Prace Naukowe Wyższej Szkoły Pedagogicznej w Częstochowie
Matematyka V, Częstochowa 1997

Uogólnianie dowodów

Piotr Wojtylak

1. Arytmetyka Peano PA jest teorią 1-go rzędu powstającą przez dołączenie do logiki predykatów z identycznością następujących aksjomatów charakteryzujących specyficzne arytmetyczne własności 0 (zera), S (operacji następnika), $+$ (dodawania) oraz $\times$ (mnożenia liczb naturalnych) :

$$
\begin{array}{llll}
(Ax1) & 0 \neq Sx & (Ax2) & Sx = Sy \to x = y \\
(Ax3) & x + 0 = x & (Ax4) & x + Sy = S(x + y) \\
(Ax5) & x \times 0 = 0 & (Ax6) & x \times Sy = (x \times y) + x
\end{array}
$$

$$(SI) \qquad A(0), \forall_x \Big(A(x) \to A(Sx) \Big) \to \forall_x A(x).$$

Aksjomatami teorii PA są, w szczególności, wszystkie formuły rozważanego języka $\{0, S, +, \times, =\}$ podpadające pod schemat indukcji następnikowej (SI). W literaturze rozważane są różne warianty, fragmenty i wersje językowe systemu. Przykładowo, PA^- jest skończenie aksjomatyzowalnym podsystemem PA zawierającym aksjomaty dyskretnie uporządkowanych (pół)pierścieni. Rozważne są ponadto rozszerzenia PA symbolami funkcyjnymi i relacjami definiowalnymi w języku standardowym, tj. P (poprzednik), $-$ (różnica względna), $\leq$ (porządek). Arytmetyka Presburgera jest fragmentem PA w języku $0, S, +, =, \leq$ (bez mnożenia). System ten, w przeciwieństwie do innych wspomnianych tutaj wersji i wariantów PA, jest rozstrzygalny, tzn. istnieje rekurencyjna metoda rozpoznawania tez Arytmetyki Presburgera. Schemat indukcji następnikowej (SI) bywa zastępowany schematem indukcji porządkowej

$$(OI) \qquad \forall_x \Big(\forall_{y<x} A(y) \to A(x) \Big) \to \forall_x A(x).$$

Modyfikując odpowiednio pozostałe aksjomaty PA otrzymujemy tzw. arytmetykę porządkową OA równoważną tradycyjnie PA. Ponieważ rozważane będą dalej aspekty teorii formalnych zależne od aksjomatyzacji, a nie tylko od relacji dowodliwości, wszystkie wprowadzone wersje PA muszą być rozróżniane. W pracy nie będzie obowiązywała zaproponowana przez A.Tarskiego identyfikacja teorii ze zbiorem jej tez. Porównując dwie teorie brane będą dodatkowo pod uwagę logiczne struktury ich dowodów formalnych. *Jednolita równoważność* teorii oznacza zachowanie podobieństwa dowodów, tzn formuły dowodliwe podobnie (krótko) w jednej teorii muszą posiadać podobne (krótkie) dowody w drugiej. Dla tej mocniejszej równoważności nie zachowają swą ważność klasyczne twierdzenia dotyczące wprowadzania nowych liter funkcyjnych. Przykładowo, PA nie jest jednolicie równoważna swej monadycznej wersji PA^*, wprowadzonej przez Parikha [1973], w której funkcyjne symbole $+$ oraz $\times$ są zastąpione literami relacyjnymi $P^+(x, y, z)$ oraz $P^\times(x, y, z)$ (reprezentującymi, odpowiednio, $x + y = z$ oraz $x \times y = z$) wraz z naturalną translacją aksjomatów $(Ax3)$ – $(Ax6)$.

2. Hipoteza Kreisla (HK), w sformułowaniu z pracy H.Friedmanna [1975] – problem 34, dotyczy wyjściowej teorii PA języka $\{0, S, +, \times, =\}$ i brzmi

> *niech $A(x)$ będzie dowolną arytmetyczną formułą oraz niech k będzie liczbą naturalą; jeżeli (Arytmetyka) Peano dowodzi $A(S^n 0)$ w co najwyżej k krokach dla każdego n, to PA dowodzi także $\forall_x A(x)$.*

Liczebniki $S^n 0$ kanonicznie reprezentują w PA liczby naturalne i niektórzy dopatrują się w wypowiedzi hipotezy pewnej wersji tzw. ω-reguły Mostowskiego. Rzeczywiście, gdyby zastąpić w (HK) dowodliwość w k krokach zwykłą dowodliwością to otrzymamy po opuszczeniu zbędnego kwantyfikatora:

$$PA \vdash A(S^n 0) \text{ dla każdego } n \quad \Rightarrow \quad PA \vdash \forall_x A(x),$$

czyli warunek dopuszczalności ω-reguły w PA. Jedna z wersji twierdzenie Gödla o niezupełności arytmetyki mówi, że powyższa implikacja jest fałszywa dla relatywnie prostej (z logicznego punktu widzenia) formuły $A(x)$. Mianowicie dla obalenia tej implikacji wystarczają Δ_0 formuły, tzn. formuły zawierająca wyłącznie (symbole specyficzne, zmienne, spójniki zdaniowe i) ograniczone kwantyfikatory $\forall_{x \leq y}$ oraz $\exists_{x \leq y}$. Wykorzystując twierdzenie Matyjasiewicza (rozwiązanie X-tego problemu Hilberta) jako kontrprzykład można zaproponować formułę $A(x)$ postaci $\exists_{\overline{y}} p_1(\overline{y}, x) = p_2(\overline{y}, x)$ gdzie $p_i(\overline{y}, x)$ są termami języka. Formułę tę można interpretować jako stwierdzenie, że istnieje pierwiastek naturalny pewnego wielomianu o współczynnikach całkowitych z parametrami.

Relacja dowodliwości w k krokach (tzw. k-dowodliwość) okazuje się więc istotnym składnikiem (HK). Zauważmy, że niedopuszczalność reguły Mostowskiego nie była nigdy uzależniana od wyboru aksjomatyki PA. Dodając regułę do jakiejkolwiek teorii równoważnej (tradycyjnie) PA otrzymujemy teorię zupełną, a więc nie posiadającą rekurencyjnej aksjomatyki.

Tymczasem dołączając (lub odejmując) do aksjomatyki teorii dodatkowe postulaty możemy skracać (lub wydłużać) dowody. Nie ma powodów aby wierzyć, że powyższe zmiany nie wpłyną na prawdziwość hipotezy. Jedynie dla teorii jednolicie równoważnych prawdziwość hipotezy będzie niezmiennicza. Zauważmy bowiem, że niezmienniczość hipotezy Kreisla wymaga aby, k-dowodliwe formuły jednej teorii były l-dowodliwe w drugiej, gdzie liczby k i l niekoniecznie muszą być identyczne. Ponieważ w grę wchodzi jednak dowodliwość nieskończonego zbioru formuł powyższy warunek nie będzie gwarantowany przez tradycyjną równoważność teorii. Możemy rozszerzać hipotezę Kreisla na inne teorie, nie tylko PA, i wcale nie musi dotyczyć ona systemów arytmetycznych. Okazuje się, że odpowiedź na postawione pytanie w nikłym stopniu zależy od tego czy teoria ma sens arytmetyczny. Wszystko to czyni podobieństwa (HK) do postulatu dopuszczalności ω-reguły pozornymi i mylącymi.

Pierwszą znaczącą odpowiedź na formułowane powyżej pytanie dostarczył Parikh [1973], który wykazał prawdziwość hipotezy dla $PA^\star$, monadycznego wariantu Arytmetyki Peano. Skończenie aksjomatyzowalne fragmenty PA także okazały się spełniać hipotezę, Krajíček i Pudlák [1988]. Pozytywne rozwiązania hipotezy dla oryginalnego systemu PA oraz OA zawierają preprinty M.Baaz'a [1989] i [1991]. Znane są także warianty PA, dla których hipoteza jest fałszywa. W każdym z rozważanych przypadków uzasadnienie odpowiedniego rezultatu wymagało jednak użycia specyficznej argumentacji i wciąż brakuje jasności co do tego od jakich parametrów formalnych aksjomatyki prawdziwość hipotezy zależy.

3. Pochodzenie (HK) jest niejasne i sam G.Kreisel wypiera się, że kiedykolwiek w powyższy sposób hipotezę formułował, por. Kreisel [1993]. Jego krytyka dotyczy po pierwsze pojęcia k-dowodliwości, tzn. dowodliwości w co najwyżej k-krokach. Wprowadzając to pojęcie zakłada się bowiem, że istnieje jakiś kanoniczny sposób liczenia długości dowodu i parametr ten jest na tyle ważny w praktyce, że można uważać go za wiarygodną miarę złożoności dowodów. Trudno jednak poglądu tego bronić. Najczęściej jako liczbę kroków w dowodzie przyjmuje się liczbę występujących w nim formuł (lub sekwentów). W ewidentny sposób miara ta zależy jednak od stylów dowodowych; zasadniczo odmienne liczby uzyskamy dla dowodów definiowanych jako drzewa, niż dla ciągów gdzie każda formuła może być użyta wiele razy jako przesłanka inferencji. Zmiana stylu dowodowego prowadzi do odmiennych rezultatów dotyczących choćby rozstrzygalności pojęcia k-dowodliwości. Dodatkowo, miara złożoności definiowana jako liczba formuł w dowodzie nie bierze pod uwagę złożoności formuł tam występujących. Łatwo wyobrazić sobie sytuację gdy długie dowody stają się krótsze dzięki znacznemu zwiększeniu długości formuł. Jeżeli za miarę złożoności przyjąć natomiast liczbę wszystkich znaków występujących w dowodzie, to (HK) trywializuje się: założenie, że $A(S^n 0)$ posiada dowód miary co najwyżej k dla każdego n oznacza bowiem wtedy, że zmienna x nie może w ogóle wystąpić w formule $A(x)$. Zdaniem G.Kreisla nieuzasadniona jest wiara, że złożoność dowodów można (i należy) opisywać liczbami naturalnymi. Lepszym podejściem jest, po pierwsze, próba formalnego opisania podobieństwa dowodów. Dowodzenie przez analogię, najbardziej rozpowszechniony sposób uzasadniania twierdzeń i poglądów (obecny także w matematyce) nie jest w ogóle reprezentowany w logice. Nie przesądzając jak podobieństwa mają wyglądać można rozważyć kilka ich wariantów i testować je w praktyce. Zapewne podobne dowody powinny mieć taką samą miarę złożoności, a więc być równocześnie długie lub krótkie; nie oznacza to jednak, że dowody podobne koniecznie muszą liczyć tyle samo formuł. Mając zdefiniowane relacje podobieństwa, a zatem także ich klasy abstrakcji – typy dowodowe, można następnie przeformułować (HK) przyjmując w założeniu hipotezy, że dowody wszystkich formuł $A(S^n 0)$ są podobne. Liczby jako miary długości dowodów mogą się ujawnić wtórnie jako parametry wyznaczane przez dany typ dowodowy.

Drugim powodem dla którego Kreisel odrzuca sformułowanie (HK) jest fakt, że założenie hipotezy zawiera nieskończenie wiele przesłanek. Dysponując nieskończoną liczbą dowodów mamy skonstruować jeszcze jeden dowód, ale ogólniejszy. Założenia tego typu trudne są do pełnego wykorzystania. W praktyce dowód ogólniejszego twierdzenia otrzymujemy uogólniając jeden z dowodów danych (lub wykorzystując ich skończoną liczbę). Sensowne wydaje się więc wzmocnienie hipotezy, w którym dodatkowo oderwiemy się mylącej analogii sugerującej, że liczebniki są wszystkimi elementami naszego uniwersum. Najprostszą postacią uogólniania twierdzeń będzie zatem, dla ustalonej teorii T języka z S oraz 0:

$$(BM) \qquad T \vdash A(S^n 0) \text{ oraz } n \text{ jest dostatecznie duże } \Rightarrow T \vdash A(S^n x).$$

„Dostatecznie duże" oznacza oczywiście, że liczba n jest dostatecznie duża wzg. długości dowodu i długości formuły $A(x)$, tzn $n > f(l(\pi), l(A))$ gdzie f jest funkcją rekurencyjną oraz $l(\pi)$ jest liczbowo wyrażoną długością dowodu π formuły $A(S^n 0)$ oraz $l(A)$ jest liczbową miarą złożoności formuły $A(x)$. Zauważmy że (BM) implikuje (HK) (przeformułowanej dla dowolnej teorii T) jeżeli założymy, iż rozważana teoria jest systemem arytmetyki, a więc

$$T \vdash x = 0 \vee \ldots \vee x = S^{n-1}0 \vee x \geq S^n 0, \qquad \text{dla każdego } n.$$

W rezultacie dowodliwość ogólnego twierdzenia $\forall_x A(x)$ wynika z dowodliwości (w ograniczonej liczbie kroków) skończnej liczby jego szczególnych przypadków. Dla arytmetycznego systemu spełniającego (BM) otrzymujemy zatem dowód finitarnej wersji Hipotezy Kreisla. Hipotezę (BM) może dotyczyć dowolnego systemu gdzie S jest dowolną monadyczną operacją. Nawet w przypadku logiki jej zachodzenie, lub niezachodzenie, nie jest oczywiste. Hipotezę można poddawać dalszym uogólnieniom przyjmując choćby jakikolwiek długi term t zamiast S^n0 w założeniu i otrzymując w konkluzji dowód $A(t')$ dla t' krótszego i ogólniejszego (tzn. takiego, że t jest podstawieniem t'). Rozważana tu forma uogólnień nie jest jedyna (tylko najprostsza). Można sobie wyobrazić sytuację, która ma właśnie miejsce w przypadku PA^*, gdzie krótki dowód $A(S^n0)$ nie pozwala na uogólnienia postaci $A(S^n x)$, ale uogólnia się, przykładowo, jako $x =_r S^n0 \to A(x)$ dla pewnego r. Proponowana w (BM) forma uogólnień ma oczywiste odwołanie historyczne do *Babilońskiej Matematyki*. Uważa się nie bez racji, że matematyka jako nauka powstała w starożytnej Grecji. Pewne umiejętności matematyczne znane są jednak z okresu wcześniejszej kultury babilońskiej. Zachowały się obliczenia, przykładowo pól figur, gdzie nie podano ogólnego wzoru ale pokazano na konkretnych (kilku kolejnych) liczbach jak te obliczenia przeprowadzać. Oczywiście w każdym przypadku obliczenia podpadały pod ten sam schemat i uogólniały się na kolejne liczby. Zatem teksty te moża intepretować jako próby użycia dużych liczb naturalnych w charakterze zmiennych. Stąd teoria T spełniające (BM) będzie nazywana Babilońską Matematyką.

4. Nie trzeba chyba dodawać, że (BM) przypomina schemat niezupełnej indukcji, której użycie w matematyce jest surowo zakazane. Tym niemniej okazuje się, że pewne standardowe teorie arytmetyczne mogą spełniać tę hipotezę.

Twierdzenie 1. *(i) PA nie jest Babilońską Matematyką;*
(ii) OA jest Babilońską Matematyką.

Udowodnienie negatywnego rezultatu jest, jak zazwyczaj, łatwiejsze choć niebanalne – o czym przekonuje choćby *(ii)*. Posługując się indukcją następnikową, wykażemy że, że $S^n0 + x = S^n x$ jest jednolicie (tzn. niezależnie od n) dowodliwe. Otóż, jeżeli $x = 0$, to $S^n0+0 = S^n0$ na podstawie $(Ax3)$; a w kroku indukcyjnym $S^n Sx = SS^n x = S(S^n0 + x) = S^n0 + Sx$ dzięki $(Ax4)$ i założeniu indukcyjnemu. Stąd $S^n0 + S^m0 = S^{n+m}0$ a zatem także $\exists_y(y + y = S^{2n}0)$ dla dowolnego n. Przyjmując $\exists_y(y + y = x)$ jako $A(x)$ otrzymujemy dowód, w ograniczonej liczbie kroków, formuły $A(S^n0)$ dla dowolnej liczby parzystej n. Możemy zatem znaleźć „dowolnie dużą” liczbę n taką, iż $A(S^n 0)$ będzie dowodliwe w ograniczonej liczbie kroków, bez możliwości dowiedzenia $A(S^n x)$. Z powyższej argumentacji wynika ponadto, że tabliczka dodawania $S^n 0 + S^m 0 = S^{n+m} 0$ jest jednolicie dowodliwa w *PA*. Dodawanie i mnożenie nie wykazują symetrii gdyż

Twierdzenie 2. *Jeżeli hipoteza Kreisla jest spełniona dla niesprzecznego i rekurencyjnie przeliczalnego rozszerzenia T teorii PA, to* $S^n 0 \times S^m 0 = S^{n \times m} 0$ *nie będzie dowodliwa jednolicie w T.*

DOWÓD. Niech $A(x)$ będzie Δ_0 formułą prawdziwą w standardowym modelu liczb naturalnych, ale niedowodliwą w T. Dzięki twierdzeniu Matyjasiewicza istnieją dwa termy $p(x, \overline{y})$ oraz $q(x, \overline{y})$ języka $\{+, \times, S, 0\}$ takie, że $A(x)$ jest równoważna w *PA* formule $\exists_{\overline{y}}(p(x, \overline{y}) = q(x, \overline{y}))$. Zatem $\exists_{\overline{y}}(p(S^n 0, \overline{y}) = q(S^n 0, \overline{y}))$ jest dowodliwa w T dla każdego n gdyż *PA* jest Σ_1-zupełna oraz $A(x)$ jest prawdziwa w standardowym modelu. Dokładniej, dla każdego n istnieje $\overline{m}$ takie, że $p(S^n 0, S^{m_p} 0 \ldots S^{m_1} 0) = q(S^n 0, S^{m_p} 0 \ldots S^{m_1} 0)$ jest dowodliwe w T. Gdyby tabliczka mnożenia była jednolicie dowodliwa w T, wtedy mielibyśmy ograniczenie na długość dowodu $\exists_{\overline{y}} p(S^n 0, \overline{y}) = q(S^n 0, \overline{y})$, które nie zależałoby od n. Zatem otrzymalibyśmy dowody $A(S^n 0)$ dla każdego n, w ograniczonej liczbie kroków, a więc dzięki Hipotezie Kreisla $T \vdash \forall_x A(x)$ przecząc założeniom. ∎

Ponieważ wiemy, że (HK) zachodzi dla *PA*, to na podstawie powyższego twierdzenia $S^n 0 \times S^m 0 = S^{n \times m} 0$ nie będzie jednolicie dowodliwa w *PA*. Kluczową dla jednolitego dowodu $S^n 0 + S^m 0 = S^{n+m} 0$ jest tożsamość $S^n S x = S S^n x$. Brak symetrii między dodawanie i mnożeniem wynika z braku analogicznej tożsamości reprezentującej mnożenie. Powyższe twierdzenie może być użyte do konstrukcji wersji *PA*, w której (HK) nie jest spełniona: wystarczy dołączyć do aksjomatyki *PA* tabliczkę mnożenia jako dodatkowy schemat aksjomatyczny.

5. Niech LK oznacza logikę predykatów w standardowej formalizacji. Można podać przykład formuły $A(x)$ i liczby k takich, że $LK \vdash^k A(S^n 0)$ dla każdego n, ale nie jest prawdą, że $LK \vdash^k A(S^n x)$. Innymi słowy, zastępując w dowodzie formuły $A(S^n 0)$ term $S^n 0$ przez ogólniejszy term $S^n x$, nie otrzymamy wcale dowodu formuły $A(S^n x)$. Termy postaci $S^n 0$ są wyrażeniami złożonymi, a więc klasyczne twierdzenia o niewyróżnianiu stałych w logice, nie mają w tym przypadku zastosowania. Pomimo wszystko dowodzi się

Twierdzenie 3. *LK jest Babilońską Matematyką.*

Aby to wykazać należy określić transformacje, pozwalającą przekształcić dowód $A(S^n0)$ dla dostatecznie dużego n w dowód $A(S^n x)$. Wiemy już, że proste zastąpienie 0 przez zmienną (wewnątrz dużego termu) nie jest poprawną operacją. Trasformacji dostarczają „wielkie" twierdzenia logiczne tj. twierdzenie o eliminacji cięcia lub twierdzenie Herbranda. Można zastosować je także celem wykazania (BM) dla dowolnego skończonego rozszerzenia LK. Transformacje te zawodzą w przypadku rozszerzeń schematami aksjomatów, jak choćby (SI). Na problemy napotykamy nawet w przypadku LK_e będącej rozszerzeniem LK schematem

$$(ES) \qquad s = t \;\rightarrow\; r(s) = r(t)$$

i skończoną liczbą aksjomatów wyrażających podstawowe własności $=$. Oczywiście logikę predykatów z identycznością można opisać skończoną liczbą aksjomatów (w języku ze skończoną liczbą liter funkcyjnych i relacyjnych). Taka teoria będzie Babilońską Matematyką na podstawie twierdzenia 3, będzie także teorią tradycyjnie równoważną LK_e. Nie będzie jednak jej jednolicie równoważna gdyż

Twierdzenie 4. *LK_e nie jest Babilońską Matematyką.*

Dla dowodu wystarczy rozważyć $0 = S0 \rightarrow x = Sx$ jako formułę $A(x)$. Oczywiste jest, że $A(S^n x)$ nie jest tezą LK_e dla żadnego n mimo, iż $LK_e \vdash^1 A(S^n0)$ dla każdego n. Hipoteza (BM) jest jednak bardzo niestabilna. Zauważmy, że rozważana tutaj formuła $A(x)$ jest arytmetycznie prawdziwa, a więc nie da się jej wykorzystać do negatywnego rozstrzygnięcia hipotezy w arytmetycznych rozszerzeniach LK_e. Co więcej, dla arytmetycznych teorii mamy

Twierdzenie 5. *Teoria powstająca z LK_e przez dołączenie aksjomatów PA^- w monadycznym języku (tj. języku gdzie dodawanie i mnożenia są reprezentowane przez predykaty) jest Babilońską Matematyką.*

Hipoteza (BM) pozostaje nierozstrzygnięta dla $LK_e \cup PA^-$ w pełnym języku arytmetycznym z dodawaniem i mnożeniem jako funkcjami.

6. Założenie, że język jest monadyczny tzn. nie zawiera dwu-(lub więcej) arnej litery funkcyjnej, może być istotne o czym świadczy choćby

Twierdzenie 6. *$LK_e \cup \{\forall_x\, x = Sx\}$ jest Babilońską Matematyką w monadycznym języku; natomiast teoria ta nie będzie Babilońską Matematyką w języku z dwuargumentową literą funkcyjną.*

Udowodnimy jedynie rezultat negatywny. Niech $+$ będzie dwuargumentową literą naszego języka. Rozważmy rozszerzenie LK_e formułami $a + b = a \to b = 0$ oraz $0 + 0 = 0$. W teorii tej wykażemy jednolicie:

$$S(0) = 0 \to S^n(0) = 0, \qquad \text{dla każdego } n.$$

Niech $t_0(a, b) = a$ oraz $t_{n+1}(a, b) = t_n(a, b) + S^n(b)$. Zauważmy następnie, że termy $t_n(0, 0) + S^n(0)$ oraz $t_n(0 + 0, S(0))$ są identyczne. Zatem, dzięki (ES),

$$0 + 0 = 0 \land S(0) = 0 \to t_n(0, 0) + S^n(0) = t_n(0, 0)$$

co kończy dowód naszej formuły. Okazuje się zatem, że

$$0 + 0 = 0 \land \forall_{xy}(x + y = x \to y = 0) \to S^n(0) = 0$$

posiadają jednolite dowody w $LK_e \cup \{\forall_x\, x = Sx\}$, dla wszystkich n. W teorii tej nie można jednak dowieść żadnego ogólniejszego twierdzenie postaci

$$0 + 0 = 0 \land \forall_{xy}(x + y = x \to y = 0) \to S^n(x) = 0.$$

W powyższej argumentacji nie trzeba zakładać, że S jest literą funkcyjną, Może to być dowolny term jednej zmiennej. W ten sposób można więc wykazać, jeżeli weźmiemy $a+0$ jako $S(a)$, że $0+\cdots+0 = 0$ są jednolicie dowodliwe w $PA^- \cup (ES)$. Nie istnieje jednak jednolita krótka translacja tych dowodów w monadycznej wersji teorii. Uogólnianie twierdzeń w postaci zaproponowanej m.in. przez (BM) nie jest zatem możliwe w żadnym niesprzecznym rozszerzeniu PA^- schematem ES gdyż $a + 0 + \ldots + 0 = 0$ nie może być tezą takiej teorii. Otrzymamy więc krótkie dowody $A(t)$ dla dowolnie długiego termu t bez możliwości uzasadnienia $A(t')$ dla krótszego i ogólniejszego termu t'.

Zajmując się problematyką uogólniania dowodów, należy jako bazowy przyjąć podział na teorie monadyczne i niemonadyczne. Nie odgrywa tutaj roli liczba i arność liter relacyjnych, liczą się tylko litery funkcyjne. Należy nadto brać pod uwagę to czy teoria posiada skończony zbiór aksjomatów, czy też aksjomatyzowalna jest schematami. Nie jest wogóle ważne, czy rozważana teoria jest logiką, czy też opisuje jakiś model, a więc centralne dla logiki pojęcia zupełności i pełności nie mają dla poruszanych zagadnień znaczenia.

7. Zastanawiać się można w jaki sposób wykazano Hipotezę Kreisla dla teorii, które nie spełniają warunku (BM). Otóż, Parikh [1973] wykazał hipotezę dla monadycznej wersji $PA^{\star}$ wykorzystując w tym celu zasadę refleksji:

$$Prov_k(\ulcorner A \urcorner) \longrightarrow A$$

gdzie $Prov_k$ reprezentuje w arytmetyce predykat dowodliwości w k krokach. Powyższa zasada refleksji jest dowodliwa w PA, i różnych fragmentach, wersjach i rozszerzeniach wyjściowego systemu (nie odgrywa tu roli monadyczność języka). Zauważmy, że mocniejsza zasada refleksji $Prov(\ulcorner A \urcorner) \longrightarrow A$ jest, wobec twierdzenia Löba, dowodliwa tylko gdy A posiada dowód. Zdefiniujemy następnie dla dowolnej formuły $A(x)$ oraz liczby k zbiór „rozwiązań":

$$(*) \qquad n \in X(k, A) \quad \text{wtedy i tylko, gdy} \quad \vdash^k A(S^n 0).$$

Zakładamy, że ustalona została teoria (może to być $PA^{\star}$, choć nie ma to specjalnego znaczenia dla argumentacji) i do niej odnosi się $\vdash^k$. W przypadku gdy $\{0, S\}$ są jedynymi literami funkcyjnymi języka, zbiór $X(k, A)$ otrzymuje się się jako zbiór rozwiązań układu liniowych równań diofantycznych (z parametrami). W monadycznym przypadku z kilkoma literami funkcyjnymi pojawiają się parametryczne równania słów w wolnych półgrupach. W języku z binarną literą funkcyjną, dowolny zbiór rekurencyjnie przeliczalny można otrzymać jako $X(k, A)$. Obok hipotezy Kreisla w cytowanych poniżej pracach, rozważana jest także kwestia rozstrzygalności dowodliwości w k-krokach. Zauważmy, że reprezentacja predykatu $n \in X(k, A)$ w języku teorii równań liniowych (lub problemu słów) pociąga rozstrzygalność predykatu. Natomiast k dowodliwość w języku z binarną literą funkcyjną okazuje się nie być rozstrzygalna, Buss [1991]. Kwestie rozstrzygalności k dowodliwości nie mają jednak wiele wspólnego z usasadnieniem Hipotezy Kreisla. Dalej zakładać będziemy, że $x \in X(k, A)$ wyrażone jest formułą języka Arytmetyki Presburgera. Dowód formalny $(*)$ będzie na tyle elementarny, że daje się go przeprowadzić w rozważanej teorii (a więc $PA^{\star}$). Zatem

$$x \in X(k, A) \rightarrow Prov_k(x).$$

otrzymamy jako tezę teorii, a stąd na podstawie zasady refleksji

$$x \in X(k, A) \rightarrow A(x).$$

Ponieważ założenia (HK) gwarantują nam prawdziwość $x \in X(k, A)$, to otrzymamy $A(x)$ o ile tylko teoria jest zupełna względem arytmetyki Presburgera. Kończy to dowód hipotezy w rozważanym przypadku. Zauważmy, że monadyczność języka była nam potrzebna do wykazania $x \in X(k, A)$.

Być może prawdziwość tej formuły implikuje jej dowodliwość także w przypadku niemonadycznym, choć nie udało się tego nikomu uzasadnić. Dowód Hipotezy Kreisla dla PA w standardowym języku, Baaz [1991], przebiega inaczej i wykorzystuje ε-rachunek Hilberta.

8. Wiemy, że rozwiązania układu liniowych równań diofantycznych z jedną zmienną przyjmują postać postępu arytmetycznego. Zatem $(*)$, po zastosowaniu zasady refleksji daje to nam w monadycznym przypadku:

Twierdzenie 7. *Jeżeli $A(S^n0)$ jest dowodliwe w k krokach oraz n jest wystarczająco duże (względem k oraz formuły $A(x)$), to następująca formuła jest dowodliwa dla pewnych r oraz m, które nie są już duże:*

$$x =_r S^n0 \wedge x \geq S^m0 \to A(x).$$

Zatem zamiast uogólniania w postaci (BM) otrzymujemy uogólnianie twierdzeń w postaci postępu arytmetycznego. W powyższy sposób formułował Kreisel [1987] wzmocnioną wersję (HK). Jako prosty wniosek z powyższego twierdzenia otrzymamy następującą finitarną postać (HK).

Wniosek 8. *Niech T będzie monadyczną teorią zupełną ze względu na Arytmetykę Presburgera oraz niech n będzie dostatecznie duże względem $A(a)$ oraz k. Jeżeli $\vdash^k A(S^m0)$ dla każdego $m \leq n!$, to $\vdash \forall_x A(x)$.*

Podobna postać uogólniania twierdzeń zachodzić będzie dla formuł wielu zmiennych i uzasadnimy $\forall_{x_1 \ldots x_p} A(x_1, \ldots, x_p)$ wykorzystując k-dowodliwość skończenie wielu jej szczególnych przypadków. Uogólnianie dowodów dla formuł wielu zmiennych przyjmuje jednak bardziej skomplikowaną formę niż

$$n_1 =_{r_1} x_1 \wedge \ldots \wedge n_p =_{r_p} x_p \to A(x_1 \ldots x_p).$$

Literatura

[1] Baaz M., *Generalization of proofs with order induction*, preprint, 1989; *Generalizing proofs with successor induction*, preprint, 1991.

[2] Baaz M. and Wojtylak P.,*Generalizing proofs in monadic languages.*

[3] Buss S.R., *The undecidability of k-provability*, Annals of Pure and Applied Logic 53 (1991), pp. 75-102.

[4] Krajíček J., Pudlák P., *The number of proof lines and size of proofs in first order logic*, Archive for Mathematical Logic 27 (1988), pp. 69-84.

[5] Kreisel G.,*Proof theory: some personal recollections*, Appendix to G.Takeuti, *Proof theory* 2nd ed., North-Holland 1987, 397-407.

[6] Parikh R.J.,*Some results on the length of proofs*, TAMS 117 (1973), 29-36.