

Lista zadań z matematycznych podstaw informatyki nr 6.

Zad. 1. Wykaż następujący lemat: Przypuśćmy, że $\mathcal{A}$ jest strukturą, x – zmienną, s – termem w języku tej struktury, a h – wartościowaniem zmiennych w tej strukturze. Niech h' będzie wartościowaniem zmiennych takim, że $h'(x) = s[h]$ oraz $h'(y) = h(y)$ dla wszystkich zmiennych $y \neq x$. Wtedy mamy

$$t[x \leftarrow s][h] = t[h']$$

dla wszystkich termów t oraz

$$\mathcal{A} \models \varphi[x \leftarrow s][h] \Leftrightarrow \mathcal{A} \models \varphi[h']$$

dla wszystkich formuł φ , w których s jest podstawialny za x .

Zad. 2. (Twierdzenie o poprawności) Pokaż, że twierdzenia teorii T są prawdziwe w każdym modelu teorii T . Właściwie przez indukcję ze względu na pozycję w dowodzie należy pokazać, że wszystkie formuły znajdujące się w jakimkolwiek dowodzie w teorii T są spełnione w dowolnym modelu tej teorii.

Zad. 3. Niech $Z[x]$ oznacza zbiór wielomianów (formalnych) o współczynnikach całkowitych. W tym zbiorze w naturalny sposób określamy dodawanie i mnożenie. Ponadto w zbiorze $Z[x]$ w następujący sposób definiujemy porządek: wielomian $w(x)$ jest dodatni wtedy i tylko wtedy, gdy jest dodatni jego współczynnik przy najwyższej potęgze x występującej w $w(x)$ ze współczynnikiem różnym od 0; wielomian $w_1(x)$ jest mniejszy od wielomianu $w_2(x)$ (zachodzi relacja $w_1(x) < w_2(x)$) wtedy i tylko wtedy, gdy wielomian $w_2(x) - w_1(x)$ jest dodatni. Z algebraicznego punktu widzenia $Z[x]$ jest uporządkowanym pierścieniem. Pokaż, że w zbiorze nieujemnych elementów $Z[x]$ z tak zdefiniowanymi działaniami i porządkiem spełnione są wszystkie aksjomaty teorii Q .

Zad. 4. Niech N_∞ oznacza zbiór $N \cup \{\infty\}$. W tym zbiorze w następujący sposób definiujemy dodawanie i porządek: $m + n$ jest zwykłą sumą, jeżeli $m, n \in N$, $x + \infty = \infty + x = \infty$ w pozostałych przypadkach; $m < n$, jeżeli $m, n \in N$ oraz m jest mniejsze od n w zwykłym sensie, $x < \infty$ dla wszystkich $x \in N_\infty$. Mnożenie i operację następnika definiujemy analogicznie, jak dodawanie. Pokaż, że w zbiorze N_∞ z tak zdefiniowanymi działaniami i porządkiem spełnione są wszystkie aksjomaty teorii Q .

Zad. 5. Rozstrzygnij, które z niżej podanych formuł są prawdziwe przy standardowym rozumieniu liczb naturalnych, a które są dowodliwe w arytmetyce Peano lub teorii Q :

- 1) $x < S(x)$,
- 2) $x \neq S(x)$,
- 3) $\exists y (x = y + y \vee x = S(y + y))$.

Zad. 6. Niech Φ oznacza formułę

$$\exists x \exists y \forall z ((A(x, y) \Rightarrow A(y, z) \wedge A(z, z)) \wedge (A(x, y) \wedge B(x, y) \Rightarrow B(x, z) \wedge B(z, z)))$$

(jest to formuła wykorzystywana do testowania programu Gilmora). Udowodnij, że Φ jest tautologią (prawem logiki). Zrób to wprost oraz korzystając z algorytmu Herbranda.

Zad. 7. Korzystając z algorytmu Herbranda pokaż, że formuła

$$\exists x \forall y R(x, y) \rightarrow \forall y \exists x R(x, y)$$

jest tautologią, natomiast formuła

$$\forall x \exists y R(x, y) \rightarrow \exists y \forall x R(x, y)$$

nie jest. Druga część zadania dzięki twierdzeniu Herbranda sprowadza się do problemu unifikacji.

Zad. 8. Rozważamy formuły bez stałych i symboli funkcyjnych, formuła φ nie zawiera ponadto kwantyfikatorów. Udowodnij, że Zdanie $\exists x_1 \dots \exists x_n \varphi$ jest tautologią wtedy i tylko wtedy, gdy formuła φ jest spełniona przy każdym (jedynym możliwym) wartościowaniu w każdej strukturze o jednoelementowym uniwersum. Jak sprawdzić warunek z prawej strony tej równoważności posługując się metodą zerojedynkową? Zbadaj, czy formuła

$$\exists x \exists y \exists z ((F(x, y) \Rightarrow F(y, z) \wedge F(z, z)) \wedge (F(x, y) \wedge G(x, y) \Rightarrow G(x, z) \wedge G(z, z)))$$

jest tautologią.

Zad. 9. Zmodyfikuj równoważność z poprzedniego zadania tak, aby była prawdziwa dla formuł φ , w których mogą dodatkowo występować stałe.

Zad. 10. Opracuj algorytm, który odpowiada na pytanie, czy zdanie

$$\forall x_1 \dots \forall x_n \exists y_1 \dots \exists y_m \varphi$$

jest tautologią. Zakładamy, że w formule φ nie ma już kwantyfikatorów.

Zad. 11. Przypuśćmy, że formuła φ nie zawiera kwantyfikatorów i zdanie $\exists x \forall y \varphi$ jest tautologią. Podaj dowód tego zdania. Wskazówka. Trudno napisać dowód, ale można korzystając z twierdzenia Herbranda opisać metodę konstruowania dowodu. Taka metoda powinna składać się z dwóch części: z metody konstruowania dowodu tautologii rachunku zdań (na poziomie rachunku zdań) i rozumowania dotyczącego kwantyfikatorów. Pierwsza część powinna być znana z logiki, można też posłużyć się koniunkcyjną postacią, druga część nie jest trudna, zawiera dość oczywiste rozumowanie. Reszta rozumowania to pewien trick. Twierdzenie Herbranda w tym przypadku mówi, że pewna alternatywa postaci $\forall \varphi(t, f(t))$ (f to symbol skolemowski) jest tautologią w sensie rachunku zdań. W tej tautologii, dla kolejnych t wszystkie wystąpienia termu $f(t)$ zastępujemy zmienną. Robimy to tak, aby nie utożsamiać jakichkolwiek dwóch termów w całej alternatywie. Dzięki temu, ta alternatywa po zastąpieniu nadal jest tautologią. Po zamianie wszystkich termów postaci $f(t)$ na zmienne dowodzimy tautologię, a następnie wyprowadzamy z niej wyjściową formułę. W ten sposób z twierdzenia Herbranda wyprowadzamy twierdzenie o pełności, a także otrzymujemy ogólną metodę konstruowania dowodów w rachunku kwantyfikatorów.

Zad. 12. 1) [Jacques Herbrand, 1930] Rozważamy teorię następnika, a więc zapisaną w języku złożonym z trzech symboli pozalogicznych: stałej 0, symbolu funkcyjnego S oraz relacji $=$, złożoną ze zdań w tym języku, prawdziwych w standardowym modelu liczb naturalnych. Wykaż rozstrzygalność teorii następnika, a więc dowiedź istnienie algorytmu pozwalającego na sprawdzenie, czy dane zdanie należy do teorii następnika. **Wskazówka.** Algorytm rozwiązujący to zadanie ma następującą konstrukcję: najpierw sprowadza daną do postaci normalnej, z blokiem kwantyfikatorów na początku formuły. Następnie poprawia tę postać tak, aby ostatni kwantyfikator był egzystencjalny, a bezkwantyfikatorowa część formuły miała alternatywną postać

normalną (wymaga to czasem umieszczenia negacji wśród kwantyfikatorów, ale to nam nie przeszkadza). Teraz kwantyfikator egzystencjalny jest przedstawiany z alternatywą. W rozważanej teorii koniunkcję formuł atomowych i negacji takich formuł, poprzedzoną kwantyfikatorem egzystencjalnym, można zastąpić formułą pozbawioną kwantyfikatorów. Prowadzi to do skrócenia bloku kwantyfikatorów, a po stosownej iteracji postępowania, do zastąpienia danego zdania zdaniem pozbawionym kwantyfikatorów. Prawdziwość tych ostatnich zdań jest łatwo rozstrzygalna.

- 2) Udowodnij, że teoria następnika z (równością oraz) aksjomatami

$$\forall x \forall y S(x) = S(y) \Rightarrow x = y,$$

$$\forall x (\neg S(x) = 0),$$

$$\forall x (x = 0 \vee \exists y x = S(y)),$$

$$\forall x (x = 0 \vee x = S(0) \vee \exists y x = S(S(y))) (? , itd.).$$

jest zupełna.

- 3) Pokaż, że algorytm z pierwszej części zadania jest wielomianowy pod warunkiem, że możemy posłużyć się czarną skrzynką pozwalającą sprowadzić formułę bezkwantyfikatorową do alternatywnej postaci normalnej. Pokaż też, że jest to algorytm NP-trudny.
- 4) (*) Uogólnij dwie pierwsze części zadania tak, by dotyczyły teorii dodawania, w której zamiast następnika S mamy symbol dodawania $+$. Zadanie jest trochę trudniejsze, ale metoda rozwiązania – podobna. Zrobił je po raz pierwszy w 1928 roku Mojżesz Presburger, Polak pochodzenia żydowskiego, studiujący matematykę na Uniwersytecie Warszawskim u prof. Alfreda Tarskiego. Po ukazaniu się pracy Gödla wynik okazał się znaczący, ale w pierwszej chwili nie został doceniony przez profesora i był tylko podstawą magisterium Presburgera. Dzisiaj teoria dodawania nazywa się arytmetyką Presburgera.