Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Paweł Parys
Nr albumu: 209216

Układy równań spełnione we wszystkich przemiennych półgrupach skończonych

Praca magisterska
na kierunku INFORMATYKA
w zakresie INFORMATYKI

Praca wykonana pod kierunkiem
dra Mikołaja Bojańczyka
Instytut Informatyki

Maj 2007

Oświadczenie kierującego pracą

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Data Podpis kierującego pracą

Oświadczenie autora (autorów) pracy

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Data Podpis autora (autorów) pracy

Streszczenie

Rozważany jest następujący problem: sprawdzić, czy dany układ równań ma rozwiązanie w każdej przemiennej półgrupie skończonej. Pokazano, że ten problem jest rozstrzygalny i NP-zupełny.

Słowa kluczowe

układ równań, równanie, półgrupa, półgrupa skończona, półgrupa przemienna, rozstrzygalność, NP-zupełność

Dziedzina pracy (kody wg programu Socrates-Erasmus)

11.3 Informatyka

Klasyfikacja tematyczna

F. Theory of Computation
F.2 Analysis of Algorithms and Problem Complexity
F.2.2 Nonnumerical Algorithms and Problems

Tytuł pracy w języku angielskim:

Systems of Equations Satisfied in All Commutative Finite Semigroups

Spis treści

Rozdział 1

Wstęp

Istnieją co najmniej dwa problemy związane z rozwiązywaniem układów równań w półgrupach. Pierwszym z nich jest rozwiązywanie układu równań w danej półgrupie wolnej. Algorytm rozstrzygający to zagadnienie został podany przez Makanina [6]. Drugim jest rozwiązywanie układu równań w danej półgrupie skończonej [5].

Innym interesującym problemem jest sprawdzanie, czy układ równań jest spełniony we wszystkich półgrupach na raz. Jednak można łatwo pokazać, że układ równań mający rozwiązanie w półgrupie wolnej, ma również rozwiązanie w każdej innej półgrupie. W tym sensie dla równań półgrupa wolna jest najtrudniejszą z półgrup, czyli algorytm Makanina rozstrzyga również ten problem. Natomiast dla półgrup skończonych ten argument już nie przechodzi. Istnieją układy, które mają rozwiązania we wszystkich półgrupach skończonych, ale nie w półgrupie wolnej. Dla przykładu w półgrupie skończonej, gdy dowolny element dodajemy do siebie wiele razy, to otrzymywane wyniki zaczną się powtarzać, co może powodować istnienie rozwiązania, którego by nie było w półgrupie wolnej. Tym sposobem łatwo można pokazać, że w każdej półgrupie skończonej istnieje element idempotentny (tzn. rozwiązanie równania $x + x = x$). To równianie nie ma rozwiązania w półgrupie wolnej (bez słów pustych). Rozwiązywanie innych równań będzie uogólnieniem tej obserwacji.

Dokładniej, następujący problem będzie rozważony: Dla danego układu równań (ze zmiennymi i współczynnikami) rozstrzygnij, czy w każdej półgrupie skończonej i dla każdego wartościowania współczynników w tej półgrupie istnieje jego rozwiązanie. Szukamy więc odpowiednika algorytmu Makanina dla półgrup skończonych.

Problem sprawdzania, czy układ równań ma rozwiązanie w każdej półgrupie skończonej, jest interesujący sam w sobie, lecz ma także pewną motywację. Istnieje odpowiedniość pomiędzy półgrupami skończonymi a językami regularnymi, więc pytania o półgrupy skończone są także pytaniami o języki regularne. Rozwiązywanie równań w półgrupach skończonych może być rozumiane jako uogólnienie pompowania. Co to znaczy, że układ równań ma rozwiązanie w każdej półgrupie skończonej? Jakąkolwiek półgrupę skończoną (automat skończony) weźmiemy, będą istniały takie wartości zmiennych, że w tej półgrupie lewe i prawe strony wyliczą się do tego samego elementu. Zatem używając tych wartości przechytrzymy tą (w ogólności dowolną) półgrupę: nie będzie ona umiała rozróżnić pomiędzy lewą i prawą stroną. Dla przykładu w niedawnych pracach na temat automatów chodzących po drzewach (tree-walking) zwykłe lematy o pompowaniu okazały się niewystarczające i wyniki o niewyrażalności zostały pokazane za pomocą równań w półgrupach. Na przykład w [1] dla każdej półgrupy i dla dowolnych a i b potrzebne jest istnienie u i v takich, że $u = u + a + u = u + b + v$ i $v = v + a + u = v + b + v$.

W tej pracy koncentruję się na półgrupach przemiennych i na problemie, czy układ ma

rozwiązanie w każdej przemiennej półgrupie skończonej.

Twierdzenie 1.1 *Następujący problem jest NP-zupełny: Czy dany układ równań ma rozwiązanie w każdej przemiennej półgrupie skończonej.*

Przypadek nieprzemienny pozostaje pytaniem otwartym.

Rozdział 2

Notacje i definicje

Ciągi liter jak $c_1, \ldots, c_m$ lub $X_1, \ldots, X_n$ itp. będą oznaczane przez $\bar{c}, \bar{X}, \ldots$ Kiedy potrzebuję rozważać jednocześnie wiele ciągów tego samego typu, używam indeksów górnych w nawiasach: $\bar{X}^{(1)}, \ldots, \bar{X}^{(h)}, \ldots$

Na działanie w półgrupie używam notacji addytywnej. Dla elementu a w półgrupie i $k \geqslant 1$ piszę $k \cdot a$, aby oznaczyć a dodane do siebie k razy.

Ustalam następujące niepuste alfabety:

$\Sigma_0 = \{X_1, \ldots, X_\gamma\}$ — alfabet *zmiennych*,

$\Sigma_1 = \{C_1, \ldots, C_\omega\}$ — alfabet *współczynników*.

Interpretacją współczynników w półgrupie S jest ciąg $\bar{c} = (c_1, \ldots, c_\omega)$ elementów S (element c_i odpowiada współczynnikowi C_i). Jest prościej traktować interpretację współczynników jako część półgrupy. Para $(S, \bar{c})$, składająca się z półgrupy i interpretacji współczynników w niej, będzie nazywana *półgrupą ze współczynnikami*. Od tego miejsca jako półgrupę będę rozumiał półgrupę ze współczynnikami i czasem będę pisał S zamiast $(S, \bar{c})$.

Układem równań $\bar{\phi}$ jest układ równości w postaci

$$\begin{cases} \phi_{11} = \phi_{12} \\ \ldots \\ \phi_{m1} = \phi_{m2}, \end{cases}$$

gdzie $\phi_{11}, \ldots, \phi_{m1}, \phi_{12}, \ldots, \phi_{m2}$ są niepustymi słowami nad $\Sigma_0 \cup \Sigma_1$. Czasem będę stawiał znaki plus pomiędzy symbolami w równaniach (dla większej czytelności). Dla danej półgrupy ze współczynnikami $(S, \bar{c})$ i ciągu $\bar{x}$ elementów z S, przez $\phi_{js}(\bar{x})$ oznaczam wylicznie ϕ_{js} w półgrupie S z c_i (i x_i) podstawionymi za C_i (i X_i). Dla danej półgrupy ze współczynnikami $(S, \bar{c})$, *rozwiązaniem* układu $\bar{\phi}$ jest ciąg $\bar{x} \in S$ taki, że $\phi_{i1}(\bar{x}) = \phi_{i2}(\bar{x})$ dla każdego $1 \leqslant i \leqslant m$.

Homomorfizmem półgrup ze współczynnikami z $(S, \bar{c})$ do $(S', \bar{c}')$ jest homomorfizm półgrup $f\colon S \to S'$ taki, że $f(c_i) = c'_i$ dla każdego i. Widzimy, że jeśli układ $\bar{\phi}$ ma rozwiązanie $\bar{x}$ w $(S, \bar{c})$ i mamy homomorfizm $f\colon (S, \bar{c}) \to (S', \bar{c}')$, to obraz $\bar{x}$ jest oczywiście rozwiązaniem w $(S', \bar{c}')$.

Będziemy krótko mówić, że układ *ma rozwiązanie w klasie FinComm*, jeśli dla każdej przemiennej półgrupy skończonej z współczynnikami istnieje rozwiązanie układu. Proszę zwrócić uwagę na kolejność kwantyfikatorów: dla każdej półgrupy i dla każdych wartości współczynników powinno dać się znaleźć wartości zmiennych, które tworzą rozwiązanie. W tej pracy przedstawiam algorytm rozwiązujący następujący problem:

> Wejście: Układ równań.
> Wyjście: Czy ten układ ma rozwiązanie w każdej przemiennej półgrupie skończonej ze współczynnikami?

Co by się stało, gdybyśmy pominęli słówko „skończone”? Jeśli układ ma rozwiązanie w każdej półgrupie przemiennej, to ma także w każdej (tj. o dowolnej licznie generatorów) przemiennej półgrupie wolnej. Istnieje homomorfizm z przemiennej półgrupy wolnej do dowolnej innej, więc z rozwiązania w przemiennej półgrupie wolnej dostajemy rozwiązanie w dowolnej innej półgrupie przemiennej. Zatem problem zredukowałby się do znajdowania rozwiązań w przemiennej półgrupie wolnej, co jest łatwe.

Rozdział 3

Specjalna postać równań: zmienne po obu stronach

Definicja 3.1 *Będę mówił, że równanie jest* zrównoważone*, jeśli na każdej jego stronie występuje co najmniej jedna zmienna. Będę mówił, że układ równań jest* zrównoważony*, jeśli każde równanie jest zrównoważone.*

Nasz problem jest nieco prostszy, jeśli rozważamy tylko układy zrównoważone. Na początku rozwiążę ten specjalny przypadek problemu. Wyniki z tego rozdziału zostaną użyte później do rozwiązywania przypadku ogólnego.

3.1. Jeden współczynnik

Na samym początku rozważę jeszcze prostszą postać układów, taką, że najwyżej jeden współczynnik występuje w układzie. Dowolny układ zrównoważony zostanie później sprowadzony do kilku takich układów. Następujące dwa twierdzenia mówią nam, że wystarczy rozwiązywać takie układy nad $\mathbb{Z}$.

Twierdzenie 3.2 *Niech C będzie współczynnikiem i niech $\bar{\phi}$ będzie zrównoważonym układem, w którym nie występują współczynniki inne niż C. Wówczas następujące warunki są równoważne:*

1. *układ $\bar{\phi}$ ma rozwiązanie w FinComm;*
2. *dla każdego $n \geqslant 1$ układ $\bar{\phi}$ ma rozwiązanie w grupie $\mathbb{Z}_n$ (liczb całkowitych modulo n) z interpretacją $C \mapsto 1$.*

Interpretacja współczynników innych niż C nie ma znaczenia, gdyż nie występują one w układzie, aczkolwiek dla ścisłości powinniśmy je jakoś ustalić.

W dowodzie powyższego twierdzenia użyję następującego faktu:

Fakt 3.3 *Dla danego elementu c półgrupy skończonej S istnieje N takie, że $2N \cdot c = N \cdot c$.*

Dowód Popatrzmy na wszystkie wielokrotności c. Ponieważ w S jest tylko skończenie wiele elementów, musi być $k \cdot c = (k + l) \cdot c$ dla pewnych $k, l \geqslant 1$. Dodając wielokrotnie $l \cdot c$ do tej równości dostajemy

$$k \cdot c = (k + l) \cdot c = (k + 2l) \cdot c = \ldots = (k + kl) \cdot c.$$

Dodając następnie do skrajnych wyrazów $(l-1)k \cdot c$ dostajemy $kl \cdot c = 2kl \cdot c$. Zatem możemy wziąć $N = kl$. ■

Dowód twierdzenia 3.2 $1 \Rightarrow 2$. Oczywiste, ponieważ 2 jest szczególnym przypadkiem 1.

$1 \Leftarrow 2$. Ustalmy przemienną półgrupę skończoną S z interpretacją $c \in S$ współczynnika C, dla której układ powinien mieć rozwiązanie. Niech N będzie takie, że $2N \cdot c = N \cdot c$ (z faktu 3.3). Mamy następujące własności dla wszystkich $k, l \geqslant 0$:

- zachodzi $(N+k) \cdot c + (N+l) \cdot c = (N+k+l) \cdot c$;
- jeśli dodatkowo $k \equiv l \pmod{N}$ to $(N+k) \cdot c = (N+l) \cdot c$.

Niech $\bar{y}$ będzie rozwiązaniem rozważanego układu w $\mathbb{Z}_N$ (rozumianym jako liczby od 0 do $N-1$), które istnieje z punktu 2. Bierzemy $x_j = (N+y_j) \cdot c$ dla wszystkich $1 \leqslant j \leqslant \gamma$. Wtedy dla każdego $1 \leqslant i \leqslant m$, $s = 1, 2$ mamy $\phi_{is}(\bar{x}) = (N + \phi_{is}(\bar{y})) \cdot c$. Skoro $\bar{y}$ jest rozwiązaniem w $\mathbb{Z}_n$, to $\phi_{i1}(\bar{y}) \equiv \phi_{i2}(\bar{y}) \pmod{N}$, więc $(N + \phi_{i1}(\bar{y})) \cdot c = (N + \phi_{i2}(\bar{y})) \cdot c$, co oznacza, że $\bar{x}$ jest rozwiązaniem w S. ■

Wiemy już zatem, że dla układu rozważanej postaci wystarczy istnienie jego rozwiązania w dowolnym $\mathbb{Z}_n$. Teraz okaże się, że istnienie rozwiązania w każdym $\mathbb{Z}_n$ oznacza tak naprawdę istnienie rozwiązania w $\mathbb{Z}$.

Twierdzenie 3.4 *Niech C będzie współczynnikiem i niech $\bar{\phi}$ będzie zrównoważonym układem równań, w którym nie występują współczynniki inne niż C. Wówczas następujące warunki są równoważne:*

1. *dla każdego $n \geqslant 2$ układ $\bar{\phi}$ ma rozwiązanie w grupie $\mathbb{Z}_n$ z interpretacją $C \mapsto 1$;*
2. *układ $\bar{\phi}$ ma rozwiązanie w grupie $\mathbb{Z}$ z interpretacją $C \mapsto 1$.*

Dowód $1 \Leftarrow 2$. Ta implikacja jest prawie oczywista. Dla każdego n istnieje homomorfizm z $\mathbb{Z}$ do $\mathbb{Z}_n$ (branie reszt z dzielenia przez n), więc jeśli mamy rozwiązanie w $\mathbb{Z}$, to mamy je także w $\mathbb{Z}_n$.

$1 \Rightarrow 2$. W tym twierdzeniu faktycznie mamy do czynienia ze zwykłymi układami równań na liczbach w $\mathbb{Z}$ lub $\mathbb{Z}_n$. Układ może być zapisany w postaci $\bar{\bar{a}} \cdot \bar{X} = \bar{b}$, gdzie $\bar{\bar{a}}$ i $\bar{b}$ są odpowiednio macierzą i wektorem liczb całkowitych oraz $\bar{X}$ jest wektorem zmiennych. Aby rozwiązać taki układ w $\mathbb{Z}$ możemy przeprowadzić eliminację Gaussa na parze $(\bar{\bar{a}}, \bar{b})$. Aby stałe pozostały w $\mathbb{Z}$ nie możemy dzielić równania przez liczbę, możemy jedynie mnożyć, ale to wystarczy. Jedyna różnica w porównaniu ze zwykłą eliminacją Gaussa (z dozwolonym dzieleniem) jest taka, że nie jesteśmy w stanie dostać jedynek „na przekątnej", dostajemy tam dowolne niezerowe liczby. Po ewentualnym przenumerowaniu zmiennych (zmianie kolejności kolumn w $\bar{\bar{a}}$) dostajemy następujący równoważny układ

$$\begin{bmatrix} a_{11} & 0 & 0 & \dots & 0 & a_{1,k+1} & a_{1,k+2} & \dots & a_{1\gamma} \\ 0 & a_{22} & 0 & \dots & 0 & a_{2,k+1} & a_{2,k+2} & \dots & a_{2\gamma} \\ 0 & 0 & a_{33} & \dots & 0 & a_{3,k+1} & a_{3,k+2} & \dots & a_{3\gamma} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{kk} & a_{k,k+1} & a_{k,k+2} & \dots & a_{k\gamma} \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ \vdots \\ X_k \\ X_{k+1} \\ X_{k+2} \\ \vdots \\ X_\gamma \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_k \\ b_{k+1} \\ \vdots \\ b_m \end{bmatrix},$$

gdzie $a_{11}, \ldots, a_{kk}$ są niezerowe.

Te same czynności możemy wykonać, gdy rozważamy układ w $\mathbb{Z}_n$. Dostaniemy wówczas taki sam układ (z wyjątkiem tego, że wszystkie liczby są traktowane modulo n). Tutaj otrzymany układ niekoniecznie jest równoważny początkowemu (podczas mnożenia przez liczbę, która ma wspólny dzielnik z n, równość z fałszywej może stać się prawdziwa). Jednak jeśli początkowy układ miał rozwiązanie, to ten także ma (dla każdego $\mathbb{Z}_n$).

Najpierw zauważmy, że $b_{k+1} = b_{k+2} = \ldots = b_m = 0$. Jeśli by tak nie było, to dla $b_i \neq 0$ mamy równanie $0 = b_i$, które powinno być spełnione we wszystkich półgrupach $\mathbb{Z}_n$, lecz nie jest w prawie wszystkich, np. dla dowolnego $n > b_i$.

Niech $n = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{kk}$. Niech $x_1, \ldots, x_\gamma$ będzie rozwiązaniem w tym $\mathbb{Z}_n$. Wtedy i-te równanie ($1 \leqslant i \leqslant k$) mówi, że

$$a_{ii}x_i + a_{i,k+1}x_{k+1} + a_{i,k+2}x_{k+2} + \ldots + a_{i\gamma}x_\gamma \equiv b_i \pmod{a_{11} \cdot a_{22} \cdot \ldots \cdot a_{kk}},$$

skąd mamy

$$a_{ii}x_i + a_{i,k+1}x_{k+1} + a_{i,k+2}x_{k+2} + \ldots + a_{i\gamma}x_\gamma \equiv b_i \pmod{a_{ii}},$$

co oznacza, że

$$a_{ii} | b_i - a_{i,k+1}x_{k+1} - a_{i,k+2}x_{k+2} - \ldots - a_{i\gamma}x_\gamma. \tag{3.1}$$

Jako rozwiązanie w $\mathbb{Z}$ bierzemy:

$$x'_i = \begin{cases} (b_i - a_{i,k+1}x_{k+1} - a_{i,k+2}x_{k+2} - \ldots - a_{i\gamma}x_\gamma) \cdot \frac{1}{a_{ii}} & \text{dla } 1 \leqslant i \leqslant k \\ x_i & \text{dla } k+1 \leqslant i \leqslant \gamma. \end{cases}$$

Warunek (3.1) zapewnia nam, że x'_i jest liczbą całkowitą. Łatwo sprawdzić, że powyższy wzór rzeczywiście opisuje rozwiązanie. ■

3.2. Wiele współczynników

Definicja 3.5 *Dla danego zrównoważonego układu $\bar{\phi}$ i współczynnika $C \in \Sigma_1$ definiujemy rzutowanie $\bar{\phi}^{(C)}$ jako układ otrzymany z $\bar{\phi}$ przez usunięcie wszystkich współczynników poza C.*

Zauważmy, że założenie, że $\bar{\phi}$ ma zmienną po każdej stronie (jest zrównoważony) gwarantuje, że $\bar{\phi}^{(C)}$ również ma zmienną po każdej stronie. W szczególności strony są niepuste, więc dostajemy dobrze określony układ.

Lemat 3.6 *Niech $\bar{\phi}$ będzie układem zrównoważonym. Wówczas następujące warunki są równoważne:*

1. *układ $\bar{\phi}$ ma rozwiązanie w FinComm;*
2. *dla każdego współczynnika $C \in \Sigma_1$ i $n \geqslant 2$ układ $\bar{\phi}^{(C)}$ ma rozwiązanie w grupie $\mathbb{Z}_n$ z interpretacją $C \mapsto 1$.*

Dowód $1 \Rightarrow 2$. Prawie oczywiste. Ustalmy C i n. Jako szczególny przypadek 1 dostajemy, że układ $\bar{\phi}$ ma rozwiązanie w $\mathbb{Z}_n$ z interpretacją $C \mapsto 1$ oraz $D \mapsto 0$ dla wszystkich $D \in \Sigma_1$, $D \neq C$. Ale to rozwiązanie jest także rozwiązaniem $\bar{\phi}^{(C)}$, ponieważ strony $\bar{\phi}$ i $\bar{\phi}^{(C)}$ wyliczają się w ten sam sposób (jedyną różnicą jest to, że w $\bar{\phi}$ pewną liczbę razy jeszcze dodajemy 0).

$1 \Leftarrow 2$. Ustalmy przemienną półgrupę skończoną S ze współczynnikami $\bar{c}$. Z założenia 2 i twierdzenia 3.2 dla każdego $C_i \in \Sigma_1$ mamy rozwiązanie $\bar{x}^{(C_i)}$ rzutowania $\bar{\phi}^{(C_i)}$ w S. Jako nasze rozwiązanie całego układu bierzemy sumę tych rozwiązań: $x_j = x_j^{(C_1)} + x_j^{(C_2)} + \ldots + x_j^{(C_\omega)}$ dla każdego $1 \leqslant j \leqslant \gamma$. Wówczas strona równania będzie się wyliczała jako suma wyliczeń stron równań dla jednego współczynnika:

$$\phi_{ks}(\bar{x}) = \phi_{ks}^{(C_1)}(\bar{x}^{(C_1)}) + \phi_{ks}^{(C_2)}(\bar{x}^{(C_2)}) + \ldots + \phi_{ks}^{(C_\omega)}(\bar{x}^{(C_\omega)}).$$

Tak jest ponieważ każde c_i i $x_j^{(C_i)}$ pojawia się taką samą liczbę razy w $\phi_{ks}(\bar{x})$ jak w $\phi_{ks}^{(C_i)}(\bar{x}^{(C_i)})$ i nie pojawia się w żadnym innym elemencie. Oczywiście użyliśmy założenia, że półgrupa jest przemienna. ■

Jako natychmiastowy wniosek z lematu 3.6 i twierdzenia 3.4 dostajemy następujące twierdzenie:

Twierdzenie 3.7 *Niech $\bar{\phi}$ będzie układem zrównoważonym. Wówczas następujące warunki są równoważne:*

1. *układ $\bar{\phi}$ ma rozwiązanie w FinComm;*
2. *dla każdego współczynnika $C \in \Sigma_1$ układ $\bar{\phi}^{(C)}$ ma rozwiązanie w grupie $\mathbb{Z}$ z interpretacją $C \mapsto 1$.*

Zatem otrzymaliśmy łatwe kryterium spradzania, czy układ zrównoważony ma rozwiązanie w klasie *FinComm*.

Rozdział 4

Przypadek ogólny

4.1. Zamiana kwantyfikatorów

Udowodnię teraz ważny lemat techniczny, który upraszcza dalszą argumentację. Tutaj potrzebujemy wersji dla przemiennych półgrup skończonych, lecz taki sam lemat jest prawdziwy dla dowolnych półgrup skończonych.

Lemat 4.1 *Niech $\{\bar{\phi}^{(1)}, \ldots, \bar{\phi}^{(N)}\}$ będą układami równań takimi, że w każdej przemiennej półgrupie skończonej z współczynnikami pewien $\bar{\phi}^{(i)}$ ma rozwiązanie. Wówczas pewien układ $\bar{\phi}^{(i)}$ ma rozwiązanie w każdej z tych półgrup.*

Dowód Załóżmy przeciwnie, że dla każdego układu $\bar{\phi}^{(i)}$ istnieje półgrupa S_i, w której $\bar{\phi}^{(i)}$ nie ma rozwiązania. Spójrzmy na półgrupę produktową $S = S_1 \times \ldots \times S_N$ (naturalnie interpretacją współczynnika w S jest ciąg jego interpretacji w każdym S_i). Pewien układ $\bar{\phi}^{(i)}$ musi mieć rozwiązanie w S. Ale mamy homomorfizm z S do S_i (rzutowanie), więc $\bar{\phi}^{(i)}$ ma także rozwiązanie w S_i. Lecz założyliśmy, że nie ma, dostaliśmy sprzeczność, zatem twierdzenie jest prawdziwe. ■

4.2. Usuwanie „złych" zmiennych

Niech $\bar{\phi}$ będzie układem, w którym w pewnym równaniu po którejś stronie znajdują się wyłącznie współczynniki, a po drugiej stronie są także zmienne. Zamienimy taki układ na wiele prostszych układów. Dla uproszczenia notacji załóżmy, że zdarzyło się to w pierwszym równaniu, że po prawej stronie tego równania (ϕ_{12}) są same współczynniki, a po jego lewej stronie (ϕ_{11}) występuje co najmniej zmienna X_1. Dla słowa współczynników $w \in \Sigma_1^*$ określimy układ $\bar{\phi}^{(w)}$. Będzie to $\bar{\phi}$ w którym zamieniamy każde wystąpienie X_1 w każdym równaniu przez słowo w. Będziemy rozważać te układy dla wszystkich niepustych podciągów prawej strony pierwszego równania (tak naprawdę kolejność współczynników w w nie ma znaczenia, gdyż mamy tylko półgrupy przemienne, więc możemy także myśleć o wszystkich podmultizbiorach ϕ_{12}). Oczywiście jest tylko skończenie wiele takich podciągów.

Poniższe twierdzenie pozwoli nam usunąć z układu jedno niezrównoważone równanie. Stosując je wielokrotnie uda nam się sprowadzić każdy układ do układu zrównoważonego.

Twierdzenie 4.2 *Dla układu $\bar{\phi}$ jak wyżej, układ ma rozwiązanie w FinComm wtedy i tylko wtedy, gdy dla pewnego w — podciągu ϕ_{12}, układ $\bar{\phi}^{(w)}$ ma rozwiązanie w FinComm.*

Dowód $\Leftarrow$. Niech w będzie podciągiem ϕ_{12}, dla którego $\phi^{(w)}$ ma rozwiązanie w *FinComm*. Ustalmy przemienną półgrupę skończoną ze współczynnikami S, w której szukamy rozwiązania układu $\bar{\phi}$. Niech $\bar{x}$ będzie rozwiązaniem układu $\bar{\phi}^{(w)}$ w niej. Jako rozwiązanie układu $\bar{\phi}$ możemy wziąć wynik wyliczenia w jako x_1 oraz wartości z $\bar{x}$ jako pozostałe zmienne. Wtedy strony układów $\bar{\phi}$ i $\bar{\phi}^{(w)}$ wyliczają się do tego samego, więc to jest rozwiązanie układu $\bar{\phi}$ (jedyna różnica pomiędzy $\bar{\phi}$ i $\bar{\phi}^{(w)}$ jest taka, że na miejscu X_1 mamy w, ale obie te rzeczy wyliczają się do tego samego).

$\Rightarrow$. Zgodnie z lematem 4.1 wystarczy pokazać, że w każdej przemiennej półgrupie skończonej dla każdej interpretacji współczynników co najmniej jeden z tych układów ma rozwiązanie. Wtedy wspomniany lemat zagwarantuje nam, że jeden z tych układów będzie miał rozwiązanie w każdej z tych półgrup.

Ustalmy przemienną półgrupę skończoną ze współczynnikami S, dla której szukamy rozwiązania pewnego z układów $\bar{\phi}^{(w)}$. Skonstruujemy półgrupę ze współczynnikami S' i na podstawie rozwiązania $\bar{\phi}$ w niej, skonstruujemy rozwiązanie pewnego $\bar{\phi}^{(w)}$ w S. Niech N będzie długością ϕ_{12} (czyli prawej strony pierwszego równania, która zawiera wyłącznie współczynniki). Półgrupa S' będzie zawierała dwie rozłączne części:

1. wszystkie elementy S;
2. wszystkie przemienne słowa (multizbiory) współczynników z Σ_1 o długości nie większej niż N.

Potrzebujemy jeszcze określić działanie. W obrębie S dodajemy po prostu jak w S. Kiedy dodajemy pomiędzy częściami, obliczamy słowo współczynników w S i potem dodajemy w S. Kiedy dodajemy dwa słowa współczynników, łączymy je (konkatenujemy). Jeśli wynik mieści się w drugiej części (ma długość $\leqslant N$), bierzemy go. Jeśli jest dłuższy, obliczamy go w S. Pomysł jest taki, że S' dla krótkich słów udaje przemienną półgrupę wolną. Słowa nie dłuższe niż N są zapamiętywane same w sobie, dla dłuższych słów pamiętamy tylko ich wartość w S.

Interpretację współczynników w S' bierzemy taką, że współczynnik jest interpretowany jako jednoliterowe słowo zawierające go. S' jest przemienną półgrupą skończoną, więc $\bar{\phi}$ ma rozwiązanie $\bar{x}'$ w niej. Zauważmy, że jeśli coś jest już w pierwszej części, to po dodaniu czegokolwiek, nadal pozostanie w tej części. Prawa strona pierwszego równania, która zawiera N współczynników, w S' wyliczy się do samej siebie w drugiej części. To oznacza, że x'_1 (i cała lewa strona) jest także w drugiej części. Co więcej, x'_1 jest podmultizbiorem prawej strony. Bierzemy to x'_1 jako słowo w. Teraz potrzebujemy mieć rozwiązanie układu $\bar{\phi}^{(w)}$ w S. Jako x_i (dla $2 \leqslant i \leqslant \gamma$) weźmiemy x'_i kiedy jest ono w pierwszej części lub wyliczenie x'_i w S, jeśli jest ono w drugiej części. Łatwo zauważyć, że $\bar{\phi}^{(w)}$ daje nam te same równości, co $\bar{\phi}$ wcześniej (kiedy równanie z $\bar{\phi}$ w S' dawało równość na słowach, to zachodzi ona także po wyliczeniu stron w S). Zatem to jest rozwiązanie w S, co kończy dowód. ■

4.3. Algorytm

Twierdzenie 4.2 prawie daje nam algorytm. W każdej chwili będziemy mieć zbiór układów, o których chcemy wiedzieć, czy co najmniej jeden z nich ma rozwiązanie w *FinComm*. Na samym początku zbiór ten zawiera wyłącznie oryginalny układ. Następnie w kółko zamieniamy układ, w którym w którymś równaniu zmienne są tylko po jednej stronie, przez pewną liczbę układów, jak opisano powyżej. Zauważmy, że w wyniku takiego kroku otrzymujemy układy zawierające mniej zmiennych, więc ten proces musi się skończyć. Ostatecznie dostajemy zbiór

układów, w których w każdym równaniu po każdej stronie jest co najmniej zmienna lub nie ma zmiennych po żadnej stronie.

Zobaczmy teraz co się dzieje, jeśli w równaniu są same współczynniki. Jeśli liczba współczynników każdego rodzaju jest taka sama po obu stronach (strony są równe jako multizbiory), to równanie to jest zawsze spełnione, bo nasze półgrupy są przemienne. W tym przypadku możemy po prostu usunąć to równanie i dostajemy równoważny układ. W przeciwnym przypadku istnieje współczynnik C, który po lewej stronie występuje k razy, a po prawej stronie l razy, gdzie $k \neq l$. Rozważmy grupę $\mathbb{Z}_{k+l+1}$ z interpretacją $C \mapsto 1$ oraz $D \mapsto 0$ dla wszystkich $D \in \Sigma_1$, $D \neq C$. Tutaj lewa strona wylicza się do k, a prawa do l, które nie są równe, więc równianie nie jest spełnione. To oznacza, że możemy natychmiast powiedzieć, że układ zawierający takie równanie nie może mieć rozwiązania w *FinComm*.

Ostatecznie dostajemy zbiór układów zrównoważonych; chcemy stwierdzić, czy któryś z nich ma rozwiązanie w *FinComm*. Ale dla takich układów to może być rozstrzygnięte przez algorytm z rozdziału 3.

Rozdział 5

Złożoność

W tym rozdziale udowodnię, że rozważany problem jest NP-zupełny. Najpierw pokażę, że rozważany problem jest w NP. Oczywiście użyję algorytmu opisanego powyżej w pracy. Aby algorytm rzeczywiście działał w NP, trzeba wybrać odpowiedni sposób reprezentacji układu. Najprostszy (choć nie wystarczająco dobry) sposób to pamiętanie równania tak, jak ono wygląda, jako listę współczynników i zmiennych. Jeślibyśmy używali tej reprezentacji, to podczas działania naszego algorytmu rozmiar układu może wzrosnąć wykładniczo, czyli nie działałby on w NP. Ale możemy zrobić to lepiej: strona równania będzie opisana przez liczby wystąpień każdego symbolu (współczynnika i zmiennej). Zatem jeśli symbol powtarza się N razy, to będzie zapamiętany zapis binarny liczby N, który ma długość $\Theta(\log N)$.

Ogólnie rzecz biorąc algorytm składa się z dwóch części. W pierwszej części wielokrotnie usuwamy zmienną z niezrównoważonego równania i zastępujemy ją pewnym podciągiem drugiej strony równania (rozdział 4.2). Zauważmy, że w modelu niedeterministycznym możemy po prostu zgadnąć właściwe podstawienie zamiast sprawdzać wszystkie możliwości. W drugiej części rozwiązujemy zrównoważony układ równań nad $\mathbb{Z}$. To może być zrobione w NP (patrz [2], rozwiązanie będzie miało rozmiar wielomianowy, więc możemy je zgadywać).

Pozostaje jedynie pytanie, jaka jest długość układu po pierwszej części. Potrzebujemy pokazać, że większy się ona najwyżej wielomianowo. Niech V_i oraz B_i będą całkowitymi liczbami wystąpień odpowiednio zmiennych i współczynników po i-tym kroku algorytmu (w szczególności V_0 i B_0 są tymi liczbami w początkowym układzie). Zauważmy, że długość początkowego układu to co najmniej $\Omega(\log |V_0+B_0|)$. W i-tym kroku podstawiamy za zmienną najwyżej B_{i-1} współczynników, a zmienna występuje najwyżej V_{i-1} razy, więc

$$B_i \leqslant B_{i-1} + V_{i-1}B_{i-1} = (V_{i-1}+1)B_{i-1}.$$

Liczba wystąpień zmiennych nawet maleje, czyli $V_i \leqslant V_{i-1}$. Po k krokach mamy: $V_k \leqslant V_0$ oraz $B_k \leqslant (V_0+1)^k B_0$. Niech N będzie długością początkowego układu, $\gamma \leqslant N$ — liczbą różnych zmiennych oraz $\omega \leqslant N$ — liczbą różnych współczynników. W każdym kroku usuwamy jedną zmienną, jest więc co najwyżej $k \leqslant \gamma \leqslant N$ kroków. Długość wynikowego układu będzie wynosiła najwyżej:

$$\begin{aligned} 2m(\gamma \log V_k + \omega \log B_k) &\leqslant 2N^2(\log V_0 + \log((V_0+1)^N B_0)) = \\ &= 2N^2(\log V_0 + N\log(V_0+1) + \log B_0) \leqslant \\ &\leqslant O(N^3)O(\log|V_0+B_0|) \leqslant O(N^4), \end{aligned}$$

więc jest wielomianowa.

Pokażę teraz, że rozważany problem jest NP-trudny. Aby to zrobić, zredukuję do niego NP-zupełny problem kliki (zdefiniowany w [3]). Załóżmy, że poszukujemy kliki rozmiaru k w

grafie $G = (V, E)$. Załóżmy, że $V = \{1, 2, \ldots, |V|\}$. Będziemy mieli tylko jeden współczynnik C. Będziemy mieli zmienne X_i dla każdego wierzchołka oraz pomocnicze zmienne X'_i i X''_{ij} dla każdego wierzchołka i dla każdej pary wierzchołków. Równania są następujące:

$$\begin{cases} X_1 + X_2 + \ldots + X_{|V|} = (|V| + k) \cdot C & \\ X_i + X'_i = 3 \cdot C & \text{dla każdego } i \in V \\ X_i + X_j + X''_{ij} = 4 \cdot C & \text{dla każdego } (i,j) \notin E. \end{cases}$$

Jeśli istnieje klika rozmiaru k, to będziemy mieli rozwiązanie w każdej przemiennej półgrupie skończonej (a nawet w przemiennej półgrupie wolnej). Bierzemy $X_i = 2 \cdot C$ jeśli wierzchołek i jest w klice lub $X_i = C$ jeśli nie jest. Pierwsze równanie jest spełnione, bo jest dokładnie k wierzchołków w klice. Równania drugiego i trzeciego rodzaju mogą być spełnione, przez wzięcie X'_i i X''_{ij} równego C lub $2 \cdot C$ w zależności od potrzeb. Jeśli nie ma krawędzi (i, j), wtedy najwyżej jeden z wierzchołków i i j jest w klice, więc jest możliwe spełnienie równań trzeciego rodzaju.

Jeśli jest rozwiązanie w każdej przemiennej półgrupie skończonej, to jest też pewno rozwiązanie $\bar{x}$ w następującej półgrupie S: Elementami S są $\{1, 2, \ldots, M\}$ dla wystarczająco dużego $M = \max(5, |V| + k + 1)$. Działanie $a + b$ jest zdefiniowane jako $\min(M, a + b)$. Współczynnik C wylicza się do 1. Z równania drugiego rodzaju widzimy, że $x_i = 1$ lub 2. Bierzemy wierzchołek i do kliki wtedy i tylko wtedy, gdy $x_i = 2$. Równania trzeciego rodzaju gwarantują, że dwa wierzchołki nie mogą być w klice, jeśli nie ma między nimi krawędzi. Pierwsze równanie mówi, że klika ma rozmiar k.

Co ciekawe, jak łatwo można sprawdzić, jeśli powyższy układ równań ma rozwiązanie we wspomnianej półgrupie skończonej, to jest ono także rozwiązaniem w półgrupie wolnej (o jedym generatorze). Przy okazji dowiedliśmy więc także NP-trudności problemu rozwiązywania układów równań w przemiennej półgrupie wolnej.

Rozdział 6

Inne pytania

Innymi ciekawymi zagadnieniami może być sprawdzanie, czy układ ma rozwiązanie w innych klasach półgrup, na przykład we wszystkich półgrupach skończonych lub wszystkich idempotentnych półgrupach skończonych.

Dla idempotentnych półgrup skończonych to pytanie jest proste, gdyż wiemy, że jest tylko skończenie wiele półgrup idempotentnych o danej liczbie generatorów (co więcej, wszytskie są skończone) — patrz [4]. Co więcej, wszystkie te półgrupy mogą być wymienione, gdyż istnieje wzór ograniczający z góry liczbę elementów w takiej półgrupie. Wystarczy więc sprawdzić, czy układ ma rozwiązanie we wszystkich półgrupach idempotentnych generowanych przez nasze współczynniki, co możemy zrobić półgrupa po półgrupie. Dla dowolnej półgrupy, jeśli istnieje rozwiązanie w podpółgrupie generowanej przez współczynniki, to jest ono także rozwiązanie w całej półgrupie.

Sprawdzanie, czy układ jest spełniony we wszystkich półgrupach skończonych, pozostaje pytaniem otwartym.

Bibliografia

[1] M. Bojańczyk, T. Colcombet, *Tree-walking automata cannot be determinized* Theoretical Computer Science, Volume 350, Issues 2-3, (Feb., 2006), pages 164-173

[2] I. Borosh, L.B. Trebig, *Bounds on positive integral solutions of linear Diophantine equations* Proc. Amer. Math. Soc. 55 (1976), 299304

[3] R.M. Karp, *Reducibility Among Combinatorial Problems* Complexity of Computer Computations, Proc. Sympos. IBM Thomas J. Watson Res. Center, Yorktown Heights, New York (1972), pages 85-103

[4] D. McLean, *Idempotent semigroups*, The American Mathematical Monthly, Volume 61, Number 2 (Feb., 1954), pages 110-113

[5] O. Klíma, P. Tesson, D. Thérien, *Dichotomies in the Complexity of Solving Systems of Equations over Finite Semigroups* Electronic Colloquium on Computational Complexity, Report 091 (2004)

[6] G.S. Makanin, *The problem of solvability of equations in a free semigroup* Mathematics of the USSR – Sbornik, Volume 32 (1977), pages 129-198