

4. WYKŁAD 4: DOWODY INDUKCYJNE, STRATEGIE DOWODOWE.

4.1. Dowody indukcyjne. Dotychczas zobaczyliśmy w jaki sposób można specyfikować definicje indukcyjne kategorii syntaktycznych lub osądów, czy też w zasadzie indukcyjne systemy kategorii syntaktycznych lub osądów. Okazuje się jednak, że definicje indukcyjne jako takie mają ograniczone zastosowanie o ile nie pokażemy, że zdefiniowany przez nie system ma pożądane przez nas własności. Innymi słowy, nie możemy indukcyjnie zdefiniować danego systemu a następnie niezwłocznie zacząć go używać bez wcześniejszego sprawdzenia pewnych jego własności. Na przykład intuicyjnie czujemy, że każdy ciąg w kategorii syntaktycznej **mparen** ma taką samą liczbę nawiasów lewych jak i prawych, aczkolwiek definicja tej kategorii nie dowodzi automatycznie takiej własności. Tym samym musimy jakoś formalnie udowodnić, że kategoria **mparen** opisuje ciągi odpowiadających sobie lewych i prawych nawiasów zanim zaczniemy ją używać.

Istnieją także inne powody, dla których musimy być w stanie przeprowadzać formalne dowody własności systemów indukcyjnych. Na przykład systemy indukcyjne często są tak rozbudowane i skomplikowane, że ich niesprzeczność wcale nie jest oczywista. W takich wypadkach na ogół próbujemy udowodnić pewną własność, o której spodziewamy się, że zachodzi w danym systemie. Wówczas każda usterka w definicji, która psuje żądaną własność, prędzej czy później ujawni się w dowodzie. Na przykład wyrażenie w języku funkcyjnym powinno ewaluować się do wartości o zadanym typie, ale odpowiedzialna za to własność języka funkcyjnego (zwana **własnością zachowywania typu**) wcale nie jest oczywista. Chcąc udowodnić zachowywanie typów musimy albo zlokalizować usterki w definicjach, albo częściowo dowieść niesprzeczności systemu. Tym samym dowodzenie własności systemów indukcyjnych staje się najbardziej efektywną pomocą w poprawianiu błędów w definicjach.

Na początek poznamy zasadę zwaną **indukcją strukturalną** służącą dowodzeniu własności systemów indukcyjnych kategorii syntaktycznych. Następnie zajmiemy się studiowaniem zasady zwanej **indukcją reguł** służącą dowodzeniu indukcyjnych systemów osądów. Jako że indukcyjny system kategorii syntaktycznej jest w istocie uproszczonym przedstawieniem odpowiadającego mu indukcyjnego systemu osądów, indukcja strukturalna to w rzeczywistości specjalny przypadek indukcji reguł. Niezależnie od tego indukcja strukturalna zasługuje na osobne potraktowanie ze względu na rolę jaką kategorie syntaktyczne grają w studiowaniu języków programowania.

4.1.1. Indukcja strukturalna. Zasada indukcji strukturalnej orzeka, iż własność kategorii syntaktycznej może być udowodniona indukcyjnie poprzez analizę struktury jej definicji: dla każdego przypadku bazowego pokazujemy, że własność zachodzi bez żadnych dodatkowych założeń, a dla każdego przypadku w kroku indukcyjnym zakładamy, że własność zachodzi dla każdego mniejszego elementu kategorii i następnie pokazujemy, że zachodzi dla całego przypadku.

Kilka przykładów powinno wyjaśnić o co chodzi. Rozważmy kategorię syntaktyczną liczb naturalnych. Chcemy pokazać, że $P(n)$ zachodzi dla dowolnej liczby naturalnej n . Przykładami $P(n)$ mogą być:

- n ma następnik,
- n jest równe 0 lub n ma poprzednik n' ,
- n jest iloczynem liczb pierwszych (zakładamy tu, że definicje liczby pierwszej i iloczynu są dane).

Przez indukcję strukturalną dowodzimy następujących dwóch stwierdzeń:

- $P(0)$ zachodzi,
- jeżeli $P(n)$ zachodzi, to zachodzi również $P(S\ n)$.

Pierwsze stwierdzenie dotyczy przypadku bazowego, gdy 0 nie zawiera elementu mniejszego od siebie, pokazujemy więc, że $P(0)$ zachodzi bez żadnych założeń. Drugie stwierdzenie dotyczy kroku indukcyjnego, w którym $S\ n$ zawiera mniejszy element n , przyjmujemy więc, jako **założenie indukcyjne**, że zachodzi

$P(n)$, a następnie dowodzimy, iż zachodzi $P(S\ n)$. Taka indukcja strukturalna zasadniczo niczym nie różni się od znanej ze szkoły średniej zasady indukcji matematycznej.

Jako kolejny przykład rozważmy kategorię syntaktyczną drzewek binarnych **tree**. Aby udowodnić, że $P(t)$ zachodzi dla każdego regularnego drzewka binarnego t , musimy udowodnić następujące stwierdzenia:

- $P(\text{leaf } n)$ zachodzi,
- jeżeli $P(t_1)$ i $P(t_2)$ zachodzą jako założenia indukcyjne, to zachodzi również $P(\text{node } (t_1, n, t_2))$.

Taka indukcja strukturalna bywa czasami nazywana **indukcją po drzewach**.

Jako przykład dowodu indukcyjnego przez indukcję strukturalną pokażemy, że każdy ciąg nawiasów z kategorii **mparen** ma taką samą liczbę nawiasów lewych jak i prawych. Zdefiniujmy na początek dwie funkcje pomocnicze $left$ i $right$ które będą zliczały liczbę lewych i prawych nawiasów, odpowiednio. Dla poprawienia czytelności zamiast $left(s)$ i $right(s)$ będziemy pisali $left[s]$ i $right[s]$. Tym samym mamy:

$$\begin{aligned} left[\epsilon] &= 0 \\ left[(s)] &= 1 + left[s] \\ left[s_1\ s_2] &= left[s_1] + left[s_2] \\ right[\epsilon] &= 0 \\ right[(s)] &= 1 + right[s] \\ right[s_1\ s_2] &= right[s_1] + right[s_2]. \end{aligned}$$

Teraz możemy zinterpretować $P(s)$ jako " $left[s] = right[s]$ ". Chcemy zatem pokazać, że jeśli s jest elementem **mparen**, co zapisujemy jako $s \in \text{mparen}$, to wówczas zachodzi $P(s)$.

Twierdzenie 1. *Jeśli $s \in \text{mparen}$, to $left[s] = right[s]$.*

Dowód. W dowodzie każda linijka odpowiada jednemu krokowi, przy czym stosujemy następującą konwencję notacyjną:

konkluzja

uzasadnienie

Akurat taki format zapisu sprawia, że dowód jest łatwy w czytaniu, gdyż zawsze na pierwszym miejscu widzimy konkluzję poprzedniego kroku, a nie jej uzasadnienie.

Przypadek $s = \epsilon$:

$$left[\epsilon] = 0 = right[\epsilon]$$

Przypadek $s = (s')$:

$$left[s'] = right[s']$$

wobec założenia indukcyjnego o s'

$$left[s] = 1 + left[s'] = 1 + right[s'] = right[s]$$

wobec $left[s'] = right[s']$

Przypadek $s = s_1\ s_2$:

$$left[s_1] = right[s_1]$$

wobec założenia indukcyjnego o s_1

$$left[s_2] = right[s_2]$$

wobec założenia indukcyjnego o s_2

$$left[s_1\ s_2] = left[s_1] + left[s_2] = right[s_1] + right[s_2] = right[s_1\ s_2]$$

$$\text{wobec } left[s_1] = right[s_1] \text{ oraz } left[s_2] = right[s_2]$$

□

W dowodach takich jak powyższy często mówimy o dowodzie "przez indukcję ze względu na strukturę s " zamiast "przez indukcję strukturalną na s ".

4.1.2. *Inkdukcja reguł.* Zasada indukcji reguł jest podobna do zasady indukcji strukturalnej z tym zastrzeżeniem, że stosuje się ją do drzew dowodowych raczej niż do definicji kategorii syntaktycznych. Rozważmy mianowicie definicję indukcyjną osądu J z następującymi regułami wnioskowania:

$$\frac{}{J_b} R_{\text{base}} \quad \frac{J_1 \quad J_2 \quad \dots \quad J_n}{J_i} R_{\text{ind}}$$

Chcemy pokazać, że gdy tylko J zachodzi, inny osąd $P(J)$ również zachodzi, przy czym $P(J)$ jest nową formą osądu parametryzowaną przez J . Na przykład jeśli w roli J weźmiemy " $n \text{ nat}$ ", to wówczas jako $P(J)$ możemy wziąć " $\text{albo } n \text{ par albo } n \text{ npar}$ ". Tym samym dowodzić będziemy następujących stwierdzeń:

- $P(J_b)$ zachodzi,
- jeżeli $P(J_1), P(J_2), \dots, P(J_n)$ zachodzą, to zachodzi również $P(J_i)$.

Wobec pierwszego stwierdzenia, następująca reguła wnioskowania ma sens, jako że zawsze jesteśmy w stanie dowieść $P(J_b)$:

$$\frac{}{P(J_b)} R'_{\text{base}}$$

Następująca reguła wnioskowania również będzie miała sens z racji drugiego stwierdzenia: jeżeli zachodzą $P(J_1), P(J_2), \dots, P(J_n)$, to $P(J_i)$ również zachodzi:

$$\frac{P(J_1) \quad P(J_2) \quad \dots \quad P(J_n)}{P(J_i)} R'_{\text{ind}}$$

Teraz dla każdego drzewa dowodowego dla osądu J wykorzystującego reguły R_{base} oraz R_{ind} możemy udowodnić $P(J)$ stosując reguły R'_{base} oraz R'_{ind} :

$$\begin{array}{ccc} \frac{}{J_b} R_{\text{base}} & \Rightarrow & \frac{}{P(J_b)} R'_{\text{base}} \\ \vdots & & \vdots \\ \frac{J_1 \quad J_2 \quad \dots \quad J_n}{J_i} R_{\text{ind}} & \Rightarrow & \frac{P(J_1) \quad P(J_2) \quad \dots \quad P(J_n)}{P(J_i)} R'_{\text{ind}} \end{array}$$

Innymi słowy, J zawsze pociąga $P(J)$. Uogólnienie powyższej strategii nazywamy zasadą indukcji reguł.

Jako trywialny przykład udowodnimy, że $n \text{ nat}$ pociąga $n \text{ par}$ lub $n \text{ npar}$. Niech $P(n \text{ nat})$ oznacza " $\text{albo } n \text{ par albo } n \text{ npar}$ " i zastosujmy zasadę indukcji reguł. Reguły *Zero* i *Succ* wymuszają konieczność dowodu następujących dwóch stwierdzeń:

- $P(0 \text{ nat})$ zachodzi. Innymi słowy, w przypadku gdy reguła *Zero* jest użyta do dowodu $n \text{ nat}$, otrzymujemy $n = 0$ i tym samym dowodzimy $P(0 \text{ nat})$.
- Jeżeli $P(n' \text{ nat})$ zachodzi, to zachodzi $P(S n' \text{ nat})$. Innymi słowy, w przypadku gdy reguła *Succ* jest użyta do dowodu $n \text{ nat}$, otrzymujemy $n = S n'$ i tym samym dowodzimy $P(S n' \text{ nat})$ wykorzystując założenie indukcyjne $P(n' \text{ nat})$.

Wobec definicji $P(J)$, powyższe dwa stwierdzenia są równoważne następującym:

- zachodzi 0 par lub 0 npar ,
- jeżeli zachodzi $n' \text{ par}$ lub $n' \text{ npar}$, to zachodzi $S n' \text{ par}$ lub $S n' \text{ npar}$.

Formalny dowód indukcyjny będzie wyglądał następująco:

Twierdzenie 2. *Jeżeli $n \text{ nat}$, to wówczas $n \text{ par}$ lub $n \text{ npar}$.*

Dowód. Podkreślmy tutaj, że w dowodzie będziemy stosować zasadę indukcji reguł w odniesieniu do osądu $n \text{ nat}$, a nie do liczby naturalnej n . Innymi słowy, będziemy analizowali strukturę dowodu $n \text{ nat}$, nie zaś strukturę liczby n . Analiza struktury liczby n spowodowałaby, że dowód zdegenerowałby się do przykładu indukcji strukturalnej!

Przypadek $\frac{}{0 \text{ nat}} \text{Zero}$ (gdzie n akurat równe jest 0).

(W tym przypadku osąd $n \text{ nat}$ jest dowodzony z wykorzystaniem reguły Zero . Nie jest to to samo co przypadek, gdy n jest równe 0, jako że nie odwołujemy się do struktury n . Nie stosujemy tu też założenia indukcyjnego.)

0 par wobec reguły ZeroE

Przypadek $\frac{n' \text{ nat}}{S n' \text{ nat}} \text{Succ}$ (gdzie n akurat równe jest $S n'$).

(W tym przypadku osąd $n \text{ nat}$ jest dowodzony z wykorzystaniem reguły Zero .)

$n' \text{ par}$ lub $n' \text{ npar}$ wobec założenia indukcyjnego

$S n' \text{ par}$ lub $S n' \text{ npar}$ wobec reguły SuccO lub SuccE . $\square$

Indukcja reguł może być także użyta do równoczesnego dowodu dwóch lub więcej osądów. Jako przykład udowodnimy, że liczba n w osądzie $n \text{ par}$ odpowiada liczbie parzystej, zaś n w osądzie $n \text{ npar}$ odpowiada liczbie nieparzystej. Użyjemy reguł ZeroE , SuccE i SuccO razem z następującymi regułami odnoszącymi się do osądu $n \text{ double } n'$:

$$\frac{}{0 \text{ double } 0} \text{Dzero} \quad \text{fracn double } n' S n \text{ double } S S n' \text{Dsucc}$$

Intuicyjnie osąd $n \text{ double } n'$ oznacza, że n' jest podwojeniem n , a więc $n' = 2 \times n$. Własności liczb parzystych i nieparzystych, które będziemy chcieli dowieść, zawarte są w następującym twierdzeniu:

Twierdzenie 3. *Jeżeli $n \text{ par}$, to wówczas istnieje n' takie, że $n' \text{ double } n$.*

Jeżeli $n \text{ npar}$, to wówczas istnieją n' i n'' takie, że $n' \text{ double } n''$ oraz $S n'' = n$.

Dowód twierdzenia będzie przebiegał podobnie jak poprzednie dowody z wykorzystaniem indukcji reguł z tą różnicą, że teraz $P(J)$ będzie rozróżniało dwa przypadki, a mianowicie $J = n \text{ par}$ i $J = n \text{ npar}$:

- $P(n \text{ par})$ oznacza “istnieje n' takie, że $n' \text{ double } n$,”
- $P(n \text{ npar})$ oznacza “istnieją n' oraz n'' takie, że $n' \text{ double } n''$ oraz $S n'' = n$ ”.

Dowód przebiegać będzie teraz następująco:

Dowód.

Przypadek $\frac{}{0 \text{ par}} \text{ZeroE}$ gdzie $n = 0$:

0 double 0 wobec reguły Dzero

Przyjmujemy $n' = 0$.

Przypadek $\frac{n_p \text{ npar}}{S n_p \text{ par}} \text{SuccE}$ gdzie $n = S n_p$:

$n'_p \text{ double } n''_p$ oraz $S n''_p = n_p$ wobec założenia indukcyjnego

$S n'_p \text{ double } S S n''_p$ wobec reguły Dsucc zastosowanej dla $n'_p \text{ double } n''_p$

$S n'_p \text{ double } n$ wobec $S S n''_p = S n_p = n$

Przyjmujemy $n' = S n'_p$.

Przypadek $\frac{n_p \text{ par}}{s \ n_p \ \text{npar}} \text{SuccO}$ gdzie $n = S \ n_p$:

$n'_p \text{ double } n_p$

Przyjmujemy $n' = n'_p$ oraz $n'' = n_p$.

wobec założenia indukcyjnego

□

4.2. Techniki dowodzenia przez indukcję. Dowód indukcyjny nie zawsze jest tak bezpośredni jak w przytoczonych powyżej przykładach. Może się też zdarzyć, iż dowodzone twierdzenie jest fałszywe. W takim wypadku próba dowodu może pomóc nam w znalezieniu kontrprzykładu do twierdzenia. Jeżeli twierdzenie daje się jednak udowodnić, a mimo to bezpośredni dowód nie daje rozstrzygnięcia, możemy spróbować jednej z popularnych technik dowodzenia przez indukcję. Poniżej przedstawiamy trzy z nich: przez zastosowanie lematu, uogólnienie twierdzenia i zastosowanie reguły odwracania.

4.2.1. Stosowanie lematów. Zaczniemy od przededefiniowania kategorii **mparen** i **lparen** jako systemu osądów i reguł wnioskowania:

$$\begin{array}{c} \frac{}{\epsilon \text{ mparen}} \text{Meps} \quad \frac{s \text{ mparen}}{(s) \text{ mparen}} \text{Mpar} \quad \frac{s_1 \text{ mparen } s_2 \text{ mparen}}{s_1 s_2 \text{ mparen}} \text{Mseq} \\[10pt] \frac{}{\epsilon \text{ lparen}} \text{Leps} \quad \frac{s_1 \text{ lparen } s_2 \text{ lparen}}{(s_1) s_2 \text{ mparen}} \text{Lseq} \end{array}$$

Naszym celem jest udowodnienie, że $s \text{ mparen}$ pociąga $s \text{ lparen}$. Okazuje się, że próba bezpośredniego dowodu przez indukcję reguł zawodzi i potrzebne będzie użycie lematu. Aby nieformalnie wyjaśnić, do czego potrzebny będzie lemat, rozważmy sytuację w której reguła *Mseq* jest użyta do dowodu $s \text{ mparen}$. Możemy napisać $s = s_1 s_2$ z wykorzystaniem $s_1 \text{ mparen}$ oraz $s_2 \text{ mparen}$. Wobec założenia indukcyjnego o $s_1 \text{ mparen}$ oraz $s_2 \text{ mparen}$, możemy wywnioskować $s_1 \text{ lparen}$ oraz $s_2 \text{ lparen}$. Wobec $s_1 \text{ lparen}$ musimy rozważyć dwa podprzypadki:

- jeżeli $s_1 = \epsilon$, to wówczas $s = s_1 s_2 = s_2$ i $s_2 \text{ lparen}$ pociąga $s \text{ lparen}$;
- jeżeli $s_1 = (s'_1) s''_1$ z wykorzystaniem $s'_1 \text{ lparen}$ i $s''_1 \text{ lparen}$, to wówczas $s = (s'_1) s''_1 s_2$.

W drugim podprzypadku musimy udowodnić $s''_1 s_2 \text{ lparen}$ z wykorzystaniem $s''_1 \text{ lparen}$ oraz $s_2 \text{ lparen}$, do czego z kolei nie odnosi się nic, co jest przez nas dowodzone. Tym samym konieczne jest zastosowanie następującego lematu:

Lemat 1. *Jeżeli $s \text{ lparen}$ oraz $s' \text{ lparen}$, to wówczas $ss' \text{ lparen}$.*

Jak udowodnić powyższy lemat z użyciem indukcji reguł? Na pierwszy rzut oka wydaje się to niemożliwe, albowiem lemat nie jest w postaci “jeżeli J zachodzi, to zachodzi też $P(J)$ ” – w lemacie poprzednik implikacji zawiera dwa osądy. Okazuje się jednak, że zasadę indukcji reguł można zastosować w zwyczajny sposób. Trik polega na zinterpretowaniu tezy lematu w następujący sposób:

Jeżeli $s \text{ lparen}$, to wówczas jeżeli $s' \text{ lparen}$, to wówczas $ss' \text{ lparen}$.

W takiej postaci możemy zastosować zasadę indukcji reguł do osądu $s \text{ lparen}$ przyjmując $P(s \text{ lparen})$ jako “jeżeli $s' \text{ lparen}$ to wówczas $ss' \text{ lparen}$.” Dowód lematu będzie wówczas wyglądał następująco:

Dowód. Nie zapominajmy, że założeniem indukcyjnym wobec $s \text{ lparen}$ jest “jeżeli $s' \text{ lparen}$, to wówczas $ss' \text{ lparen}$ ”. W konsekwencji jeśli $s' \text{ lparen}$ jest dostępne jako założenie, to wówczas założenie indukcyjne wobec $s \text{ lparen}$ daje $ss' \text{ lparen}$.

Przypadek $\frac{}{\epsilon \text{ lparen}} \text{Leps}$ gdzie $s = \epsilon$:

$s' \text{ lparen}$

wobec założenia

$$ss' = \epsilon s' = s'$$

$$ss' \text{ lparen}$$

wobec $s' \text{ lparen}$.

Przypadek $\frac{s_1 \text{ lparen } s_2 \text{ lparen}}{(s_1)s_2 \text{ mparen}} Lseq$ gdzie $s = (s_1)s_2$:

$$s' \text{ lparen}$$

wobec założenia

$$ss' = (s_1)s_2s'$$

“jeżeli $s' \text{ lparen}$ to wówczas $s_2s' \text{ lparen}$ ”

wobec założenia indukcyjnego dla $s_2 \text{ lparen}$

$$s_2s' \text{ lparen}$$

wobec założenia $s' \text{ lparen}$

$$(s_1)s_2s' \text{ lparen}$$

wobec reguły $Lseq$ zastosowanej do $s_1 \text{ lparen}$ oraz $s_2s' \text{ lparen}$.

□

Zadanie 7. Udowodnić powyższy lemat z zastosowaniem zasady indukcji reguł dla osądu $s' \text{ lparen}$.

Możemy teraz przejść do dowodu twierdzenia.

Twierdzenie 4. Jeżeli $s \text{ mparen}$, to wówczas $s \text{ lparen}$.

Dowód.

Przypadek $\frac{}{\epsilon \text{ mparen}} Meps$ dla $s = \epsilon$:

$$\epsilon \text{ lparen}$$

wobec reguły $Leps$.

Przypadek $\frac{s \text{ mparen}}{(s) \text{ mparen}} Mpar$ dla $s = (s')$:

$$s' \text{ lparen}$$

wobec $\frac{s' \text{ lparen } \frac{}{\epsilon \text{ lparen}} Leps}{(s')\epsilon \text{ lparen}} Lseq$ oraz $(s') = (s')\epsilon$.

Przypadek $\frac{s_1 \text{ mparen } s_2 \text{ mparen}}{s_1s_2 \text{ mparen}} Mseq$ dla $s = s_1s_2$:

$$s_1 \text{ lparen}$$

wobec założenia indukcyjnego dla $s_1 \text{ mparen}$

$$s_2 \text{ lparen}$$

wobec założenia indukcyjnego dla $s_2 \text{ mparen}$

$$s_1s_2 \text{ lparen}$$

wobec lematu.

□

4.2.2. Uogólnianie twierdzeń. Pokazaliśmy, że jeśli ciąg nawiasów s należy do kategorii syntaktycznej mparen , to s ma taką samą liczbę lewych i prawych nawiasów, a więc że $left[s] = right[s]$. Z naszego dowodu nie wynika wszelako, że ciąg s jest ciągiem odpowiadających sobie lewych i prawych nawiasów, nie bierze bowiem pod uwagę tego, w jaki sposób poszczególne nawiasy są rozmieszczone. Na przykład $s =)(($ spełnia $left[s] = right[s]$, ale nie jest ciągiem odpowiadających sobie lewych i prawych nawiasów.

Aby nauczyć się rozpoznawać ciągi odpowiadających sobie nawiasów, wprowadzamy nowy osąd $k \triangleright s$, gdzie k jest nieujemną liczbą całkowitą:

$$k \triangleright s \Leftrightarrow k \text{ lewych nawiasów doklejonych do } s \text{ jest ciągiem odpowiadających sobie lewych i prawych nawiasów}$$

$$\Leftrightarrow \underbrace{((\dots (s \text{ jest ciągiem odpowiadających sobie nawiasów.}}_k$$

Pomysł jest następujący: parsujemy dany ciąg nawiasów z lewej do prawej i liczymy pojawiające się lewe nawiasy, które nie mają jeszcze swoich prawych odpowiedników. Zaczynamy więc od $k = 0$, zwiększamy

k o 1 za każdym razem, gdy napotkamy na lewy nawias i zmniejszamy k o 1 za każdym razem, gdy napotkamy prawy nawias:

$$\frac{}{0 \triangleright \epsilon} Peps \quad \frac{k+1 \triangleright s}{k \triangleright (s)} Pleft \quad \frac{k-1 \triangleright s \quad k > 0}{k \triangleright)s} Pright$$

Druga przesłanka, czyli $k > 0$, w regule *Pright* zapewnia, iż w dowolnym ciągu nawiasów liczba prawych nawiasów nie może przekroczyć liczby lewych nawiasów. Osąd $0 \triangleright s$ oznacza, że s jest ciągiem odpowiadających sobie nawiasów. Oto przykład:

$$\begin{array}{lcl} \frac{0 \triangleright \epsilon}{1 \triangleright)} Peps & 1 > 0 & \\ \frac{}{2 \triangleright))} Pright & 2 > 0 & \\ \frac{1 \triangleright ()}{0 \triangleright (())} Pleft & & \end{array}$$

Zauważmy, że o ile reguły wnioskowania dobrze jest czytać od przesłanek do wniosków, a więc w formie “jeżeli zachodzą przesłanki, to zachodzi też wniosek”, o tyle w przypadku powyższych reguł wygodniej jest je czytać od wniosku do przesłanki, czyli w formie “aby udowodnić wniosek, dowodzimy następującą przesłankę”. Na przykład, reguła *Peps* może być odczytana jako “aby udowodnić $0 \triangleright \epsilon$, nie musimy niczego innego dowodzić”. Taki sposób czytania reguł wnioskowania “od dołu do góry” odpowiada kierunkowi parsowania ciągów nawiasów od lewej do prawej. Na przykład, dowód osądu $0 \triangleright (())$ przebiegałby zgodnie z następującym ciągiem osądów czytanych od lewej do prawej:

$$0 \triangleright (()) \rightarrow 1 \triangleright () \rightarrow 2 \triangleright) \rightarrow 1 \triangleright) \rightarrow 0 \triangleright \epsilon$$

Zadanie 8. Przepisać reguły wnioskowania dla osądu $k \triangleright s$ tak, aby wygodniej było go czytać w kierunku od przesłanek do wniosków.

Naszym celem jest teraz następujące twierdzenie:

Twierdzenie 5. Jeżeli $0 \triangleright s$, to wówczas s mparen.

Łatwo sprawdzić, że próba bezpośredniego dowodu powyższego twierdzenia musi zawieść. Na przykład, jeżeli osąd $0 \triangleright (s$ jest wnioskiem z osądu $1 \triangleright s$ po zastosowaniu reguły *Pleft*, nie możemy zastosować założenia indukcyjnego do przesłanki, ponieważ ta nie jest postaci $0 \triangleright s'$. To, czego wobec tego potrzebujemy, to uogólnienie powyższego twierdzenia, które obejmie wszystkie osady postaci $k \triangleright s$, a nie tylko szczególny przypadek $k = 0$.

Lemat 2. Jeżeli $k \triangleright s$, to wówczas $\underbrace{((\dots (}_{k} \text{mparen.}$

Powyższy lemat formalnie dowodzi to, co jest intuicyjnie jasne w definicji osądu $k \triangleright s$. Dowodzone twierdzenie jest prostym wnioskiem z powyższego lematu.

Z kolei dowód powyższego lematu wymaga dowodu innego lematu, który pozostawiamy tu jako ćwiczenie:

Lemat 3. Jeżeli $\underbrace{((\dots (}_{k} \text{mparen}$, to wówczas $\underbrace{((\dots ((}_{k} \text{mparen.}$

Dowód naszego lematu będzie przebiegał następująco:

Dowód.

Przypadek $\frac{0 \triangleright \epsilon}{0 \triangleright \epsilon} Peps$ gdzie $k = 0$ oraz $s = \epsilon$:

ϵ mparen
 $\underbrace{((\dots (s \text{mparen}}_k$

wobec reguły *Meps*
 wobec $\underbrace{((\dots (s = \epsilon}_k$.

Przypadek $\frac{k+1 \triangleright s'}{k \triangleright s'} Pleft$ gdzie $s = (s'$:

$\underbrace{((\dots (s' \text{mparen}}_{k+1}$
 $\underbrace{((\dots (s \text{mparen}}_k$

wobec założenia indukcyjnego dla $k + 1 \triangleright s'$

wobec $\underbrace{((\dots (s'}_{k+1} = \underbrace{((\dots (s'}_k = \underbrace{((\dots (s}_k$.

Przypadek $\frac{k-1 \triangleright s' \quad k > 0}{k \triangleright s'} Pright$ gdzie $s =)s'$:

$\underbrace{((\dots (s' \text{mparen}}_{k-1}$
 $\underbrace{((\dots ((s' \text{mparen}}_{k-1}$
 $\underbrace{((\dots (s \text{mparen}}_k$

wobec założenia indukcyjnego dla $k - 1 \triangleright s'$

wobec Lematu

wobec $\underbrace{((\dots ((s'}_{k-1} = \underbrace{((\dots (s')_k} = \underbrace{((\dots (s}_k$.
 $\square$

Jest ważne aby zrozumieć, że uogólnianie twierdzenia nie jest tym samym co stosowanie lematu. Lematy stosujemy, gdy założenia indukcyjne stosują się do wszystkich przesłanek w dowodzie indukcyjnym, ale wśród możliwych do wyciągnięcia wniosków nie ma naszego celu dowodowego. W typowej sytuacji lemat wypełnia lukę pomiędzy założeniem indukcyjnym a żądanym wnioskiem i sam wymaga dowodu indukcyjnego który przeprowadza się osobno. W przypadku uogólniania twierdzenia mamy do czynienia z sytuacją, gdy założenia indukcyjne nie stosują się do niektórych z przesłanek i dowód indukcyjny nie jest w ogóle możliwy do przeprowadzenia. Zastosowanie lematu nie jest w takim razie możliwe, albowiem założenia indukcyjne stosują się tylko do przesłanek reguł wnioskowania i niczego innego. Tym samym uogólniamy twierdzenie tak, aby można je udowodnić wprost indukcyjnie.

Uogólnienie twierdzenia na ogół oznacza znalezienie twierdzenia, które jest trudniejsze w dowodzie, ale z którego żądane twierdzenie wynika natychmiastowo. Nie ma jakiejś szczególnej recepty na to, w jaki sposób twierdzenia można uogólniać, warto wszakże pamiętać, iż niektóre problemy wymagają naprawdę szerokiego spojrzenia na osąd, do którego dowodu ma być zastosowane założenie indukcyjne. W wielu wypadkach wyodrębnienie niezmiennika danego osądu dają pożyteczną wskazówkę w jaki sposób możliwe jest uogólnianie rezultatu. Na przykład przytoczone powyżej twierdzenie dotyczy specjalnego przypadku osądu $k \triangleright s$ i jego uogólnienie dokładnie wyjaśnia co właściwie znaczy osąd $k \triangleright s$.

4.2.3. *Zastosowanie reguły odwracania.* Rozważmy regułę wnioskowania

$$\frac{J_1 \quad J_2 \quad \dots \quad J_n}{J} R.$$

Aby zastosować regułę R musimy najpierw znaleźć dowody przesłanek $J_1, \dots, J_n$. W nieco odmienny sposób możemy wyrazić to samo mówiąc, że aby udowodnić J , wystarczy pokazać $J_1, \dots, J_n$. Tak czy inaczej, w obydwu przypadkach zawsze najpierw interesuje nas dowód przesłanek.

Założmy, że istnieje dowód wniosku J . Innymi słowy, założmy, że J jest dowodliwe, jakkolwiek nie dysponujemy gotowym dowodem J . Zwróćmy uwagę, że z tego, że osąd J jest dowodliwy, nie musi wcale wynikać, że dowodliwe są przesłanki $J_1, \dots, J_n$. Może się na przykład zdarzyć, że będziemy dysponowali regułą wnioskowania

$$\frac{J'_1 \quad J'_2 \quad \dots \quad J'_m}{J} R'$$

która pozwala dojść do tego samego wniosku z zastosowaniem innych przesłanek. W takim wypadku nie możemy być pewni, że reguła R została zastosowana w końcowym kroku dowodu osądu J , w szczególności nie gwarantuje, że istnieją dowody osądów $J_1, \dots, J_n$.

Jeżeli jednak reguła R jest *jedynym* sposobem, aby udowodnić wniosek J , możemy bezpiecznie “odwrócić” regułę R i wywnioskować w ten sposób przesłanki $J_1, \dots, J_n$ z istniejącego dowodu osądu J . Innymi słowy, jako że reguła R jest jedynym sposobem wywnioskowania osądu J , istnienie dowodu J zależy od istnienia dowodów osądów $J_1, \dots, J_n$. Tego typu rodzaj wnioskowania “od dołu do góry” nazywany jest dowodzeniem przez **zastosowanie reguły odwracania**.

Jako przykład udowodnimy następujące twierdzenie:

Twierdzenie 6. *Jeżeli $S \ n \ \text{nat}$, to również $n \ \text{nat}$.*

Dowód. Zaczniemy od założenia, że zachodzi osąd $S \ n \ \text{nat}$. Jako że jedynym sposobem udowodnienia $S \ n \ \text{nat}$ jest poprzez regułę *Succ*, $S \ n \ \text{nat}$ musi być udowodnione przy użyciu $n \ \text{nat}$ następująco:

$$\frac{n \ \text{nat}}{S \ n \ \text{nat}} \text{Succ}$$

Tym samym fragment dowodu $S \ n \ \text{nat}$ pociąga również dowód interesującego nas faktu. □