38 Złożoność

Lemat 38.1 *Dla każdego równania słowowego $R(\vec{x})$ ze zmiennymi $\vec{x}$ istnieje układ równań słowowych $U(\vec{x}, \vec{y}$ ze zmiennymi $\vec{x}$ i $\vec{y}$, który jest równoważny R w tym sensie, że*

$$R(\vec{x}) \iff \exists \vec{y} U(\vec{x}, \vec{y}),$$

w którym każda zmienna występuje $\leqslant 3$ razy.

38.1 Problemy

Rozważamy równania w słowach i zakładamy, że dla równania R symbolami V i A będziemy oznaczać odpowiednio zbiór zmiennych i stałych, które mają prawo wystąpić w R. O zbiorze A zakładamy, że ma przynajmniej dwa elementy.

Trzy główne problemy, którymi będziemy się zajmować są następujące:

Problem 38.1 (niesprzeczności równań w słowach)
Dane: (dowolne) równanie w słowach R.
Zadanie: czy istnieje rozwiązanie równania R?

Problem 38.2 (niesprzeczności równań z regularnymi więzami)
Dane: równanie w słowach R i język regularny $L_v \subseteq A^*$ dla każdej zmiennej v występującej w R.
Zadanie: czy istnieje rozwiązanie równania R, które zmiennej zmiennej v występującej w R przyporządkowuje słowo z języka L_v?

Problem 38.3 (niesprzeczności układu równań w słowach)
Dane: układ równań w słowach U.
Zadanie: czy istnieje rozwiązanie układu U?

Będą nas też interesować pewne podproblemy podanych problemów.

Problem 38.4 (niesprzeczności równań z n zmiennymi)
Dane: równanie w słowach R, w którym występuje $\leqslant n$ zmiennych ($|V| \leqslant n$).
Zadanie: czy istnieje rozwiązanie równania R?

Problem 38.5 (niesprzeczności kwadratowych równań w słowach)
Dane: kwadratowe równanie w słowach R
Zadanie: czy istnieje rozwiązanie równania R?

Problem 38.6 (istnienie specjalnych rozwiązań równań w słowach)
Dane: równanie w słowach R i pewne zależności postaci $|v_i| \leqslant |v_j|$ dla $v_i, v_j \in V$,
Zadanie: czy istnieje rozwiązanie równania R spełniające podane zależności?

Problem 38.7 (istnienie ograniczonych rozwiązań równań w słowach)
Dane: równanie w słowach R i pewne ograniczenia długości, np. długości składowych rozwiązania lub sumy długości składowych rozwiązania są mniejsze od podanych liczb, lub też tego typu ograniczenia zależne od długości równania
Zadanie: czy istnieje rozwiązanie równania R spełniające podane ograniczenia?

Problem 38.8 (istnienie rozwiązań równań w słowach o danych długościach)
Dane: równanie w słowach R i długości składowych rozwiązania,
Zadanie: czy istnieje rozwiązanie równania R ze składowymi o podanych długościach?

Problem 38.9 (niesprzeczności układu równań w słowach, w którym każda zmien-na występuje $\leqslant n$ razy)

Dane: układ równań w słowach U, w którym każda zmienna występuje $\leqslant n$ razy
Zadanie: czy istnieje rozwiązanie układu U?

Problem 38.10 (istnienie ograniczonego rozwiązania układu równań w słowach,w którym każda zmienna występuje $\leqslant n$ razy)

Dane: układ równań w słowach U, w którym każda zmienna występuje $\leqslant n$ razy
Zadanie: czy istnieje rozwiązanie układu U spełniające podane ograniczenia?

38.2 Górne ograniczenia złożoności

Rozmiarem równania w słowach $u = v$ jest długość słowa $| uv |$. Rozmiarem układu równań jest suma rozmiarów poszczególnych równań.

Lemat 38.2 *Problemy 38.1, 38.3 i 38.9 dla* $n \geqslant 3$ *są wielomianowo równoważne.* □

38.2.1 Ogólny problem niesprzeczności

Do 1977 roku nie było wiadomo, czy problem 38.1 niesprzeczności równań w słowach jest rozstrzygalny. W podanym roku Makanin dowiódł rozstrzygalności problemu podając tzw. algorytm Makanina. Analiza algorytmu Makanina dokonana przez Jaffara i (później) Schulza pozwala stwierdzić, że problem 38.1 należy do klasy 4-NEXPTIME, a więc można algorytm Makanina zrealizować na niedeterninistycznej maszynie Turinga, która po uruchomieniu z równaniem rozmiaru n wykonuje

$$\leqslant 2^{2^{2^{2^n}}}$$

rozkazów.

Podane oszacowanie było kilkakrotnie poprawiane. Z Leszkiem Pacholskiego pokazaliśmy, że można poprawić oszacowania złożoności algorytmu Makanina i problem 38.1 należy do 3-NEXPTIME. Później Gutiérrez dowiódł, że ten problem jest w klasie EXPSPACE. Najlepsze oszacowania złożoności problemu niesprzeczności równań w słowach wynikają z prac Plandowskiego. Pokazał on najpierw, że problem 38.1 jest w klasie NEXPTIME, a następnie poprawił ten rezultat umieszczając problem 38.1 w PSPACE. W tej chwili jest to chyba najlepsze górne oszacowanie złożoności problemu 38.1. Prace Plandowskiego wykraczają poza metody wykorzystywane przez Chmielewskiego i Makanina.

38.2.2 Złożoność podproblemów problemu niesprzeczności

Twierdzenie 38.3 *Problem 38.4 dla $n = 2$ niesprzeczności równań w słowach z dwoma zmiennymi jest wielomianowy.*

Dowód. Twierdzenie to dowodzi się przez szczegółową analizę algorytmu Chmielewskiego. □

Lemat 38.4 *Istnieje niedeterministyczny algorytm, który dla danego kwadratowego układu U równań w słowach bada niesprzeczność U i ma złożoność pamięciową zależną liniowo od $|U|$.*

Twierdzenie 38.5 *Problem istnienia rozwiązania kwadratowego układu równań w słowach o danych długościach składowych można rozwiązać w czasie liniowym (rozmiar danych to rozmiar układu powiększony o sumę długości binarnych przedstawień danych liczb).*

Dowód. Najpierw z układu usuwamy wszystkie równania postaci $x = y$. Następnie dany układ rozmiaru d zastępujemy równoważnym kwadratowym układem złożonym z równań postaci $x = yz$ (x jest zmienną, y i z to zmienne lub stałe). Np. równanie $xyz = uwv$ można zastąpić układem $xy = p_1$, $uw = p_2$, $p_1 z = p_3$ i $p_2 v = p_3$. Jeżeli każde równanie danego układu tak przekształcimy, to otrzymamy układ o rozmiarze $\leqslant 3d$ zawierający najwyżej $\leqslant d$ nowych zmiennych. Długości nowych zmiennych są łatwe do wyliczenia i są sumami długości $\leqslant d$ starych zmiennych. Jeżeli stare zmienne miały długości $\leqslant d'$, to każda nowa ma długość $\leqslant d + d'$, a wszystkie razem mają przedstawienia o długości $\leqslant (d + d')d$.

Z przeprowadzonych rozważań wynika, że twierdzenie wystarczy dowieść dla kwadratowych układu E złożonego z równań postaci $x = yz$. Przyjmijmy, że jeżeli x jest zmienną, to $|x|$ oznacza długość x-owej składowej rozwiązania, czyli jedną z danych liczb. Możemy też założyć, że jeżeli $x = yz \in E$, to $|x| = |y| + |z|$, a także, że $lhx > 0$ dla każdej zmiennej x.

Zmienna x jest definiowana w układzie E, jeżeli E jest równanie postaci $x = yz$. Zmienna x jest podwójnie definiowana w ukladzie E, jeżeli w E są dwa równania $x = yz$ i $x = uv$. Nietrudno zauważyć, że jeżeli w układzie nie ma zmiennych podwójnie definiowanych, to po nadaniu zmiennym, które nie są definiowane dowolnych wartości jednoznacznie możemy określić wartości pozostałych zmiennych tak, aby całe równanie było spełnione.

Wagą układu E nazywamy liczbę

$$W(E) = |V| + dd(E) + \frac{3}{-\log_2(c)} \sum_{v \in V} \log_2 |x|,$$

gdzie c jest pewną liczbą (zostanie sprecyzowana poźniej) spełniającą nierówności $1/2 < c < 1$, a V oznacza zbiór zmiennych występujących w E. Dodatkowo sumę występującą we wzorze na wagę oznaczmy symbolem

$$S(E) = \sum_{v \in V} \log_2 |x|.$$

W przypadku, gdy $dd(E) > 0$ będziemy układ E zastępować innym układem E' którego obliczenie wymaga stałego czasu i takim, że $W(E') \leqslant W(E) - 1$. Zauważmy, że rozmiar $r(E)$ układu E jest

$$\geqslant |V| + dd(E) + \sum_{v \in V} \log_2 |x|$$

oraz

$$k = \frac{3}{-\log_2(c)} \geqslant 3,$$

więc

$$W(E) \leqslant k \cdot r(E).$$

Wobec tego przedstawiony plan pozwala dowieść tezę.

Przypuśćmy,że z jest zmienną podwójnie definiowaną w E oraz

$$E = E_0 \cup \{z = xy, z = uv, R(x)\},$$

gdzie x jest zmienną taką, że $|x| \geqslant |u|$, a $R(x)$ jest drugim równaniem w E, w którym występuje x. Zauważmy, że z i x nie występują już w E_0. W takiej sytuacji, jeżeli mamy układy E i E' różniące się zmiennymi, to będziemy je nazywać równoważnymi, jeżeli rozwiązanie pierwszego z układów daje się rozszerzyć do rozwiązania drugiego i odwrotnie.

Przypadek 1: $| x | = | u |$. Zamiast rozwiązywać E możemy rozwiązywać równoważny mu układ

$$E' = E_0 \cup \{x = u, y = v, R(x)\}$$

(można go jeszcze trochę uprościć usuwając równania $x = u$ i $y = v$). Zauważmy, że w układzie E' nie występuje zmienna z, ale każda ze zmiennych x, y, u lub v mogła stać się podwójnie zdefiniowana. Usunięcie z zmniejsza $W(E)$ o 2, pojawienie się nowych podwójnie zdefiniowanych zmiennych zwiększa o $\leqslant 4$. Usuwając z E' niepotrzebne zmienne (korzystając z równości $x = u$ i $y = v$) można wyeliminować efekt zwiększenia liczby podwójnie zdefiniowanych zmiennych. Ostatecznie można przyjąć, że $W(E') \leqslant W(E) - 2$.

Przypadek 2: $| u | < | x |$.

Przypadek 2.1: $|x|-|u| \leqslant c|z|$. Teraz bierzemy nową zmienną w i przypisujemy jej długość $| w | = | x | - | u |$. Niech

$$E' = E_0 \cup \{x = uw, v = wy, R(x)\}.$$

Układ E' jest równoważny z E. Zmienna z zostaje zastąpiona przez w, suma $S(E)$ zmniejsza się o $\log_2(1/c) = -\log_2 c$. Stąd ostatni składnik $W(E)$ zmniejsza się o 3. Jednocześnie $dd(E')$ może być większe od $dd(E)$ tylko o jeden. Ostatecznie $W(E') \leqslant W(E) - 2$.

Przypadek 2.2: $| x | - | u | > c| z |$.

Przypadek 2.2.1: x jest definiowana (równaniem $R(x)$ równym $x = pq$).

Przypadek 2.2.1.1: $| p | \geqslant c| z |$. Weźmy nową zmienną r o długości $| z | - | p |$. Niech

$$E' = E_0 \cup \{z = pr, r = qy, z = uv\}.$$

układy E i E' są równoważne. Pojawiła się więc nowa zmienna r, zniknęła zmienna x, więc suma dwóch pierwszych składników $W(E)$ nie zmieniła się. Z drugiej strony,

$$| z | = | pr | \geqslant | p | \geqslant c| z |.$$

Stąd $(1-c)|\,z\,| \geqslant |\,r\,|$. Mamy także $|\,x\,| > |\,x\,| - |\,u\,| > c|\,z\,|$. Suma z $W(E)$ zmieniła się o

$$S(E) - S(E'') = \log_2|\,x\,| - \log_2|\,r\,| \geqslant \log_2(c|\,z\,|) - \log_2((1-c)|\,z\,|) = \log_2(\frac{c}{1-c}).$$

Wobec tego

$$\frac{3}{-\log_2 c}(S(E) - S(E'')) \leqslant \frac{3}{-\log_2 c}\log_2(\frac{c}{1-c}) > 1$$

dla $c = 0.55$.

Tak więc ostatni składnik $W(E)$ zmniejszył się przynajmniej o 1. Stąd cała waga $W(E)$ zmniejszyła się przynajmniej o 1.

Przypadek 2.2.1.2: $|\,p\,| < c|\,z\,|$. Przypomnijmy, że teraz $|\,x\,| - |\,u\,| > c|\,z\,|$. Mamy też

$$|\,z\,| = |\,xy\,| \geqslant |\,x\,| = |\,u\,| + (|\,x\,| - |\,u\,|) \geqslant |\,x\,| - |\,u\,| \geqslant c|\,z\,|,$$

a więc $|\,u\,| \leqslant (1-c)|\,z\,|$.

Przypadek 2.2.1.2.1: $|\,u\,| = |\,p\,|$. W tym przypadku układ E jest równoważny

$$E' = E_0 \cup \{u = p, v = qy\}$$

o mniejszej liczbie zmiennych (usunęliśmy z i x, z przestała być podwójnie definiowana). Za to trzy zmienne (u, p i v) mogą stać się podwójnie definiowane. Jeżeli u lub p nie stała się podwójnie definiowana, to $W(E)$ zminiejszyło się przynajmniej o 1. Jeżeli u i p są podwójnie definiowane, to możemy usunąc np. p podstawiając u za p. W ten sposób $W(E)$ zmniejszy się o 1.

Przypadek 2.2.1.2.2: $|\,u\,| < |\,p\,|$. Weźmy zmienną w o długości $|\,x\,| - |\,u\,|$ oraz zmienną r o długości $|\,p\,| - |\,u\,|$. W tym przypadku układ E jest równoważny

$$E' = E_0 \cup \{u = pr, q = rw, v = wy\}.$$

Zauważmy, że $|\,w\,| < |\,x\,|$ oraz $|\,r\,| < |\,p\,| < c|\,z\,|$. Stąd

$$S(E) - S(E') = \log_2|\,z\,| - \log_2|\,r\,| + \log_2|\,x\,| - \log_2|\,w\,|) \geqslant -\log_2 c$$

oraz

$$\frac{3}{-\log_2 c}(S(E) - S(E')) \geqslant 3.$$

Tak więc zastąpienie E przez E' nie spowodowało zmiany liczby zmiennych, spowodowało, że zmienna z przestała być podwójnie definiowana, ale jednocześnie być może zmienne u, q i v stały się podwójnie definiowane i spowodowało zmiejszenie ostatniego składnika wagi $W(E)$ przynajmniej o 3. Łącznie waga $W(E)$ zmniejszyła się przynajmniej o 1.

Przypadek 2.2.1.2.3: $|\,u\,| > |\,p\,|$. Analogicznie do poprzedniego przypadku.

Przypadek 2.2.2: x nie jest definiowana. Przypomnijmy, że $|\, u \,| < |\, x \,|$ i $|\, x \,| - |\, u \,| > c|\, z \,|$. Teraz też bierzemy nową zmienną w i przypisujemy jej długość $|\, w \,| = |\, x \,| - |\, u \,|$. Niech

$$E' = E_0 \cup \{x = uw, v = wy, R(x)\}.$$

Układ E' jest równoważny z E. Zmienna z została zastąpiona przez w. Zamiast podwójnie definiowanej zmiennej z mogła się pojawić podwójnie definiowana zmienna v. Mamy jednak

$$S(E) - S(E') = \log_2 |\, z \,| - \log_2 |\, w \,| \geqslant -\log_2 c.$$

Stąd $W(E)$ zmniejszyło się przynajmniej o 3.

38.2.3 Problem niesprzeczności z regularnymi więzami

Problem 38.2 niesprzeczności równań w słowach z więzami regularnymi jest naturalnym uogólnieniem problemu 38.1. Rozstrzygalność tego problemu została wykazana przez Schulza. Algorytm przedstawiony przez Schulza jest nieznacznym uogólnieniem algorytmu Makanina i ma niewiele większą, podobną złożoność. Rozumowania poprawiające oszacowania złożoności algorytmu Makanina często dają się zastosować w przypadku modyfikacji wykorzystanej przez Schulza. Zgodnie z najlepszym, znanym mi i jawnie sformułowym twierdzeniem będącym uogólnieniem wyniku Gutiérreza, problem 38.2 należy do klasy EXPSPACE.

Twierdzenie 38.6 *Problem niesprzeczności kwadratowego układu równań z regularnymi więzami należy do PSPACE.*

38.3 Dolne oszacowania złożoności

38.3.1 Problem niesprzeczności

Lemat 38.7 *Problem niesprzeczności równania w słowach jest NP-trudny.*

Dowód. Pokażemy, że problem 3SAT można zredukować do porblemu niesprzeczności. Przypuśćmy, że φ jest formułą, która może być daną dla 3SAT (φ jest koniunkcją trójczłonowych alternatyw zmiennych zdaniowych i ich negacji). Przypuśćmy, że w φ występują zmienne zdaniowe $x_1, \ldots, x_n$. Niech $y_1, \ldots, y_n$ odpowiadają negacjom zmiennych $x_1, \ldots, x_n$. Zmienne te będziemy też uważać za zmienne słowowe. Bierzemy też pomocnicze zmienne słowowe $z_1, \ldots, z_m$ odpowiadające alternatywom formuły φ. Za pomocą tych zmiennych zapiszemy pewne równanie w słowach. Weźmy równania postaci

$$x_i a = a x_1, \quad y_i a = a y_i \ \text{ oraz } \ z_j a = a z_j$$

dla $i = 1, \ldots, n$, $j = 1, \ldots, m$,

$$(a\wedge)^n = [x_i y_i \wedge]_{i=1}^n$$

oraz

$$\varphi^- = [a z_i \wedge]_{i=1}^m,$$

gdzie φ^- powstaje z φ przez zamianę negacji zmiennych x_1 na y_i i wykreślenie nawiasów oraz znaków alternatywy (w tych równaniach występują dwie stałe a i $\wedge$). $\square$

Lemat 38.8 *Problem niesprzeczności kwadratowych układów równań w słowach jest NP-trudny.*

Dowód. Przyjmijmy, że

$$\varphi = \bigwedge_{i=1}^{m} (x_{3i} \vee x_{3i+1} \vee x_{3i+2})$$

(x_j są więc literałami, uważamy je też za zmienne słowowe). Bierzemy też pomocnicze zmienne słowowe c_i, d_i, $i = 1, \ldots, m$, odpowiadające klauzulom (alternatywom) oraz zmienne p_i, q_i, $i = 1, \ldots, n$ odpowiadające zmiennym. Dodatkowo zakładamy, że dla każdego wystąpienia zmiennej mamy odpowiadające mu wystąpienie zmiennej zanegowanej (wymaga to rozważania wystąpień zmiennych, które w rzeczywistości nie występują w φ).

Niech a i b będą dwoma stałymi. Formule φ przyporządkowujemy układ złożony z następujących równań:

$$c_i = ad_i \quad \text{oraz} \quad c_i = x_{3i}x_{3i+1}x_{3i+2}$$

dla $i = 1, \ldots, m$, a także

$$p_iq_i = b \quad \text{oraz} \quad x_{i_1} \ldots x_{i_k} p_i a^k b x_{j_1} \ldots x_{j_k} q_i = a^k b a^k b,$$

dla $i = 1, \ldots, n$, gdzie $i_1, \ldots, i_k$ to numery wystąpień i-tej zmiennej, a $j_1, \ldots, j_k$ to numery wystąpień negacji tej zmiennej. □

Wniosek 38.9 *Problem niesprzeczności kwadratowego równania w słowach jest NP-trudny.* □

Twierdzenie 38.10 *Problem niesprzeczności kwadratowego układu równań liniowych z regularnymi więzami jest zupełny w klasie PSPACE.*