Wykłady ze Złożoności Obliczeniowej *

Antoni Kościelski

1 Twierdzenie Fagina

1.1 Problemy teoriografowe

Układ

$$\langle V, R_0, R_1, \ldots, R_p, c_1, \ldots, c_q \rangle \tag{1}$$

taki, że V jest zbiorem, R_i dla $i = 0, \ldots, p$ są relacjami w zbiorze V i $c_i \in V$ dla $i = 1, \ldots q$ nazywamy strukturą. Zbiór V nazywamy uniwersum tej struktury. Często rozważa się się podobne układy zawierające – oprócz relacji i wyróżnionych elementów – także funkcje. Teraz będziemy rozważać wyłącznie struktury bez funkcji.

Sygnaturą struktury (1) nazywamy ciąg liczb $(k_0, k_1, \ldots, k_{p+q})$ taki, że dla $i = 0, \ldots, p$ zachodzi zawieranie

$$R_i \subseteq V^{k_i}$$

oraz $k_i = 0$ dla $i = n + 1, \ldots p + q$. Tak więc liczba 0 w sygnaturze wskazuje, że na odpowiednim miejscu w strukturze jest wyróżniony element, a liczby dodatnie – że na odpowiednich miejscach są relacje o podanej arności. Jeżeli to będzie istotne z jakichkolwiek względów, to będziemy mieszać relacje z wyróżnionymi elementami i wymieniać je w dowolnej kolejności.

Strukturę (1) będziemy nazywać grafową, jeżeli ma sygnaturę $(k_0, k_1, \ldots, k_{p+q})$ taką, że $k_0 = 2$. Struktury grafowe w skrócie będziemy nazywać grafami. Elementy uniwersów struktur grafowych będziemy nazywać wierzchołkami.

Problemem teoriografowym będziemy nazywać rodzinę struktur grafowych o ustalonej sygnaturze i o skończonych, przynajmniej dwuelementowych uniwersach, zamkniętą ze względu na izomorfizm.

*Wykłady są prowadzone według książki Computational Complexity Christosa Papadimitriou

Przykład 1.1 Problem osiągalności możemy formalizować jako odpowiednią rodzinę struktur o sygnaturze $(2, 0, 0)$.

Przykład 1.2 Problem istnienia kliki możemy formalizować jako rodzinę struktur o sygnaturze $(2, 1)$, a więc grafów z wyróżnionym zbiorem wierzchołków. Problem ten składa się ze struktur $\langle V, E, R\rangle$ takich, że w grafie $\langle V, E\rangle$ istnieje klika, która ma tyle elementów, co dany zbiór R.

Przykład 1.3 Problem kojarzenia małżeństw możemy uważać za zbiór struktur o sygnaturze $(2, 1, 1)$. Do tego problemu należe struktury $\langle V, E, R_1, R_2\rangle$ takie, że R_1 i R_2 mają tyle samo elementów i są rozłączne, $V = R_1 \cup R_2$, $E \subseteq R_1 \times R_2$ oraz istnieje zbiór $E_0 \subseteq E$ równoliczny z R_1 i taki, że dowolny element V jest jedną ze współrzędnych elementu z E_0.

Maszyny Turinga mogą rozwiązywać problemy teoriografowe. Wymaga to jednak ustalenia sposobu przekazywania informacji o danej strukturze. Jest oczywiste, że tę informację możemy przekazywać na wiele sposobów. Na przykład, możemy wybrać i ustalić porządek wierzchołków grafu. Porządek ten wyznacza porządek leksykograficzny w zbiorze k elementowych ciągów wierzchołków. Mówimy, że słowo $s \in \{0, 1\}^*$ reprezentuje k argumentową relację R, jeżeli dla dowolnego i, i-tym znakiem tego słowa jest 1 wtedy i tylko wtedy, gdy i-ty (w porządku leksykograficznym) ciąg k wierzchołków należy do relacji R. Wyróżniony wierzchołek a możemy utożsamiać z jednoargumentową relacją $\{a\}$. W ten sposób relacje i wyróżnione elementy dowolnej struktury możemy reprezentować jako pewne słowa. Całą strukturę możemy reprezentować jako konkatenację słów reprezentujących poszczególne relacje i wyróżnione elementy, wraz z separatorami rozdzielającymi te słowa. Nietrudno zauważyć, że każda struktura może być reprezentowana na wiele sposobów (na $\leq n!$, gdzie n jest liczbą wierzchołków rozważanej struktury, sposobów wyznaczonych przez porządki w zbiorze wierzchołków i wielu innych), oraz słowo reprezentujące strukturę pozwala jedynie na odtworzenie reprezentowanej struktury z dokładnością do izomorfizmu.

Przypuśćmy, że rozważamy struktury (1) o sygnaturze $(2, k_1, \ldots, k_p, 0, \ldots, 0)$ złożonej z $p + q + 1$ liczb. Niech $k = \max(2, k_1, \ldots, k_p) + 1$. W dowodzie twierdzenia Fagina będziemy przyjmować, że takie struktury $\mathcal{G}$ o n wierzchołkach są reprezentowane za pomocą słów

$$s(\mathcal{G}) = \sqcup^{n^k-1} \prod_{i=0}^{p} \left(\sqcup^{(n-2)\cdot n^{k+\zeta(i+1)}} s_i \sqcup^{n^k-n^{k_i}}\right) \prod_{i=1}^{q} \left(\sqcup^{(n-2)\cdot n^{k+\zeta(i+p+1)}} s_{p+i} \sqcup^{n^k-n}\right)$$

gdzie słowa s_i reprezentują poszczególne relacje i wyróżnione wierzchołki, a $\zeta(i)$ oznacza liczbę zer znajdujących się końcu przedstawienia dwójkowego liczby i. Definiując $s(\mathcal{G})$ stosujemy następującą zasadę: bierzemy ciąg słów $(s_0, \ldots, s_{p+q})$, każde z tych słów uzupełniamy znakami $\sqcup$ tak, aby otrzymać słowo długości n^k (słowo s_0 ma n^2 znaków, s_1 ma n^{k_1} znaków), do otrzymanego w ten sposób ciągu na początku dopisujemy słowo $\sqcup^{n^k-1}$, a następnie między kolejne słowa wstawiamy dodatkowo napisy postaci $\sqcup^{(n-2)\cdot n^{k+\zeta(i)}}$.

Przypuśćmy, że znaki słowa $s(\mathcal{G})$ numerujemy liczbami od 1 przedstawianymi w systemie pozycyjnym o podstawie n. Definicja $s(\mathcal{G})$ zapewnia łatwą do wyrażenia zależność między przedstawieniem numeru pewnego znaku i informacją zakodowaną w tym znaku. Na przykład, nie zawierają istotnych informacji znaki, których numery mają przedstawienia o długości mniejszej lub równej $k+1$, w których $k+1$ cyfra jest mniejsza od $n-1$ (czyli od największej cyfry). Znaki o numerach z przedstawieniami długości $k+1$, które zaczynają się cyfrą $n-1$, a na pozostałych pozycjach z wyjątkiem najwyżej dwóch ostatnich mają cyfry 0, zawierają informację o relacji R_0.

Zauważmy, że w $s(\mathcal{G})$ poszczególne słowa s_i są oddzielone przynajmniej jednym znakiem $\sqcup$. Pierwsze słowo we wzorze na $s(\mathcal{G})$ ma długość n^k-1, a łączna długość słów s_i i następujących po nich znaków $\sqcup$ wynosi n^k. Przyjmijmy, że $l = 1 + \lfloor \log(1+p+q) \rfloor$. Wtedy $1+p+q < 2^l$. Długość słow reprezentujących rozważane struktury można oszacować w następujący sposób:

$$|s(\mathcal{G})| < n^k + \sum_{i=1}^{2^l-1} ((n-2)\cdot n^{k+\zeta(i)} + n^k).$$

Grupując w tej sumie dwa kolejne składniki postaci n^k i składnik znajdujący się między nimi otrzymujemy

$$|s(\mathcal{G})| < (n^k+(n-2)\cdot n^{k+\zeta(1)}+n^k) + \sum_{i=1}^{2^{l-1}-1} ((n-2)\cdot n^{k+\zeta(2\cdot i)} + (n^k+(n-2)\cdot n^{k+\zeta(2\cdot i+1)}+n^k)).$$

Zachodzą wzory $\zeta(2\cdot i+1) = 0$ oraz $\zeta(2\cdot i) = 1+\zeta(i)$, a więc

$$|s(\mathcal{G})| < n^{k+1} + \sum_{i=1}^{2^{l-1}-1} ((n-2)\cdot n^{k+1+\zeta(i)} + n^{k+1}).$$

Powtarzając to rozumowanie jeszcze $l-1$ razy otrzymujemy, że

$$|s(\mathcal{G})| < n^{k+l}.$$

Liczbę n będziemy nazywać rozmiarem słowa $s(\mathcal{G})$. Zauważmy, że znając słowo $s(\mathcal{G})$ znamy także słowo s_0, którego długość jest równa kwadratowi rozmiaru $s(\mathcal{G})$. W ogólnym przypadku rozmiar danych możemy definiować jako $\left\lceil \sqrt{|s_0|} \right\rceil$, gdzie s_0 jest pierwszym blokiem bez znaku $\sqcup$, zawartym w danym słowie.

1.2 Tablice obliczeń

Będziemy rozważać maszyny Turinga rozwiązujące problemy teoriografowe złożone ze struktur o sygnaturze takiej, jak sygnatura struktury (1). Niech $l = \lfloor \log(1 + p + q) \rfloor + 1$, $k = \max(2, k_1, \ldots, k_p) + 1$ i niech t będzie liczbą naturalną $> k + l$. Interesują nas takie maszyny Turinga, które dodatkowo

1. są jednotaśmowe,
2. w dowolnej konfiguracji wykonują nie więcej niż dwa rozkazy,
3. po rozpoczęciu pracy nie znajdują się w konfiguracji, w której obserwują $\triangleright$,
4. podczas pracy nie zapisują w jakiejkolwiek komórce znaku $\triangleright$, a więc w dowolnej konfiguracji znak ten będzie się znajdował tylko w pierwszej komórce,
5. mają dwa specjalne stany *'y'* i *'n'*: przechodzą do tych stanów tylko wtedy, gdy obserwują drugi znak na taśmie, a w tych stanach – bez względu na obserwowaną literę – zapisują znak $\sqcup$, nie zmieniają swojego stanu i położenia głowicy,
6. po uruchomieniu w konfiguracji $(s, \triangleright, x)$ ze stanem początkowym s i dowolnym słowem x rozmiaru n, długości $|x| \leq n^{k+l}$, złożonym z dokładnie $1 + p + q$ niepustych zerojedynkowych podsłów bez znaków $\sqcup$ i rozdzielonych znakami $\sqcup$, bez względu na sposób pracy, przed wykonaniem $n^t - 1$ ruchów przechodzą do jednego ze specjalnych stanów,
7. akceptują dane słowo wtedy i tylko wtedy, gdy podczas pracy przechodzą do stanu *'y'*.

Lemat 1.4 *Niech* $\mathbf{G}$ *będzie problemem teoriografowym. Problem* $\mathbf{G} \in \mathbf{P}$ *(*$\mathbf{G} \in \mathbf{NP}$*) wtedy i tylko wtedy, gdy istnieją liczba t i maszyna Turinga M (odpowiednio: niedeterministyczna maszyna Turinga M) spełniająca podane warunki taka, że dla dowolnej struktury* $\mathcal{G}$*, warunek* $\mathcal{G} \in \mathbf{G}$ *jest równoważny akceptowaniu przez maszynę M słowa* $s(\mathcal{G})$.

Dowód. Istotną częścią lematu jest implikacja stwierdzająca, że jeżeli **G** jest problemem wielomianowym, to istnieje maszyna spełniająca podane warunki. Ograniczymy się do uwag dotyczących tej implikacji.

Aby zapewnić warunek 5. możemy podwoić alfabet maszyny Turinga. Każda litera podwojonego alfabetu będzie pamiętać dwie informacje: literę alfabetu danej maszyny i dodatkowo, czy ta litera znajduje się w drugiej komórce. Bez trudu dowolną maszynę przekształcamy tak, aby posługiwała się podwojonym alfabetem w sposób zapewniający prawdziwość dodatkowej informacji zawartych w jego literach. Taka maszyna może podczas pracy nie obserwować pierwszej komórki (zawierającej $\triangleright$) oraz – po zakończeniu obliczeń – odszukać drugą komórkę i dopiero wtedy przekazać wynik obliczeń.

Główna różnica między zwykłą maszyną Turinga i maszyną spełniającą podane warunki polega na tym, że ta druga korzysta z niestandardowych danych. Powoduje to, że kłopotliwe jest znalezienie końca danych, a także analiza takich danych może wymagać wykonania większej niż normalnie liczby ruchów. Zakładamy jednak, że konstruujemy maszynę, która może działać niepoprawnie dla niepoprawnych lub zbyt długich danych, a działa poprawnie, jeżeli jako dane dostanie ściśle określoną liczbę bloków bez znaku $\sqcup$ i długość tych bloków razem z rozdzielającymi znakami $\sqcup$ spełnia ograniczenia podane w punkcie 6. Maszyna ta może najpierw z danych usunąć zbędne znaki $\sqcup$ i przekształcić dane do standardowej postaci. Następnie może uruchomić zwykłą, wielomianową maszynę Turinga rozwiązującą problem **G**. $\Box$

Niech $M = (K, \Sigma, \delta, s)$ będzie maszyną Turinga spełniającą podane warunki dla liczby t, x – słowem rozmiaru n nad alfabetem Σ spełniającym założenia z warunku 6, $K_0, K_1, K_2, \ldots$ – dowolnym ciągiem kolejnych konfiguracji maszyny M takim, że $K_0 = (s, \triangleright, x)$. Przypuśćmy, że $K_i = (q, ua, v)$, gdzie $q \in K$, $u, v \in \Sigma^*$ oraz $a \in \Sigma$. Symbolem K_i' będziemy oznaczać słowo nad alfabetem $\Sigma \cup K\Sigma$ takie, że $K_i' = u(qa)v$ (symbole (qa) oznaczają literę z alfabetu $K\Sigma$). Tablicą obliczeń dla słowa x, wyznaczoną przez ciąg konfiguracji $K_0, K_1, K_2, \ldots$ nazywamy dwuwymiarową tablicę (macierz) indeksowaną liczbami mniejszymi n^t (macierz o wymiarach $n^t \times n^t$, o wierszach i kolumnach indeksowanych liczbami od 0 do $n^t - 1$), w której na przecięciu wiersza o numerze j i kolumny o numerze i znajduje się i-ta litera (litera o numerze i) słowa K_j', jeżeli słowo to ma taką literę, a w przeciwnym razie – znak $\sqcup$.

Nietrudno zauważyć kilka własności tablic obliczeń. Pierwsza kolumna (o numerze 0) tablicy obliczeń – z wyjątkiem pierwszego pola – zawiera znaki $\triangleright$, zaś ostatnia – znaki $\sqcup$. Pierwszy wiersz zawiera znak $(s\triangleright)$, dalej kolejne znaki słowa x, a w pozostałych polach – znaki $\sqcup$. Maszyna M akceptuje słowo x wtedy i tylko wtedy, gdy dla słowa x istnieje tablica obliczeń zawierająca znak $('y'\sqcup)$ w polu znajdującym się w ostatnim wierszu i drugiej kolumnie (kolumnie o numerze 1). Zauważmy także, że zawartość pola o współrzędnych (i, j) (pierwsza współrzędna określa kolumnę) jest wyznaczona (dla maszyn deterministycznych – jednoznacznie) przez zawartość pól o współrzędnych $(i-1, j-1)$, $(i, j-1)$ oraz $(i+1, j-1)$.

1.3 Główny lemat

Przypuśćmy, że mamy daną strukturę

$$\mathcal{G} = \langle V, E, R_1, \ldots, R_p, c_1, \ldots, c_q \rangle$$

o przynajmniej dwóch wierzchołkach, liniowy porządek $<$ w zbiorze V, liczbę naturalną t i maszynę Turinga $M = (K, \Sigma, \delta, s)$ spełniające warunki podane w rozdziale 1.2. Będziemy konstruować formułę zapisaną za pomocą symboli relacyjnych $=$, E, $R_1, \ldots, R_p$ T_σ dla wszystkich $\sigma \in \Sigma \cup K\Sigma$, C_0, C_1 i S_l oraz symboli stałych $c_1, \ldots, c_q$, min i max. Symbole $=$ i E są dwuargumentowe, R_i mają ustaloną arność k_i, wszystkie symbole T_σ oraz S_l są arności $2 \cdot t$, a C_0 i C_1 są arności t. Nie będziemy rozróżniać symboli relacyjnych i ich interpretacji, tak jak to już zostało zrobione w powyższym tekście. Przyjmujemy więc, że już mamy ustalone znaczenie symboli E, R_i i c_i. Znak $=$ będzie interpretowany jak zwykle, jako relacja identyczności. Ponadto, symbole S_l, min i max będą miały ustalone znaczenie. Symbole min i max będą odpowiednio najmniejszym i największym elementem V w sensie relacji $<$ (a więc oznaczają różne elementy). Umówmy się, że symbole takie jak $\vec{x}$ lub $\vec{y_1}$ będą oznaczały – zależnie od kontekstu – ciąg t elementów zbioru V lub zmiennych występujących w formułach (a więc interpretowanych tutaj jako elementy V). Jeżeli symbolem $<_l$ oznaczymy leksykograficzny porządek w zbiorze V^t, wyznaczony przez $<$, to S_l definiujemy jako relację następnika w sensie porządku $<_l$, a więc

$$S_l = \{(\vec{x}, \vec{y}) \in (V^t)^2 : \vec{x} <_l \vec{y} \wedge \forall \vec{z}\, (\neg \vec{x} <_l \vec{z} \vee \neg \vec{z} <_l \vec{y})\}.$$

Lemat 1.5 *Przypuśćmy, że mamy daną maszynę Turinga M i liczbę t spełniające warunki podane w rozdziale* 1.2 *oraz strukturę $\mathcal{G}$ o przynajmniej dwóch wierzchołkach i liniowy porządek $<$ w zbiorze wierzchłków $\mathcal{G}$. Jeżeli M jest maszyną niedeterministyczną, to istnieje formuła Φ (w koniunkcyjnej postaci normalnej, bez zmiennych wolnych) taka, że maszyna M akceptuje $s(\mathcal{G})$ (w definicji $s(\mathcal{G})$ używamy porządku $<$) wtedy i tylko wtedy, gdy istnieje takie rozszerzenie struktury $\langle \mathcal{G}, S_l, \min, \max \rangle$ o interpretację symboli C_0, C_1 i T_σ dla $\sigma \in \Sigma \cup K\Sigma$, że*

$$\langle \mathcal{G}, S_l, \min, \max, C_0, C_1, T_{\sigma_1}, \ldots, T_{\sigma_u} \rangle \models \Phi.$$

Dowód. Niech $\vec{x}$ będzie t elementowym ciągiem wierzchołków struktury $\mathcal{G}$. Z tym ciągiem zwiążemy liczbę naturalną

$$\lambda(\vec{x}) = \#\{\vec{y} : \vec{y} <_l \vec{x}\}.$$

Przyjmijmy, że struktura $\mathcal{G}$ ma sygnaturę o $1+p+q$ elementach. Niech k i l oznaczają – jak dotychczas – odpowiednio liczbę większą od arności relacji struktury $\mathcal{G}$ oraz liczbę znaków potrzebnych do zapisania w systemie dwójkowym liczby relacji i stałych struktury $\mathcal{G}$. Dla liczb ≥ 0 i $< 2^l$ będziemy tworzyć przedstawienia dwójkowe długości l zapisane za pomocą symboli (cyfr) min (oznaczającego 0) i max (oznaczającego 1). Jeżeli $i < 2^l$, to $\vec{\mu}(i)$ będzie oznaczać takie przedstawienie.

Weźmy maszynę M i uporządkujmy jej rozkazy. Maszyna ta w każdej konfiguracji wykonuje jeden z dwóch rozkazów: pierwszy i drugi w sensie ustalonego porządku, albo o numerach 0 i 1. Załóżmy, że M akceptuje $s(\mathcal{G})$. Wtedy istnieje ciąg konfiguracji $K_0, K_1, K_2, \ldots$ zaczynający się konfiguracją $K_0 = (s, \triangleright, s(\mathcal{G}))$, w którym istnieje konfiguracja ze stanem 'y'. Przed podaniem formuły Φ zdefiniujemy interpretacje symboli występujących w tej formule. Tak więc

$$C_i = \{\vec{x} \in V^t : \text{konfiguracja } K_{\lambda(\vec{x})+1} \text{ powstaje z } K_{\lambda(\vec{x})} \text{ w wyniku wykonania rozkazu o numerze } i\}$$

dla $i = 0, 1$. Symbole T_σ zinterpretujemy jako

$$T_\sigma = \{(\vec{x}, \vec{y}) \in (V^t)^2 : \text{w tablicy obliczeń dla } s(\mathcal{G}) \text{ wyznaczonej przez } K_0, K_1, K_2, \ldots, \text{ w polu o współrzędnych } (\lambda(\vec{x}), \lambda(\vec{y})) \text{ znajduje się znak } \sigma\}.$$

Dla liczby naturalnej i symbolem $\min^i$ oznaczamy ciąg $\min, \ldots, \min$ złożony z i symboli min. Podobnie definiujemy $\max^i$.

Zauważmy, że przy podanej interpretacji symboli prawdziwe są następujące formuły:

1. $\forall \vec{x}\, \forall \vec{y} \bigwedge_{\sigma_1 \neq \sigma_2} (\neg T_{\sigma_1}(\vec{x}, \vec{y}) \vee \neg T_{\sigma_2}(\vec{x}, \vec{y}))$

2. $T_{(s\triangleright)}(\min^t, \min^t) \;\wedge\; \forall \vec{x}\, \forall \vec{y}\, (S_l(\vec{x}, \vec{y}) \Longrightarrow T_\triangleright(\min^t, \vec{y}))$

3. $\forall \vec{x}\, T_\sqcup(\max^t, \vec{x})$

4. $\forall x_1 \ldots \forall x_k \bigwedge_{1 \leq j \leq k} (x_j \neq \min \Longrightarrow T_\sqcup(\min^{t-k}, x_1, \ldots, x_k, \min^t))$

5. $\bigwedge_{0\leq i\leq p} \forall x_1 \ldots \forall x_{k_i}\ (R_i(x_1,\ldots,x_{k_i}) \Longrightarrow T_1(\min^{t-k-l}, \vec{\mu}(i{+}1), \min^{k-k_i}, x_1,\ldots,x_{k_i}, \min^t))$

6. $\bigwedge_{0\leq i\leq p} \forall x_1 \ldots \forall x_{k_i}\ (\neg R_i(x_1,\ldots,x_{k_i}) \Longrightarrow T_0(\min^{t-k-l}, \vec{\mu}(i{+}1), \min^{k-k_i}, x_1,\ldots,x_{k_i}, \min^t))$

7. $\bigwedge_{0\leq i\leq p} \forall x_1 \ldots \forall x_k \bigwedge_{1\leq j\leq k-k_i} (x_j \neq \min \Longrightarrow T_{\sqcup}(\min^{t-k-l}, \vec{\mu}(i+1), x_1,\ldots,x_k, \min^t))$

8. $\bigwedge_{1\leq i\leq q} \forall x\ (x = c_i \Longrightarrow T_1(\min^{t-k-l}, \vec{\mu}(1+p+i), \min^{k-1}, x, \min^t))$

9. $\bigwedge_{1\leq i\leq q} \forall x\ (x \neq c_i \Longrightarrow T_0(\min^{t-k-l}, \vec{\mu}(1+p+i), \min^{k-1}, x, \min^t))$

10. $\bigwedge_{1\leq i\leq q} \forall x_1 \ldots \forall x_k \bigwedge_{1\leq j\leq k-1} (x_j \neq \min \Longrightarrow T_{\sqcup}(\min^{t-k-l}, \vec{\mu}(1{+}p{+}i), x_1,\ldots,x_k, \min^t))$

11. $\bigwedge_{1+p+q<i<2^l} \forall x_1 \ldots \forall x_k\ T_{\sqcup}(\min^{t-k-l}, \vec{\mu}(i), x_1,\ldots,x_k, \min^t)$

12. $\forall x_1 \ldots \forall x_{k+l} \bigwedge_{1\leq j\leq l} (x_j \neq \min \wedge x_j \neq \max \Longrightarrow T_{\sqcup}(\min^{t-k-l}, x_1,\ldots,x_{k+l}, \min^t))$

13. $\forall \vec{x} \bigwedge_{1\leq j\leq t-k-l} (x_j \neq \min \Longrightarrow T_{\sqcup}(\vec{x}, \min^t))$

14. $\forall \vec{x}\ (C_0(\vec{x}) \vee C_1(\vec{x}))\ \wedge\ \forall \vec{x}\ (\neg C_0(\vec{x}) \vee \neg C_1(\vec{x}))$

15. $$\forall \vec{x}\, \forall \vec{y}\, \forall \vec{z}\, \forall \vec{u}\, \forall \vec{v} \bigwedge_{\alpha,\beta,\gamma,c} (S_l(\vec{u},\vec{y}) \wedge S_l(\vec{y},\vec{w}) \wedge S_l(\vec{x},\vec{z}) \wedge$$
$$\wedge\, T_\alpha(\vec{u},\vec{x}) \wedge T_\beta(\vec{y},\vec{x}) \wedge T_\gamma(\vec{w},\vec{x}) \wedge C_c(\vec{x}) \Longrightarrow T_{\sigma(\alpha,\beta,\gamma,c)}(\vec{y},\vec{z}))$$

16. $\forall \vec{x}\ (S_l(\min^t, \vec{x}) \Longrightarrow T_{(\text{'y'}\sqcup)}(\vec{x}, \max^t))$

Prawdziwość formuł od 4. do 13. wynika stąd, że w pierwszym wierszu tablicy obliczeń dla słowa $s(\mathcal{G})$, od drugiej kolumny, jest zapisane właśnie słowo $s(\mathcal{G})$, a po nim znajdują się w tym wierszu same znaki $\sqcup$.

Formułę Φ definiujemy jako koniunkcję wymienionych formuł. Jeżeli wszystkie te formuły są prawdziwe przy podanej interpretacji symboli, to tym bardziej przy tej interpretacji jest prawdziwa formuła Φ.

Przypuśćmy, że przy pewnej interpretacji symboli C_0, C_1 i T_σ dla $\sigma \in \Sigma \cup K\Sigma$ w rozszerzonej strukturze $\mathcal{G}$ jest spełniona formuła Φ. Wtedy możemy zdefinionać pewną macierz T o rozmiarach $n^t \times n^t$ wypełnioną znakami z alfabetu $\Sigma \cup K\Sigma$. W polu macierzy T o współrzędnych (i, j) umieszczamy znak σ taki, że $(\vec{x}, \vec{y}) \in T_\sigma$ dla ciągów $\vec{x}$ i $\vec{y}$ spełniających równości $i = \lambda(\vec{x})$ i $j = \lambda(\vec{y})$. Dla tak zdefiniowanej macierzy może się zdarzyć, że zawartość pewnego pola nie jest zdefiniowana lub też jest zdefiniowana niejednoznacznie (podany warunek spełnia kilka znaków σ). Z prawdziwości pierwszego człony formuły Φ wynika jednak, że podany warunek spełnia najwyżej jeden znak σ.

Pokażemy, że wyżej zostały zdefiniowane zawartości wszystkich pól macierzy T. Spełnianie członu o numerze 2 formuły Φ gwarantuje, że zostały zdefiniowane zawartości wszystkich pól pierwszej kolumny. To samo dla ostatniej kolumny gwarantuje prawdziwość trzeciego członu. Prawdziwość członów od 4 do 13 implikuje, że mamy zdefiniowane zawartości pól z pierwszego wiersza macierzy T. Teraz możemy pokazać przez indukcję, że mamy zdefiniowane zawartości wszystkich wierszy T. Pokazując to korzystamy z prawdziwości 14. i 15. członu formuły Φ.

Następny krok w dowodzie polega na wykazaniu, że T jest tablicą obliczeń maszyny M dla słowa $s(\mathcal{G})$. Prawdziwość członów 2 i 3 formuły Φ implikuje nie tylko, że są zdefiniowane zawartości pól pierwszej i ostatniej kolumny macierzy T, ale także, że zawierają one takie znaki, jakie znajdują się w tablicy obliczeń maszyny M (spełniającej warunki z rozdziału 1.2). Analogiczna własność pierwszego wiersza wynika z prawdziwości członów formuły Φ o numerach od 4 do 13. Dla danej liczby i, analizując relacje C_0 i C_1 i dzięki prawdziwości 14. członu formuły Φ możemy ustalić, który z rozkazów maszyny M pozwala na przekształcenie konfiguracji opisanej w i-tym wierszy tablicy T w konfigurację opisaną w wierszu następnym. Jeżeli znamy ten rozkaz, to dzięki prawdziwości członu 15 możemy wykazać, że $(i+1)$-wszy wiersz zawiera informację o odpowiedniej konfiguracji maszyny M.

Aby zakończyć dowód wystarczy zauważyć, że prawdziwość członu 16 formuły Φ implikuje, że tablica T swiadczy o tym, że maszyna M akceptuje słowo $s(\mathcal{G})$. $\square$

1.4 Formuły hornowskie

Przypuśćmy, że mamy symbole relacyjne $P_1, \ldots, P_k$. Klauzule hornowskie ze względu na $P_1, \ldots, P_k$, to elementy najmniejszego zbioru formuł, do którego należą formuły postaci $P_i(\vec{x})$ oraz $\neg P_i(\vec{x})$, a także dowolne formuły nie zawierające żadnego z symboli $P_1, \ldots, P_k$, zamkniętego ze względu na alternatywę z formułami postaci $\neg P_i(\vec{x})$ i dowolnymi formułami bez symboli $P_1, \ldots, P_k$. Formułami hornowskimi ze względu na $P_1, \ldots, P_k$ nazywamy poprzedzoną blokiem kwantyfikatorów ogólnych (wieloczłonową) koniunkcję klauzul hornowskich ze względu na $P_1, \ldots, P_k$.

Przykład 1.6 Przykładem formuły hornowskiej ze względu na symbole postaci T_σ jest (po zamianie implikacji na odpowiednią alternatywę) formuła

$$\forall\vec{x}\,\forall\vec{y}\,\forall\vec{z}\,\forall\vec{u}\,\forall\vec{v} \bigwedge_{\alpha,\beta,\gamma,c} (\varphi(\vec{u},\vec{y}) \wedge \varphi(\vec{y},\vec{w}) \wedge \varphi(\vec{x},\vec{z}) \wedge$$
$$\wedge\, T_\alpha(\vec{u},\vec{x}) \wedge T_\beta(\vec{y},\vec{x}) \wedge T_\gamma(\vec{w},\vec{x}) \wedge C_c(\vec{x}) \Longrightarrow T_{\sigma(\alpha,\beta,\gamma,c)}(\vec{y},\vec{z}))$$

w której φ jest dowolną formułą bez symboli postaci T_σ.

Przykład 1.7 Przykładem formuły, która nie jest hornowska ze względu na C_0 i C_1 jest formuła 14 ze strony 8.

Fakt 1.8 *Koniunkcja formuł hornowskich ze względu na $P_1, \ldots, P_k$ jest równoważna formule hornowskiej ze względu na $P_1, \ldots, P_k$.*

Fakt 1.9 *Jeżeli Φ jest formułą hornowską ze względu na $P_1, \ldots, P_k$, a w formule φ nie występują symbole $P_1, \ldots, P_k$, to formuła*

$$\forall x\,(\varphi \Longrightarrow \Phi)$$

jest równoważna formule hornowskiej ze względu na $P_1, \ldots, P_k$.

Lemat 1.10 *Przypuśćmy, że mamy daną maszynę Turinga M i liczbę t spełniające warunki podane w rozdziale* 1.2 *oraz strukturę $\mathcal{G}$ o przynajmniej dwóch wierzchołkach i liniowy porządek $<$ w zbiorze wierzchołków $\mathcal{G}$. Jeżeli M jest maszyną deterministyczną, to istnieje formuła Φ (w koniunkcyjnej postaci normalnej, bez zmiennych wolnych,) hornowska względem symboli S_l oraz T_σ dla $\sigma \in \Sigma \cup K\Sigma$ taka, że maszyna M akceptuje $s(\mathcal{G})$ wtedy i tylko wtedy, gdy istnieje takie rozszerzenie struktury $\langle \mathcal{G}, S_l, \min, \max\rangle$ o interpretację symboli T_σ dla $\sigma \in \Sigma \cup K\Sigma$, że*

$$\langle \mathcal{G}, S_l, \min, \max, T_{\sigma_1}, \ldots, T_{\sigma_u}\rangle \models \Phi.$$

Dowód. Podany lemat dowodzimy tak samo, jak lemat 1.5. Założenie o deterministyczności M pozwala uprościć definicję Φ i spowodować, że ta formuła jest hornowska w sensie podanym w sformułowaniu lematu (formuła Φ z poprzedniego lematu nie jest hornowska, ponieważ zawiera człon 14). Uproszczenie definicji Φ polega na usunieciu z niej 14. członu i zastąpienie 15. członu przez następujący:

15. $$\forall\vec{x}\,\forall\vec{y}\,\forall\vec{z}\,\forall\vec{u}\,\forall\vec{v} \bigwedge_{\alpha,\beta,\gamma} (S_l(\vec{u},\vec{y}) \wedge S_l(\vec{y},\vec{w}) \wedge S_l(\vec{x},\vec{z}) \wedge$$
$$\wedge\, T_\alpha(\vec{u},\vec{x}) \wedge T_\beta(\vec{y},\vec{x}) \wedge T_\gamma(\vec{w},\vec{x}) \Longrightarrow T_{\sigma(\alpha,\beta,\gamma)}(\vec{y},\vec{z})).\ \square$$

1.5 Egzystencjalna logika drugiego rzędu

W logice drugiego rzędu, oprócz zmiennych indywiduowych (zmiennych pierwszego rzędu) mamy zmienne symbole relacyjne, o nieustalonej interpretacji. Zmienne relacyjne możemy kwantyfikować podobnie jak zmienne indywiduowe. Niech φ będzie formułą, w której oprócz zwykłych symboli relacyjnych występują zmienne symbole relacyjne. W definicji formuły języka drugiego rzędu umieszczamy dodatkowy warunek: jeżeli φ jest formułą języka drugiego rzędu i P jest zmienną relacyjną, to $\exists P\ \varphi$ jest formułą języka drugiego rzędu. Oczywiście, możemy posługiwać się także kwantyfikatorami uniwersalnymi, ale teraz takie kwantyfikatory nie będą nam potrzebne. Formuła $\exists P\ \varphi$ jest prawdziwa (spełniona) przy pewnej interpretacji symboli występujących w φ (w pewnej strukturze) i przy pewnym wartościowaniu występujących w tej formule zmiennych indywiduowych, jeżeli można tak zinterpretować symbol P, aby przy danej interpretacji symboli rozszerzonej o interpretację symbolu P i przy danym wartościowaniu zmiennych indywiduowych była prawdziwa formuła φ.

Przypuśćmy, że mamy dwa zmienne symbole relacyjne P_1 i P_2 o arnościach odpowiednio k_1 i k_2 spełniających $k_1 \leq k_2$. Rozszerzamy alfabet o dwie stałe a i b. Niech P będzie nowym, zmiennym symbolem relacyjnym o arności $k_2 + 1$. Dla dowolnej formuły φ zapisanej przy użyciu symboli P_1 i P_2, ale bez kwantyfikatorów wiążących te zmienne, definiujemy formułę φ' zastępując formuły $P_1(x_1, \ldots, x_{k_1})$ przez $P(x_1, \ldots, x_{k_1}, a, \ldots, a, a)$ oraz formuły $P_2(x_1, \ldots, x_{k_2})$ przez $P(x_1, \ldots, x_{k_2}, b)$.

Lemat 1.11 *Formuła*

$$\forall a\ \forall b\ \Big(a \neq b \Longrightarrow (\exists P_1\ \exists P_2\ \varphi \Longleftrightarrow \exists P\ \varphi')\Big) \tag{2}$$

jest tautologią logiki drugiego rzędu.

Dowód. Niech $\mathcal{G}$ będzie dowolną strukturą, a a i b dwoma różnymi elementami jej uniwersum. Weźmy relacje P_1 i P_2 odpowiednio o k_1 i k_2 argumentach. Niech

$$P = \{(y_1, \ldots, y_{k_2+1}) \in V^{k_2+1} : \Big((y_1, \ldots y_{k_1}) \in P_1\ \wedge \bigwedge_{k_1+1 \leq i \leq k_2+1} y_i = a\Big)\ \vee$$
$$\vee\ \Big((y_1, \ldots y_{k_2}) \in P_2\ \wedge\ y_{k_2+1} = b\Big)\}.$$

Zauważmy, że wtedy

$$\langle \mathcal{G}, P_1, P_2, P, a, b\rangle \models (\varphi \Longleftrightarrow \varphi'). \tag{3}$$

Dowodzimy to przez indukcję ze względu na budowę φ. Prawie cały dowód jest standardowy, wątpliwości może budzić jedynie pierwszy krok indukcyjny dla formuł atomowych zaczynających się symbolami P_1 i P_2. Dla takich formuł powinniśmy dowieść

$$\langle \mathcal{G}, P_1, P_2, P, a, b\rangle \models (P_1(x_1, \ldots x_{k_1}) \Longleftrightarrow P(x_1, \ldots x_{k_1}, a, \ldots, a, a))\}$$

oraz

$$\langle \mathcal{G}, P_1, P_2, P, a, b\rangle \models (P_2(x_1, \ldots x_{k_2}) \Longleftrightarrow P(x_1, \ldots x_{k_2}, b))\}.$$

W obu przypadkach prawdziwość implikacji $\Longrightarrow$ jest oczywista (wynika wprost z definicji P). Implikacje odwrotne też są łatwe do wykazania i są prawdziwe, ponieważ $a \neq b$.

Własność (3) implikuje, że

$$\langle \mathcal{G}, a, b\rangle \models (\exists P_1\, \exists P_2\, \varphi \implies \exists P\, \varphi').$$

Weźmy teraz relację P i zdefiniujmy

$$P_1 = \{(y_1, \ldots, y_{k_1}) \in V^{k_1} : (y_1, \ldots, y_{k_1}, a, \ldots, a, a) \in P\}$$

oraz

$$P_2 = \{(y_1, \ldots, y_{k_2}) \in V^{k_2} : (y_1, \ldots, y_{k_2}, b) \in P\}.$$

Podobnie jak w pierwszej częsci dowodu pokazujemy, że

$$\langle \mathcal{G}, P_1, P_2, P, a, b\rangle \models (\varphi \Longleftrightarrow \varphi') \tag{4}$$

(zauważmy, że zostały zmienione zależności między P, P_1 i P_2). Metoda dowodu pozostaje ta sama. Dowód sprowadza się do przypadku formuł atamowych. Tym razem odpowiednie własności dla formuł atomowych są oczywiste i wynikają bezpośrednio z definicji P_1 i P_2.

Konsekwencją własność (4) jest stwierdzenie, że

$$\langle \mathcal{G}, a, b\rangle \models (\exists P\, \varphi' \implies \exists P_1\, \exists P_2\, \varphi).$$

W ten sposób udowodniliśmy, że formuła (2) jest tautologią. $\square$

Wniosek 1.12 *Dla dowolnej formuły φ (bez kantyfikatorów drugiego rzędu) istnieje formuła φ' taka, że formuła*

$$\forall a\, \forall b\, \Big(a \neq b \Longrightarrow (\exists P_1 \ldots \exists P_k\, \varphi \Longleftrightarrow \exists P\, \varphi')\Big)$$

jest tautologią logiki drugiego rzędu. $\square$

1.6 Podsumowanie

Lemat 1.13 *Każdy język jest wzajemnie redukowalny (w pamięci logarytmicznej) z pewnym problemem teoriografowym bez dodatkowych relacji i stałych (a więc o sygnaturze* (2)*).* □

Lemat 1.14 *Niech*

$$\mathbf{G} = \{\mathcal{G} : \mathcal{G} \models \Phi\}$$

dla pewnej formuły Φ *języka pierwszego rzędu. Wtedy* $\mathbf{G} \in \mathbf{L}$*.* □

Lemat 1.15 *Niech*

$$\mathbf{G} = \{\mathcal{G} : \mathcal{G} \models \exists P_1 \ldots \exists P_k\ \Phi\}$$

dla pewnej formuły Φ *języka pierwszego rzędu. Wtedy* $\mathbf{G} \in \mathbf{NP}$*.* □

Lemat 1.16 *Niech*

$$\mathbf{G} = \{\mathcal{G} : \mathcal{G} \models \exists P_1 \ldots \exists P_k\ \Phi\}$$

dla pewnej formuły Φ *języka pierwszego rzędu w koniunkcyjnej postaci normalnej, hornowskiej względem symboli* $P_1, \ldots, P_k$*. Wtedy* $\mathbf{G} \in \mathbf{P}$*.* □

Twierdzenie 1.17 *Załóżmy, że* $\mathbf{G} \in \mathbf{NP}$*. Wtedy istnieje formuła języka pierwszego rzędu* Φ *w koniunkcyjnej postaci normalnej i liczba naturalna* t *takie, że dla dowolnej struktury grafowej* $\mathcal{G}$ *i dla dowolnego liniowego porządku* $<$ *w zbiorze wierzchołków* $\mathcal{G}$*, jeżeli* S_l, min *i* max *oznaczają kolejno relację następnika dla porządku leksykograficznego wyznaczonego przez* $<$ *w zbiorze* t*-elementowych ciągów wierzchołków struktury* $\mathcal{G}$ *oraz najmniejszy i największy wierzchołek* $\mathcal{G}$ *w sensie porządku* $<$*, to* $\mathcal{G} \in \mathbf{G}$ *wtedy i tylko wtedy, gdy*

$$\langle \mathcal{G}, S_l, \min, \max\rangle \models \exists P\ \Phi.$$

Jeżeli dodatkowo założymy, że $\mathbf{G} \in \mathbf{P}$*, to istnieje formuła* Φ *o wymienionych własnościach, która jest hornowska względem symboli* P*.*

Dowód. Twierdzenie to wynika z lematów 1.4 i 1.5, oraz z wniosku 1.12. Jeżeli $\mathbf{G} \in \mathbf{P}$, to zamiast lematu 1.5 wykorzystujemy lemat 1.10. □

Rozważmy następujące formuły

$$Lin(<) \iff \forall x\ \forall y\ \forall z\Big(\neg x < x \wedge (x < y \wedge y < z \Longrightarrow x < z) \wedge (x < y \vee x = y \vee y < x)\Big),$$

$$Min_{<}(v) \iff \forall x\ \neg x < v$$

oraz

$$Max_<(v) \iff \forall x\ \neg x > v.$$

Niech $Succ_<$ będzie formułą (z dwuargumentową zmienną relacyjną V) postaci

$$Succ_<(V) \iff \forall \vec{x}\ \forall \vec{y}\ \Big(V(\vec{x}, \vec{y}) \iff \psi(\vec{x}, \vec{y})\Big),$$

gdzie ψ jest formułą definiującą relację następnika dla porządku leksykograficznego w zbiorze t elementowych ciągów, wyznaczonego przez porządek $<$ (formuła ta nie zawiera innych symboli relacyjnych poza $<$ i $=$). Jest oczywiste, że warunek

$$\langle \mathcal{G}, < \rangle \models Lin(<)$$

jest spełniony wtedy i tylko wtedy, gdy symbol $<$ został zinterpretowany jako relacja $<$ będąca liniowym prządkiem w zbiorze wierzchołków struktury $\mathcal{G}$. Mamy także przy stosowanych wyżej oznaczeniach, że

$$\langle \mathcal{G}, <, S_l, \min, \max \rangle \models Succ_<(S_l) \wedge Min_<(\min) \wedge Max_<(\max).$$

Twierdzenie 1.18 (Fagina) *Niech* $\mathbf{G}$ *będzie problemem teoriografowym. Wtedy* $\mathbf{G} \in \mathbf{NP}$ *wtedy i tylko wtedy, gdy*

$$\mathbf{G} = \{\mathcal{G} : \mathcal{G} \models \exists R\ \Psi'\}$$

dla pewnej formuły pierwszego rzędu Ψ'.

Dowód. Jeżeli $\mathbf{G} \in \mathbf{NP}$, to na podstawie twierdzenia 1.17 znajdujemy formułę pierwszego rzędu $\Phi = \Phi(S_l, \min, \max)$ (a więc formułę, w której m.in. występują wymienione symbole) i liczbę t takie, że dla dowolnej struktury $\mathcal{G}$ takiego typu jak struktury należące do $\mathbf{G}$ i dowolnego liniowego porządku $<$ w zbiorze wierzchołków $\mathcal{G}$ mamy

$$\mathcal{G} \in \mathbf{G} \iff \langle \mathcal{G}, S_l, \min, \max \rangle \models \exists P\ \Phi. \tag{5}$$

Jeżeli

$$\langle \mathcal{G}, S_l, \min, \max \rangle \models \exists P\ \Phi,$$

to także

$$\langle \mathcal{G}, <, S_l, \min, \max \rangle \models \exists P\ \Big(Lin(<) \wedge Succ_<(S_l) \wedge Min_<(\min) \wedge Max_<(\max) \wedge \Phi\Big),$$

i w konsekwencji

$$\mathcal{G} \models \exists P\, \exists P_1\, \exists P_2\, \exists a\, \exists b\, \Big(Lin(P_1) \wedge Succ_{P_1}(P_2) \wedge Min_{P_1}(a) \wedge Max_{P_1}(b) \wedge \Phi(P_2, a, b)\Big).$$

Jeżeli przyjmiemy, że

$$\Psi = \exists a\, \exists b\, \Big(Lin(P_1) \wedge Succ_{P_1}(P_2) \wedge Min_{P_1}(a) \wedge Max_{P_1}(b) \wedge \Phi(P_2, a, b)\Big)$$

i skorzystamy z wniosku 1.12, to otrzymamy, że $\mathcal{G} \models \exists R\, \Psi'$. Powyższe rozumowanie świadczy o prawdziwości implikacji

$$\mathcal{G} \in \mathbf{G} \Longrightarrow \mathcal{G} \models \exists R\, \Psi'.$$

Przypuśćmy, że $\mathcal{G} \models \exists R\, \Psi'$. Wtedy także

$$\mathcal{G} \models \exists P\, \exists P_1\, \exists P_2\, \exists a\, \exists b\, \Big(Lin(P_1) \wedge Succ_{P_1}(P_2) \wedge Min_{P_1}(a) \wedge Max_{P_1}(b) \wedge \Phi(P_2, a, b)\Big)$$

i można tak zinterpretpwać symbole P_1, P_2, a i b (jako relacje $<$, S_l oraz elementy min i max odpowiednio), aby

$$\langle \mathcal{G}, <, S_l, \min, \max\rangle \models Lin(<) \wedge Succ_<(S_l) \wedge Min_<(\min) \wedge Max_<(\max) \wedge \exists P\, \Phi.$$

Ponieważ $\langle \mathcal{G}, <\rangle \models Lin(<)$, więc $<$ jest liniowym porządkiem w zbiorze wierchołków struktury $\mathcal{G}$. Ponieważ

$$\langle \mathcal{G}, <, S_l, \min, \max\rangle \models Succ_<(S_l) \wedge Min_<(\min) \wedge Max_<(\max),$$

więc S_l jest relacją następnika w odpowiednim porządku leksykograficznym, a min i max są najmniejszym i największym elementem w sensie porządku $<$. Prawdziwa jest więc prawa strona równoważności (5) i w konsekwencji $\mathcal{G} \in \mathbf{G}$.

Podane rozumowanie świadczy o prawdziwości implikacji

$$\Big(\mathcal{G} \models \exists R\, \Psi'\Big) \Longrightarrow \mathcal{G} \in \mathbf{G}$$

i tym samym problem $\mathbf{G}$ ma postać podaną w tezie twierdzenia Fagina.

Problemy postaci $\{\mathcal{G} : \mathcal{G} \models \exists R\, \Psi'\}$ należą do klasy **NP** na mocy lematu 1.15. □

Twierdzenie 1.19 *Niech* $\mathbf{G}$ *będzie problemem teoriografowym. Problem* $\mathbf{G}$ *należy do* **P** *wtedy i tylko wtedy, gdy istnieje formuła pierwszego rzędu* Ψ *hornowska ze względu na* P *taka, że dla dowolnej stryktury* $\mathcal{G}$ *o sygnaturze takiej, jak struktur należących do* $\mathbf{G}$ *i dla dowolnego liniowego porządku* $<$ *wierzchołków struktury* $\mathcal{G}$ *spełniona jest następująca równoważność:*

$$\mathcal{G} \in \mathbf{G} \Longleftrightarrow \langle \mathcal{G}, <\rangle \models \exists P\, \Psi.$$

Dowód. Twierdzenie to różni się od twierdzenia 1.17 (w przypadku deterministycznym) tylko postacią prawej strony równoważności. Warunkowi

$$\langle \mathcal{G}, S_l, \min, \max \rangle \models \exists P\ \Phi \tag{6}$$

ze wspomnianego twierdzenia chcemy nadać postać

$$\langle \mathcal{G}, < \rangle \models \exists P\ \Psi, \tag{7}$$

a więc relację S_l i stałe min i max chcemy zastąpić przez $<$. W tym celu najpierw w formule Φ zastępujemy formuły postaci $S_l(\vec{x}, \vec{y})$ przez $\psi(\vec{x}, \vec{y})$, gdzie ψ jest formułą definiującą S_l (patrz str. 14). Przyjmijmy, że w ten sposób otrzymujemy formułę $\Phi_1 = \Phi_1(\min, \max)$ oraz

$$\Psi = \forall a\ \forall b\ \Big(Min_<(a) \wedge Max_<(b) \Longrightarrow \Phi_1(a, b) \Big).$$

Jest oczywiste, że formuła Ψ jest równoważna formule hornowskiej ze względu na P, oraz że warunki (6) i (7) są równoważne. $\Box$

Możemy też dowieść wersję podanego twierdzenia, w której liniowy porządek $<$ zastępujemy relacją następnika wyznaczoną przez ten porządek.