

3. WYKŁAD 3: DOWODY INDUKCYJNE, STRATEGIE DOWODOWE.

3.1. 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.

3.1.1. 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 ".

3.1.2. *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

□

3.2. 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.

3.2.1. 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 “jeśli 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 4. Udowodnić powyższy lemat z zastosowaniem zasady indukcji reguł dla osqdu $s' \text{ lparen}$.

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.

□