Automorfizmy modeli
i twierdzenie Ehrenfeuchta—Mostowskiego

Krzysztof Kapulkin

IX Warsztaty Logiczne
5 – 12 lipca 2008

1 Wstęp

W referacie tym przedstawiamy wyniki uzyskane przez Andrzeja Ehrenfeuchta i Andrzeja Mostowskiego i zaprezentowane w [EM].
Wprowadźmy następujące oznaczenia:
$\mathbb{A} = \langle A, \ldots \rangle$—model
$\equiv$—elementarna równoważność modeli
$\cong$—izomorfizm modeli
$Fm(\mathcal{L})$—zbiór formuł języka $\mathcal{L}$

2 Podstawowe pojęcia i twierdzenia logiki

Definicja 1. $\mathbb{A}$ będziemy nazywać *elementarnym podsystemem* $\mathbb{B}$, jeśli

i. $A \subset B$

ii. dla dowolnej formuły $\alpha(x_1, \ldots, x_n)$ oraz dla dowolnych $a_1, \ldots, a_n \in A$ zachodzi: $\mathbb{A} \models \alpha[a_1, \ldots, a_n]$ wtedy i tylko wtedy, gdy $\mathbb{B} \models \alpha[a_1, \ldots, a_n]$.

Twierdzenie 1. (Kryterium Tarskiego—Vaughta) *Niech $\mathbb{A}$ - podsystem $\mathbb{B}$. Jeśli dla dowolnej formuły α, wartościowania p oraz zmiennej x mamy, że $\mathbb{B} \models \exists x\ \alpha[p]$ implikuje, że istnieje $a \in A$ takie, że $\mathbb{B} \models \alpha[p(a/x)]$, to $\mathbb{A}$ jest elementarnym podsystemem $\mathbb{B}$.*

Dowód. Indukcja względem budowy formuły α.
Gdy α jest formułą atomową—rutyna.
Kroki spójników—rutyna.
Krok kwantyfikatora $\exists$. Niech $\alpha = \alpha(x, x_1, \ldots, x_n)$. Załóżmy na początek, że $\mathbb{A} \models \exists x\ \alpha[a_1, \ldots, a_n]$. Stąd istnieje $a \in A$ takie, że $\mathbb{A} \models \alpha[a/x, a_1, \ldots, a_n]$. Z założenia indukcyjnego: $\mathbb{A} \models \alpha[a/x, a_1, \ldots, a_n]$ wtedy i tylko wtedy, gdy $\mathbb{B} \models \alpha[a/x, a_1, \ldots, a_n]$. Zatem $\mathbb{B} \models \exists x\ \alpha[a_1, \ldots, a_n]$ (świadek a). Na odwrót: załóżmy, że $\mathbb{B} \models \exists x\ \alpha[a_1, \ldots, a_n]$. Z założeń kryterium mamy, że istnieje $a \in A$ takie, że $\mathbb{B} \models \alpha[a, a_1, \ldots, a_n]$. Zatem na mocy założenia indukcyjnego: $\mathbb{A} \models \alpha[a, a_1, \ldots, a_n]$ □

Definicja 2. Niech $\alpha = \alpha(x, x_1, \ldots, x_n)$ będzie formułą języka $\mathcal{L}$ oraz $\mathbb{A}$—modelem, $x, x_1, \ldots, x_n \in FV(\alpha)$. Określamy *funkcję Skolema* $f_{\alpha,x} : A^n \to A$ jako funkcję wyboru dla rodziny $\{P_{a_1,\ldots,a_n} : a_i \in A\}$, gdzie $P_{a_1,\ldots,a_n} = \{a \in A : \mathbb{A} \models \alpha[a/x, a_1/x_1, \ldots, a_n/x_n]\}$.

Fakt 1. *Jeśli* $\mathbb{A} \models \exists x\ \alpha[a_1, \ldots, a_n]$, *to* $\mathbb{A} \models \alpha[f_{\alpha,x}(a_1, \ldots, a_n)/x, a_1, \ldots, a_n]$.

Definicja 3. *Domknięciem Skolema* $X \subset A$ (ozn. X^*) nazywamy najmniejszy podzbiór A zamknięty na wszystkie funkcje Skolema.

Stwierdzenie 1. *Dla dowolnego zbioru* $X \subset A$ *jego domknięcie Skolema* X^* *jest elementarnym podsystemem* $\mathbb{A}$.

Dowód. Najpierw pokażemy, że X^* jest podsystemem systemu $\mathbb{A}$. Stałe należą do domknięcia Skolema (wystarczy rozważyć formuły postaci: $x = c$ dla c—stała). Ponadto X^* jest zamknięty na operacje (rozważamy formuły $x = f(x_1, \ldots, x_n)$ dla f - symbolu relacyjnego).
Aby pokazać, że jest to podsystem elementarny, stosujemy kryterium Tarskiego—Vaughta. Jeśli $\mathbb{A} \models \exists x\ \alpha[a_1, \ldots, a_n]$, gdzie $a_1, \ldots, a_n \in X^*$, to istnieje $a \in X^*$ takie, że $\mathbb{A} \models \alpha[a/x, a_1, \ldots, a_n]$, mianowicie: $a = f_{\alpha,x}(a_1, \ldots, a_n)$. □

Definicja 4. Powiemy, że teoria T w języku $\mathcal{L}$ jest ma *wbudowane funkcje Skolema*, jeśli dla dowolnej formuły $\psi = \exists x\ \varphi(x_1, \ldots, x_n)$, gdzie $x_1, \ldots, x_n$ wszystkie zmienne wolne formuły φ, istnieje term $t_\psi(y_1, \ldots, y_n)$ języka $\mathcal{L}$ taki, że:

$$T \vdash \forall y_1, \ldots, y_n(\psi(y_1, \ldots, y_n) \rightarrow \varphi(t_\psi(y_1, \ldots, y_n), y_1, \ldots, y_n)).$$

Możemy więc powiedzieć, że teoria ma wbudowane funkcje Skolema wtedy i tylko wtedy, gdy są one definiowalne w jej języku.

Definicja 5. Niech dane będą typy: $\tau = \langle \tau_1, \tau_2, \tau_3 \rangle$ oraz $\sigma = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$. Typ τ nazwiemy *reduktem typu* σ, jeśli funkcje σ_i są rozszerzeniami funkcji τ_i.
Niech $\mathbb{A}$ będzie systemem typu σ. Odrzucając relacje, funkcje i elementy wyróżnione nie objęte typem τ otrzymujemy system będący *reduktem systemu* $\mathbb{A}$.
Niech $\mathcal{L}$ będzie językiem typu σ. Odrzucając symbole relacyjne i funkcyjne oraz oraz stałe nie objęte typem τ otrzymujemy język będący *reduktem języka* $\mathcal{L}$.

3 Twierdzenie Ramsey'a

Twierdzenie 2. **(Ramsey, wersja nieskończona)** *Niech* S *będzie zbiorem oraz* $n \in \mathbb{N}$. *Niech ponadto* $\mathcal{P}_n(S)$*—zbiór wszystkich* n*-elementowych podzbiorów zbioru* S. *Wówczas jeśli* $\mathcal{P}_n(S) = A_1 \cup A_2$ *(suma rozłączna), to istnieje* S_0 *taki, że albo* $\mathcal{P}_n(S_0) \subset A_1$, *albo* $\mathcal{P}_n(S_0) \subset A_1$.

Dowód. Dowód przeprowadzimy przez indukcję ze względu na n.
Gdy $n = 1$, twierdzenie sprowadza się do faktu, że jeśli A_1, A_2 stanowią podział zbioru nieskończonego, to jeden z nich musi być nieskończony.
Załóżmy więc, że twierdzenie zachodzi dla $n \leq r$. Pokażemy, że zachodzi również dla $n = r + 1$. Ustalmy $s_0 \in S$ i niech $Y = S \setminus \{s_0\}$. Podział $\mathcal{P}_{r+1}(S) = A_1 \cup A_2$ indukuje podział $\mathcal{P}_r(Y) = A'_1 \cup A'_2$. Mianowicie, niech $X \in \mathcal{P}_r(Y)$, wówczas:

$$X \in A'_i \Leftrightarrow X \cup \{s_0\} \in A_i.$$

Z założenia indukcyjnego istnieje nieskończony $Y_1 \subset Y$ taki, że każdy r-elementowy podzbiór Y_1 należy do ustalonego A'_i. Bez straty ogólności zadania możemy zakładać, że jest to A'_1. Zatem dowolny $(r + 1)$-elementowy podzbiór S, do którego należy s_0 oraz r elementów z Y_1 należy do A_1.
Wybierzmy teraz $s_1 \in Y_1$. Powtarzając poprzednie rozumowanie, mamy, że istnieje taki nieskończony $Y_2 \subset Y_1$, że dowolny $(r + 1)$-elementowy podzbiór S, do którego należy s_1 oraz r elementów z Y_2 należy do pewnego ustalonego A_i.
Powtarzając ten argument ω razy, otrzymujemy zbiór $\{s_0, s_1, s_2, \ldots\}$. Rozważmy teraz jego $(r+1)$-elementowy podzbiór $\{s_{i_1}, s_{i_2}, \ldots, s_{i_{r+1}}\}$, gdzie $i_1 < i_2 < \ldots < i_{r+1}$.

To, do którego elementu podziału $\mathcal{P}_{r+1}(S) = A_1 \cup A_2$ on należy, zależy wyłącznie od i_1. Zatem znajdziemy nieskończenie wiele wartości i_k, że s_{i_k} należą do jednego z elementów podziału.

□

Przedstawiony tu dowód twierdzenia Ramsey'a jest pewną modyfikacją dowodu z [ChK]. Alternatywny, korzystający z lematu Königa, dowód można znaleźć w [LM].

4 Twierdzenie Ehrenfeuchta - Mostowskiego

Definicja 6. Niech $\mathbb{A}$ będzie modelem dla $\mathcal{L}$ oraz niech $X \subset A$ będzie podzbiorem liniowo uporządkowanym przez $<$. Powiemy, że X jest zbiorem elementów *nierozróżnialnych* w $\mathbb{A}$, jeśli dla dowolnego $n \in \mathbb{N}$ oraz $x_1 < x_2 < \ldots < x_n$ i $y_1 < y_2 < \ldots < y_n$, gdzie $x_i, y_i \in X$ zachodzi $(\mathbb{A}, x_1, \ldots, x_n) \equiv (\mathbb{A}, y_1, \ldots, y_n)$.

Intuicyjnie, użyte w powyższej definicji słowo 'nierozróżnialne' oznacza, że ciągów $x_1 < \ldots < x_n$ i $y_1 < \ldots < y_n$ nie jesteśmy w stanie odróżnić za pomocą żadnej formuły logiki 1 rzędu postaci $\varphi(v_1, \ldots, v_n)$ w $\mathcal{L}$.

Stwierdzenie 2. *Niech $\langle X, < \rangle$ będzie liniowo uporządkowanym podzbiorem $\mathbb{A}$. Jeśli dla dowolnych dwóch ciągów: $x_1 < x_2 < \ldots < x_n$ i $y_1 < y_2 < \ldots < y_n$ elementów X istnieje automorfizm $f : \mathbb{A} \to \mathbb{A}$ taki, że $f(x_i) = y_i$ dla $i = 1, 2, \ldots, n$, to X jest zbiorem elementów nierozróżnialnych.*

Dowód. Istotnie, mamy, że $f : (\mathbb{A}, x_1, \ldots, x_n) \cong (\mathbb{A}, y_1, \ldots, y_n)$, czyli $(\mathbb{A}, x_1, \ldots, x_n) \equiv (\mathbb{A}, y_1, \ldots, y_n)$, co kończy dowód. □

Podajmy kilka przykładów zbiorów elementów nierozróżnialnych:

1. $\mathbb{A}$—ciało algebraicznie domknięte, X—zbiór elementów liniowo niezależnych.
2. $\mathbb{A}$—grupa wolna, X—zbiór generatorów.
3. $\mathbb{A}$—zbiór liczb wymiernych $\mathbb{Q}$ z porządkiem liniowym, $X = A$.
4. $\mathbb{A}$—atomowa algebra Boole'a, X—zbiór atomów.
5. $\mathbb{A}$—zbiór z relacją równoważności, X—jedna z klas abstrakcji.
6. $\mathbb{A}$—zbiór wielomianów o współczynnikach w ustalonym pierścieniu R, X—zbiór zmiennych.

Stwierdzenie 3. *Niech $\mathcal{L}' = \mathcal{L} \cup \{c_n : n \in \mathbb{N}\}$ oraz niech T będzie teorią w języku $\mathcal{L}$ mającą model nieskończony. Wówczas teoria $T' = T \cup \{\varphi(c_{i_1}, \ldots, c_{i_n}) \leftrightarrow \varphi(c_{j_1}, \ldots, c_{j_n}) : \varphi(v_1, \ldots, v_n) \in Fm(\mathcal{L}), n \in \mathbb{N}, i_1 < \ldots < i_n, j_1 < \ldots < j_n\} \cup \{\neg c_i = c_j : i \neq j\}$ jest niesprzeczna.*

Dowód. Niech $\mathbb{A}$ będzie nieskończonym modelem T oraz niech $I \subset A$ będzie przeliczalnym podzbiorem dobrze uporządkowanym przez $<$. Niech zatem $i_0 < i_1 < \ldots$ będą wszystkimi elementami I. Udowodnimy następujący lemat:

Lemat 1. *Przy powyższych założeniach, jeśli $\Delta \subset T'$ jest skończony, to istnieje nieskończony podzbiór $J_\Delta \subset I$, że dla dowolnego nieskończonego podzbioru $\{j_0, j_1, \ldots\} \subset J_\Delta$ dobrze uporządkowanego przez $<$ rozszerzenie $(\mathbb{A}, j_0, j_1, \ldots)$ jest modelem dla Δ.*

Dowód. Dowód przeprowadzimy przez indukcję względem liczby zdań w Δ. Załóżmy więc, że teza lematu zachodzi dla pewnego skończonego $\Delta \subset T'$ i niech $\varphi(v_1, \ldots, v_m)$ będzie formułą języka $\mathcal{L}$. Definiujemy podział $\mathcal{P}_m(J_\Delta) = A_1 \cup A_2$ następująco:

$$A_1 = \{x_1 < x_2 < \ldots < x_m : x_i \in J_\Delta, \mathbb{A} \models \varphi[x_1, \ldots, x_m]\}$$

$$A_2 = \{x_1 < x_2 < \ldots < x_m : x_i \in J_\Delta, \mathbb{A} \models \neg\varphi[x_1, \ldots, x_m]\}$$

Z twierdzenia Ramsey'a mamy, że istnieje nieskończony zbiór $K \subset J_\Delta$ taki, że $\mathcal{P}_m(K) \subset A_1$ lub $\mathcal{P}_m(K) \subset A_2$. Niech teraz $k_0 < k_1 < \ldots$ będzie nieskończonym podzbiorem K. Mamy, że $(\mathbb{A}, k_0, k_1, \ldots) \models \varphi(c_{s_1}, \ldots, c_{s_m}) \leftrightarrow \varphi(c_{t_1}, \ldots, c_{t_m})$ dla $s_1 < s_2 < \ldots < s_m$ i $t_1 < t_2 < \ldots < t_m$. Ponadto $(\mathbb{A}, k_0, k_1, \ldots)$ spełnia wszystkie zdania z Δ, co kończy dowód indukcyjny. $\square$

Na mocy udowodnionego właśnie lematu oraz twierdzenia o zwartości otrzymujemy tezę. $\square$

Twierdzenie 3. *Niech T będzie teorią w języku $\mathcal{L}$ z nieskończonymi modelami oraz niech $\langle X, < \rangle$ będzie liniowym porządkiem. Wówczas istnieje model $\mathbb{A}$ teorii T taki, że $X \subset A$ oraz X jest zbiorem elementów nierozróżnialnych w $\mathbb{A}$.*

Dowód. Niech $\mathcal{L}' = \mathcal{L} \cup \{c_x : x \in X\}$ oraz $T' = T \cup \{\varphi(c_{x_1}, \ldots, c_{x_n}) \leftrightarrow \varphi(c_{y_1}, \ldots, c_{y_n}) : \varphi(v_1, \ldots, v_n) \in Fm(\mathcal{L}), n \in \mathbb{N}, x_1 < \ldots < x_n, y_1 < \ldots < y_n\} \cup \{\neg c_x = c_y : x \neq y; x, y \in X\}$. Ponieważ dowolny skończony podzbiór X może być zanurzony (z zachowaniem porządku) w $\langle \omega, < \rangle$, zatem na mocy Stwierdzenia 3 mamy, że T' jest niesprzecznym zbiorem zdań w $\mathcal{L}'$. Niech $\mathbb{A}'$ - model dla T' oraz niech $\mathbb{A}$ będzie obcięciem modelu $\mathbb{A}'$ do $\mathcal{L}$. Wówczas $\mathbb{A}$ jest modelem dla T. Bez straty ogólności zadania możemy utożsamić stałe c_x z elementami $x \in X$. Z definicji teorii T' wynika, że dla dowolnej formuły $\varphi(v_1, \ldots, v_n) \in Fm(\mathcal{L})$ oraz elementów $x_1 < \ldots < x_n$ i $y_1 < \ldots < y_n$ zbioru X zachodzi:

$$\mathbb{A} \models \varphi[x_1, \ldots, x_n] \Leftrightarrow \mathbb{A} \models \varphi[y_1, \ldots, y_n]$$

Zatem $(\mathbb{A}, x_1, \ldots, x_n) \equiv (\mathbb{A}, y_1, \ldots, y_n)$, czyli X jest zbiorem elementów nierozróżnialnych w $\mathbb{A}$. $\square$

Twierdzenie 4. *Niech $\mathbb{A}$ będzie modelem teorii T z wbudowanymi funkcjami Skolema oraz $X \subset A$ będzie zbiorem elementów nierozróżnialnych. Wówczas każda bijekcja $f : X \to X$ zachowująca porządek rozszerza się jednoznacznie do automorfizmu modelu X^*.*

Dowód. T ma wbudowane funkcje Skolema, zatem dowolny element $y \in X^*$ został otrzymany za pomocą termu $t(v_1, \ldots, v_n)$ z $x_1, \ldots, x_n \in X$. Bez straty ogólności możemy założyć, że wszystkimi zmiennymi wolnymi termu t są $v_1, \ldots, v_n$ oraz, że $x_1 < \ldots < x_n$ i $y = t[x_1, \ldots, x_n]$. Takie przedstawienie będziemy nazywać *standardową reprezentacją* y w X^*.
Niech $y = t[x_1, \ldots, x_n]$ będzie standardową reprezentacją oraz niech $f : X \to X$ będzie bijekcją zachowującą porządek (automorfizmem porządkowym). Zdefiniujemy rozszerzenie f do automorfizmu modeli $\tilde{f} : X^* \to X^*$. Zadajemy je wzorem:

$$\tilde{f}(y) = t[f(x_1), \ldots, f(x_n)] \tag{1}$$

Należy zatem pokazać, że:

1. $\tilde{f}$ jest dobrze określone.

2. $\tilde{f}$ jest automorfizmem.

3. $\tilde{f}$ jest jedynym rozszerzeniem f o zadanych własnościach.

Mamy więc:
Ad. 1. Rozważmy inną standardową reprezentację $y = t'[z_1, \ldots, z_m]$. Niech $u_1 < \ldots < u_l$ będzie porządkiem na zbiorze $\{x_1, \ldots, x_n, z_1, \ldots, z_m\}$. Wówczas równość $t[x_1, \ldots, x_n] = t'[z_1, \ldots, z_m]$ można zapisać za pomocą formuły φ jako $X^* \models \varphi[u_1, \ldots, u_l]$. Z założenia $X^* \models \varphi[f(u_1), \ldots, f(u_l)]$. Stąd $t[f(x_1), \ldots, f(x_n)] = t'[f(z_1), \ldots, f(z_m)]$ w X^*, a zatem definicja jest niezależna od wyboru standardowej reprezentacji.
Ad. 2. Fakt, że $\tilde{f}$ jest bijekcją oraz $\tilde{f}$ spełnia odpowiednie równości na symbolach funkcyjnych i stałych wynika bezpośrednio z (1). Wystarczy zatem udowodnić, że $\tilde{f}(X^*)$ jest elementarnym podsystemem X^*. Rozważmy formułę: $\varphi(v_1, \ldots, v_l)$ języka $\mathcal{L}$ taką, że $\tilde{f}(X^*) \models \varphi[y_1, \ldots, y_l]$. Dla każdego z y_i $(i = 1, 2, \ldots, l)$ weźmy jego standardową reprezentację, daną przez term t_i i podzbiór zbioru zmiennych $x_1 < \ldots < x_n$. Ponieważ T ma wbudowane funkcje Skolema, zatem istnieje formuła ψ taka, że:

$$\tilde{f}(X^*) \models \varphi[y_1, \ldots, y_l] \text{ wtedy i tylko wtedy, gdy } X^* \models \psi[x_1, \ldots, x_n].$$

Ad. 3. Pozostawiamy Czytelnikowi w charakterze prostego ćwiczenia. □

Wniosek 1. *Jeśli teoria T ma modele nieskończone, to dla dowolnego liniowo uporządkowanego liniowo zbioru X istnieje taki model $\mathbb{A}_0$ teorii T, że $Aut(\langle X, < \rangle) \subset Aut(\mathbb{A}_0)$.*

Dowód. Zacznijmy od wprowadzenia kilku oznaczeń. Dla danego języka $\mathcal{L}$ przez $\mathcal{L}^*$ będziemy oznaczać najmniejsze rozszerzenie języka $\mathcal{L}$, że ma on wbudowane funkcje Skolema (a zatem umieszczenie odpowiednich symboli wśród symboli funkcyjnych). Niech teraz $\mathbb{A}$ będzie modelem dla języka $\mathcal{L}$. Rozszerzeniem Skolema $\mathbb{A}$ będziemy nazywać taki model $\mathbb{A}^*$, że jeśli $\psi = \exists x\ \varphi(xx_1, \ldots, x_n)$ jest formułą języka $\mathcal{L}^*$ (przy czym $x_1, \ldots, x_n$ - wszystie zmienne wolne w φ) oraz $y_1, \ldots, y_n$ nie występują w ψ, to $\mathbb{A} \models \forall y_1, \ldots, y_n(\psi(y_1, \ldots, y_n) \rightarrow \varphi(f_{\psi,x}(y_1, \ldots, y_n)y_1, \ldots, y_n))$.
Niech $\mathbb{A}$ będzie nieskończonym modelem dla T w języku $\mathcal{L}$. Definiujemy teorię T': jej twierdzeniami są wszystkie zdania języka $\mathcal{L}^* \cup \{c_a : a \in A\}$ prawdziwe w $(\mathbb{A}^*, a)_{a \in A}$. Oczywiście, na mocy powyższej definicji T' ma wbudowane funkcje Skolema, a jej nieskończonym modelem jest $(\mathbb{A}^*, a)_{a \in A}$. Niech teraz X będzie zbiorem elementów nierozróżnialnych w X^*, które jest modelem dla T'. Wówczas redukt X^* do języka $\mathcal{L}$ jest elementarnym rozszerzeniem $\mathbb{A}$ (tzn. $\mathbb{A}$ jest elementarnym podsystemem reduktu X^*). Przyjmujemy $\mathbb{A}_0$ = redukt X^*. □

Literatura

[EM] A. Ehrenfeucht, A. Mostowski: *Models of axiomatic theories admitting automorphisms*, Fundamenta Mathematicae 43 (1956) str. 50-68

[ChK] C. C. Chang, H. Jerome Keisler: *Model Theory*, North-Holland Amsterdam (1973)

[AZ] Z. Adamowicz, P. Zbierski: *Logika matematyczna*, PWN Warszawa (1991)

[LM] W. Lipski, W. Marek: *Analiza kombinatoryczna*, Biblioteka matematyczna tom 59, PWN Warszawa (1986)