był użyty w regule wydłużania, a to oznacza, że $\tau 0$ jest podciągiem początkowym ciągu σ. Tak samo (zamieniając role 0 i 1) pokazujemy, że $\tau 1$ jest podciągiem początkowym ciągu σ. To jednak niemożliwe. Ostatecznie, $\Sigma \vdash \sigma$.

DOWÓD 3. Niech $\Sigma_0 \subseteq \Sigma$ będzie zbiorem skończonym takim, że $\Sigma_0 \vdash \perp$ (pokazaliśmy już, że taki skończony zbiór istnieje). Wtedy istnieje dowód $\perp$ z Σ_0, w którym użycia reguł wydłużania znajdują się na końcu dowodu. Jednak reguły wydłużania zwiększają długość ciągu, a ciąg $\perp$, jako pusty, ma długość zero. Tak więc, w rozważanym dowodzie nie mogą wystąpić reguły wydłużania.

DOWÓD 4. Niech $\Sigma_0 \subseteq \Sigma$ będzie zbiorem skończonym takim, że $\Sigma_0 \vdash \perp$, przy czym stosowane są tylko reguły bazowe oraz reguły skracania. Niech Σ_1 będzie zbiorem wszystkich ciągów, które udowodnić można z Σ_0 przy użyciu jedynie reguł bazowych oraz reguł skracania. Niech n będzie maksimum długości ciągów z Σ_0 i niech σ ma długość n. Wtedy oczywiście każdy ciąg z Σ_1 jest długości co najwyżej n. Mamy pokazać, że σ z jakiegoś $\tau \in \Sigma_0$ (jako pierwszego kroku derywacji) przy użyciu jedynie reguł wydłużania.

Niech $\tau \in \Sigma_1$ będzie najdłuższym ciągiem takim, że τ jest równy σ lub τ jest podciągiem początkowym σ (taki τ istnieje, bo $\perp \in \Sigma_1$). Jeśli $\tau \in \Sigma_0$, to dowód jest zakończony. W przeciwnym przypadku, τ został otrzymany z $\tau 0$ oraz $\tau 1$ poprzez regułę skracania, a więc długość τ jest mniejsza od n. Wtedy jednak $\tau 0$ lub $\tau 1$ musi być podciągiem początkowym σ, ponieważ już τ był podciągiem początkowym σ o długości mniejszej od n. To jednak przeczy maksymalności ciągu τ. Zachodzi zatem teza twierdzenia.

3.2 Gry dowodowe: aspekty semantyczne

Jak dotąd, nasza gra była zabawą ciągami znaków, pozbawionymi znaczenia. Nadamy jej teraz interpretację semantyczną, a potem pokażemy, że gra jest *trafna* i *pełna*, że zachodzi precyzyjna odpowiedniość między operacjami na symbolach, a obiektywnymi zależnościami w świecie (matematycznym).

> DEFINICJA. Niech $\Sigma \subseteq 2^*$ oraz $\sigma \in 2^*$. Piszemy $\Sigma \models \sigma$, gdy: każda nieskończona ścieżka przechodząca przez σ przechodzi też przez co najmniej jeden ciąg $\tau \in \Sigma$.

Dla uniknięcia nieporozumień, zapiszmy to w formie symbolicznej (przy założeniu, że P jest ścieżką nieskończoną):

1. $\Sigma \models \sigma \;\equiv\; \forall P(\sigma \in P \to \exists \tau(\tau \in \Sigma \wedge \tau \in P))$

2. $\Sigma \not\models \sigma \;\equiv\; \exists P(\sigma \in P \wedge \forall \tau(\tau \in \Sigma \rightarrow \tau \notin P))$

PRZYKŁADY.

1. Jeśli $\Sigma = 2^*$ oraz $\sigma \in 2^*$, to oczywiście każda ścieżka nieskończona przechodząca przez σ przechodzi przez pewien $\tau \in \Sigma$ (a mianowicie $\tau = \sigma$). Ogólniej, jeśli $\sigma \in \Sigma$, to $\Sigma \models \sigma$, dla dowolnych Σ, σ.

2. Wszystkie ścieżki nieskończone przechodzą przez $\perp$. A zatem $\Sigma \models \perp$ wtedy i tylko wtedy, gdy każda nieskończona ścieżka przechodzi przez jakiś $\tau \in \Sigma$.

Podana wyżej definicja $\Sigma \models \sigma$ może być, na pierwszy rzut oka, mało czytelna. Uzupełnijmy ją kilkoma intuicyjnymi uwagami.

Można na wiele różnych sposobów reprezentować semantykę gry. Niech p_0, p_1, p_2, p_3, ... będzie nieskończoną listą zmiennych zdaniowych, którym nadawać możemy wartości 0 lub 1 (możesz o tych wartościach myśleć jako o *fałszu* i *prawdzie*, a o owych zmiennych, że opisują jakieś sytuacje). Każdy ciąg $\sigma = s_0 s_1 s_2 \ldots s_{k-1} \in 2^*$ reprezentuje sytuację, w której s_i jest wartością zmiennej p_i dla $i < k$ oraz nieznanych wartościach zmiennych p_i dla $i \geqslant k$. Myślmy o takiej sytuacji jako *niemożliwej*: sytuację opisaną takimi zmiennymi p_i $(i < k)$ uważamy (z jakichś powodów) za niemożliwą, niezależnie od tego, jakie wartości mają p_i dla $i \geqslant k$. Wtedy Σ reprezentuje zbiór sytuacji, z których każda jest niemożliwa. Zauważmy, że jeśli $\sigma = s_0 s_1 s_2 \ldots s_{k-1} \in 2^*$ reprezentuje sytuację niemożliwą, to $\sigma 0$ oraz $\sigma 1$ też reprezentują sytuacje niemożliwe. To stanowi rozsądne uzasadnienie dla reguły wydłużania. Jeśli $s_0 s_1 s_2 \ldots s_{k-1} 0$ oraz $s_0 s_1 s_2 \ldots s_{k-1} 1$ oba reprezentują sytuacje niemożliwe, to $s_0 s_1 s_2 \ldots s_{k-1}$ też reprezentuje sytuację niemożliwą, z oczywistych powodów (są tylko dwie wartości dla p_k). To z kolei stanowi rozsądne uzasadnienie dla reguły skracania.

Niech teraz Σ reprezentuje wszystkie sytuacje niemożliwe (dla problemu, który badamy). Jakaś sytuacja jest *możliwa*, gdy jest opisana przez przypisanie konkretnej wartości do każdej zmiennej p_i oraz żaden skończony ciąg takich wartości nie należy do Σ. Tak więc, sytuacja jest możliwa, gdy opisana jest przez nieskończoną ścieżkę, która nie przechodzi przez żaden element zbioru Σ.

A zatem w tej interpretacji $\Sigma \models \sigma$ oznacza, że jeśli każdy element $\tau \in \Sigma$ reprezentuje sytuację niemożliwą, to również σ reprezentuje sytuację niemożliwą. A kiedy $\Sigma \not\models \sigma$? Dokładnie wtedy, gdy istnieje nieskończona ścieżka przechodząca przez σ, która nie przechodzi przez żaden element $\tau \in \Sigma$: ścieżka taka podaje zatem przykład wartościowania, przy którym sytuacja reprezentowana przez σ jest niemożliwa, a wszystkie sytuacje reprezentowane przez elementy zbioru Σ nie są niemożliwe.

TWIERDZENIE O TRAFNOŚCI. Niech $\Sigma \subseteq 2^*$ oraz $\sigma \in 2^*$. Jeśli $\Sigma \vdash \sigma$, to $\Sigma \models \sigma$.

DOWÓD. Przeprowadzimy dowód przez indukcję po długości wyprowadzeń σ. Niech $H(n)$ oznacza, że jeśli $\Sigma \vdash \sigma$, przy czym dowód σ z Σ ma co najwyżej n kroków, to $\Sigma \models \sigma$.

Widać, że zachodzi $H(1)$, ponieważ jeśli $\sigma \in \Sigma$, to $\Sigma \models \sigma$.

Przypuśćmy, że $\Sigma \vdash \sigma$ i że dowód σ z Σ ma $n+1$ kroków, przy czym ostatni z nich polega na użyciu reguły wydłużania, a więc $\sigma = \tau i$, gdzie τ wyprowadzono w co najwyżej n krokach oraz $i \in \{0,1\}$. Dalej, przypuśćmy, że $P \subseteq 2^* - \Sigma$ jest ścieżką nieskończoną przechodzącą przez σ. Wtedy P musi przechodzić także przez τ, ponieważ długość τ jest o jeden mniejsza od długości σ, a więc na mocy założenia indukcyjnego $H(n)$, ścieżka P przechodzi przez jakiś element zbioru Σ.

Przypuśćmy, że $\Sigma \vdash \sigma$ i że dowód σ z Σ ma $n+1$ kroków, przy czym ostatni z nich polega na użyciu reguły skracania, a więc $\sigma 0$ oraz $\sigma 1$ mają dowody o długości co najwyżej n. Niech P będzie nieskończoną ścieżką przechodzącą przez σ. Wtedy P musi przechodzić przez $\sigma 0$ lub $\sigma 1$, a więc na mocy założenia indukcyjnego $H(n)$, ścieżka P przechodzi przez jakiś element zbioru Σ.

Zanim sformułujemy twierdzenie o pełności, przypomnimy jeszcze fakt, który powinien być znany słuchaczom z kursu *Matematyczne podstawy kognitywistyki*. Niech $(X, \leqslant)$ będzie zbiorem częściowo uporządkowanym. Jeśli każdy $\leqslant$-łańcuch $Y \subseteq X$ ma ograniczenie górne $x \in X$, to w X istnieje element $\leqslant$-maksymalny. Fakt ten znamy jako *Lemat Zorna* (także: *Lemat Kuratowskiego-Zorna*).

TWIERDZENIE O PEŁNOŚCI. Niech $\Sigma \subseteq 2^*$ oraz $\sigma \in 2^*$. Jeśli $\Sigma \models \sigma$, to $\Sigma \vdash \sigma$.

DOWÓD. Przeprowadzimy dowód nie wprost. Przypuśćmy, że $\Sigma \nvdash \sigma$. Znajdziemy ścieżkę nieskończoną $P \subseteq 2^* - \Sigma$ przechodzącą przez σ. To będzie oznaczało, że $\Sigma \not\models \sigma$, z więc zakończy dowód twierdzenia.

Niech X będzie rodziną wszystkich zbiorów Σ' takich, że $\Sigma \subseteq \Sigma'$ oraz $\Sigma' \nvdash \sigma$. Wtedy $(X, \subseteq)$ jest zbiorem częściowo uporządkowanym, w którym każdy łańcuch ma ograniczenie górne (ograniczeniem górnym łańcucha zbiorów jest suma łańcucha). Widać bowiem, że suma każdego łańcucha w $(X, \subseteq)$ zawiera zbiór Σ. Ponadto, jeśli C jest łańcuchem w $(X, \subseteq)$ oraz $\bigcup C \vdash \sigma$, to istnieje dowód σ z pewnego skończonego zbioru $\Sigma_0 \subseteq \bigcup C$. Skoro Σ_0 jest skończony, a C jest łańcuchem, to Σ_0 musi być całkowicie zawarty w jakimś elemencie tego łańcucha.

Na mocy lematu Zorna, w X istnieje element maksymalny Σ^+. Pokażemy, że Σ^+ jest dopełnieniem nieskończonej ścieżki przechodzącej przez σ. Wtedy $P = 2^* - \Sigma^+$ będzie ścieżką nieskończoną, przechodzącą przez σ, ale nie przechodzącą przez żaden element Σ, co będzie oznaczało, że $\Sigma \not\models \sigma$.

Ponieważ $\Sigma^+ \cup \{\sigma\} \vdash \sigma$ na mocy reguł bazowych oraz $\Sigma^+ \cup \{\sigma\} \notin X$, więc $\Sigma^+ \neq \Sigma^+ \cup \{\sigma\}$, a zatem $\sigma \notin \Sigma^+$.

Z maksymalności Σ^+ wynika następująca równoważność, dla dowolnego τ: $\tau \in \Sigma^+$ wtedy i tylko wtedy, gdy $\Sigma^+ \cup \{\tau\} \nvdash \sigma$. Jeśli bowiem $\tau \in \Sigma^+$, to $\Sigma^+ \cup \{\tau\} = \Sigma^+$, a skoro $\Sigma^+ \nvdash \sigma$, to $\Sigma^+ \cup \{\tau\} \nvdash \sigma$. Na odwrót, jeśli $\Sigma^+ \cup \{\tau\} \nvdash \sigma$, to ponieważ $\Sigma^+ \subseteq \Sigma^+ \cup \{\tau\}$ oraz Σ^+ jest elementem maksymalnym w X, więc $\Sigma^+ \cup \{\tau\} = \Sigma^+$, a stąd $\tau \in \Sigma^+$.

$2^* - \Sigma^+$ jest drzewem. Przypuśćmy bowiem, że $\tau i \notin \Sigma^+$, gdzie $i \in \{0, 1\}$. Pokażemy, że wtedy $\tau \notin \Sigma^+$. Na mocy poczynionego przypuszczenia oraz maksymalności Σ^+ mamy: $\Sigma^+ \cup \{\tau i\} \vdash \sigma$. Ale wtedy $\Sigma^+ \cup \{\tau\} \vdash \sigma$, na mocy tego samego wyprowadzenia plus jeden krok, polegający na użyciu reguły wydłużania. Tak więc, $\tau \notin \Sigma^+$.

$2^* - \Sigma^+$ jest nieskończoną ścieżką. Przypuśćmy bowiem, że $\tau \notin \Sigma^+$. Pokażemy, że $\tau i \notin \Sigma^+$ dla dokładnie jednego $i \in \{0, 1\}$. Na mocy maksymalności Σ^+ mamy $\Sigma^+ \cup \{\tau\} \vdash \sigma$. Gdyby $\tau 0$ oraz $\tau 1$ oba należały do Σ^+, to mielibyśmy $\Sigma^+ \vdash \sigma$ na mocy tego samego wyprowadzenia oraz jednego użycia reguły skracania. To jednak jest niemożliwe, ponieważ $\Sigma^+ \in X$ (przypomnij sobie definicję zbioru X). Gdyby żaden z ciągów $\tau 0$ oraz $\tau 1$ nie należał do Σ^+, to – na mocy maksymalności Σ^+ – mielibyśmy $\Sigma^+ \cup \{\tau 0\} \vdash \sigma$ oraz $\Sigma^+ \cup \{\tau 1\} \vdash \sigma$. Wtedy jednak (na mocy udowodnionego wcześniej faktu) mielibyśmy $\Sigma^+ \vdash \sigma$, w sprzeczności z definicją Σ^+. Ostatecznie, dokładnie jeden z ciągów $\tau 0$ oraz $\tau 1$ należy do Σ^+, a zatem τ ma jednoznaczne rozszerzenie τi takie, że $\tau i \notin \Sigma^+$.

Tym samym, dowód twierdzenia o pełności został zakończony.

4 Ciekawostka: gra Smullyana

Przypuśćmy, że masz nieskończenie wiele kul, ponumerowanych dodatnimi liczbami całkowitymi, przy czym każda taka liczba jest umieszczona na nieskończenie wielu kulach (masz więc nieskończenie wiele kul z jedynką, nieskończenie wiele z dwójką, nieskończenie wiele z trójką, itd.). Masz też pudełko, które zawiera skończenie wiele ponumerowanych kul. Celem zabawy jest opróżnienie pudełka, wedle następującej reguły. W każdym kroku wyjmujesz pewną kulę, a na jej miejsce wkładasz całkiem dowolną liczbę kul o mniejszych numerach. Ponieważ nie ma mniejszych od jedynki dodatnich liczb całkowitych, więc kuli z jedynką niczym nie zastępujesz. Rozwiązanie wygląda prosto: wystarczy, że zastąpisz każdą kulę w pudełku kulą z jedynką, a potem wyjmiesz te wszystkie kule z jedynką po kolei. Ciekawe w tej zabawie jest jednak to, że nie można z góry ograniczyć liczby kroków potrzebnych to opróżnienia pudełka – pamiętajmy, że można „utrudniać” poprzez dokładanie dowolnej skończonej liczby kul, byle o numerze mniejszym niż numer kuli zastępowanej. Czy potrafisz uzasadnić, że zabawa musi zakończyć się po skończonej liczbie kroków?

Zabawę tę przedstawić można w postaci drzewa o ponumerowanych wierzchołkach. Początkową zawartość pudełka reprezentują wierzchołki wychodzące bezpośrednio z korzenia drzewa. Zastępowanie jakiejś kuli (liścia drzewa) zbiorem innych polega na dołączeniu, w miejsce usuwanego liścia, całego zbioru nowych liści, reprezentujących kule, zastępujące usuwaną kulę. Drzewo „rośnie w górę" w miarę jak zastępujemy usuwane kule nowymi. Zauważmy, że na każdej gałęzi drzewa występują kule o coraz mniejszych numerach. Ponadto, każdy wierzchołek drzewa ma tylko skończenie wielu bezpośrednich potomków. Gdyby drzewo miało nieskończoną liczbę wierzchołków, to (na mocy *lematu Königa*) musiałoby mieć gałąź nieskończoną. To jednak jest niemożliwe, ze względu na wspomniany już fakt, że numery na każdej gałęzi maleją, w miarę oddalania się od korzenia drzewa. Tak więc, zabawa w opróżnianie pudełka musi zakończyć się w skończonej liczbie kroków.

Jedna z prac Heraklesa polegała na uśmierceniu *hydry lernejskiej*, potwora o wielu głowach, przy tym o tyle trudnym do zabicia, że w miejsce odciętej głowy wyrastały natychmiast następne. Jak pamiętamy, Herakles *praktycznie* rozwiązał ten problem, znany był zresztą z wielu *praktycznych* rozwiązań trudnych problemów. Z matematycznego punktu widzenia hydra jest *drzewem*: *korzeniem* tego drzewa jest jej kadłubek, *liśćmi* poszczególne głowy, pozostałe *wierzchołki* drzewa odpowiadają segmentom szyi, (które same mogą stać się głowami, po odcięciu innych głów). Zabicie hydry polega na takim jej okaleczeniu, iż pozostaje z niej jedynie tułów-kadłubek (korzeń drzewa). Odcinamy głowy hydry (czyli liście drzewa) w pojedynczych krokach (cięciach mieczem). Odcięcie głowy w n-tym kroku pociąga za sobą następujące konsekwencje:

1. Znika krawędź drzewa prowadząca do tej głowy, pozostawiając zatem wierzchołek, który nazwiemy, powiedzmy, *krwawiącym kikutem*.

2. W wierzchołku będącym bezpośrednim poprzednikiem krwawiącego kikuta wyrasta hydrze dodatkowo n kopii tej części hydry, która po odcięciu głowy znajduje się powyżej węzła poprzedzającego krwawiący kikut.

3. Jeśli krwawiącym kikutem właśnie odciętej głowy jest kadłub hydry, to żadna nowa głowa nie wyrasta.

Proponujemy wykonać rysunek średnio skomplikowanej hydry i przekonać się, jak wygląda jej utarczka z Heraklesem.

Zdawać by się mogło, że uśmiercenie hydry robi się coraz trudniejszym zadaniem, w miarę stopniowego ucinania jej głów (wszak z każdym cięciem odrasta nie jedna głowa, ale wiele kopii całego fragmentu hydry, a liczba dodawanych kopii rośnie wraz z liczbą kolejnych cięć). Mamy jednak złe wiadomości dla hydry, a dobre dla Heraklesa. Otóż *niezależnie* od tego, jaką przyjmie on strategię (czyli niezależnie od tego, które kolejne głowy hydry będzie odcinał), to po *skończonej* liczbie cięć z biednej hydry zostanie jedynie bezgłowy kadłubek, czyli zostanie ona uśmiercona. Zagadka polega właśnie na udowodnieniu tego faktu. Nie jest to przy tym problem banalny: okazuje się, że twierdzenie gwarantujące zwycięstwo Heraklesa jest *prawdziwe* w standardowej dziedzinie liczb naturalnych, lecz *nie jest dowodliwe* w arytmetyce. Jego dowód wykorzystuje środki *infinitarne*, niedostępne w zwykłej arytmetyce. Może znajdziemy chwilę na wykładzie *Teoria rekursji a metody dowodowe*, aby opowiedzieć o *ciągach Goodsteina*, związanych z omawianą wyżej problematyką.

Kaye, R. 2007. *The Mathematics of Logic. A guide to completeness theorems and their applications*. Cambridge University Press, Cambridge.

Smullyan, R. 2009. *Logical Labyrinths*. A K Peters, Ltd. Wellesley, Massachusetts. Istnieje przekład polski (JP), ale nie ma dlań na razie wydawcy.

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