9 Twierdzenie Papadimitriou i NP-zupełność problemów 7.2 i 7.3

9.1 Twierdzenie Papadimitriou

Lemat 9.1 *Jeżeli A jest macierzą o wymiarach $m \times m$ o wyrazach całkowitych co do wartości bezwzględnej mniejszych lub równych a, to wyznacznik macierzy A ma wartość bezwzględną mniejszą lub równą $m! \cdot a^m \leqslant (ma)^m$.* □

Lemat 9.2 *Przypuśćmy, że wektory $\vec{v}_1, \ldots, \vec{v}_k \in R^m$ mają całkowite współrzędne o wartościach bezwzględnych nie przekraczających a. Niech $M = (ma)^m$. Istnieją nieujemne liczby rzeczywiste $\alpha_1, \ldots, \alpha_k$ nie wszystkie równe 0 takie, że*

$$\sum_{j=1}^{k} \alpha_j \vec{v}_j = \vec{0}$$

wtedy i tylko wtedy, gdy istnieją nieujemne liczby całkowite $\alpha_1, \ldots, \alpha_k \leqslant M$ nie wszystkie równe 0 takie, że

$$\sum_{j=1}^{k} \alpha_j \vec{v}_j = \vec{0}.$$

Dowód. Możemy dodatkowo założyć, że a jest dodatnią liczbą naturalną. Przypuśćmy, że

$$\sum_{j=1}^{k} \alpha_j \vec{v}_j = \vec{0}$$

dla pewnych nieujemnych liczb $\alpha_1, \ldots, \alpha_k$ nie wszystkich równych 0. Umówmy się, że α_k jest różna od zera. Podaną równość możemy podzielić stronami przez α_k. Możemy więc założyć, że podana równość zachodzi dla pewnych nieujemnych liczb $\alpha_1, \ldots, \alpha_k$ takich, że $\alpha_k \geqslant 1$. Rozważmy układ złożony z następujących nierówności:

$$\sum_{j=1}^{k} \alpha_j \vec{v}_j = \vec{0}$$

$$\alpha_i \geqslant 0 \quad \text{dla } i = 1, \ldots, k-1$$

oraz

$$\alpha_k \geqslant 1.$$

Jest to układ ze zmiennymi $\alpha_1, \ldots, \alpha_k$, kolumny macierzy głównej tego układu są liniowo niezależne, i układ ten ma rozwiązanie. Wobec tego ma rozwiązanie bazowe. Rozwiązanie bazowe tego układu spełnia pewien jednoznaczny układ równań zawarty w układzie

$$\sum_{j=1}^{k} \alpha_j \vec{v}_j = \vec{0}$$

$$\alpha_i = 0 \quad \text{dla } i = 1, \ldots, k-1$$

oraz

$$\alpha_k = 1.$$

Ten jednoznaczny układ musi zawierać równanie ostatnie, gdyż w przeciwnym razie jego rozwiązaniem jest wektor $\vec{0}$, który nie spełnia ostatniego równania ($\vec{0}$ nie jest rozwiązaniem bazowym). Wobec tego kolumna wyrazów wolnych tego układu zawiera zera i dokładnie jedną jedynkę. Z wzorów Cramera wynika, że istnieją macierze $A_1, \ldots, A_k$ oraz A takie, że rozwiązanie tego układu równań jest dane wzorami

$$\alpha_i = \frac{|\, A_i \,|}{|\, A \,|}.$$

Nietrudno zauważyć, że wyżej podany układ nierówności spełniają również liczby

$$\alpha_i' = \text{znak}(|\, A \,|) \cdot |\, A_i \,|.$$

Oszacujemy więc wartości bezwzględne wyznaczników macierzy A_i.

Macierze A_i zawierają kolumnę wyrazów wolnych układu. Kolumnę tę można usunąć wraz z wierszem odpowiadającym równaniu $\alpha_k = 1$ zmieniając najwyżej znak wyznacznika. Podobnie można usunąć wiersze odpowiadające równaniom $\alpha_j = 0$ dla $j < k$ wraz z odpowiednimi kolumnami. Po tych operacjach pozostaje macierz mająca nie więcej niż m kolumn i wierszy o wyrazach będących współrzędnymi wektorów $\vec{v}_j$. Wartość bezwzględna wyznacznika tej macierzy nie przekracza $m!a^m < M$. □

Lemat 9.3 *Przypuśćmy, że wektory $\vec{v}_1, \ldots, \vec{v}_k \in R^m$ mają całkowite współrzędne o wartościach bezwzględnych nie przekraczających a. Niech $M = (ma)^m$. Istnieje wektor $\vec{h}$ taki, że $\vec{h}\vec{v}_j > 0$ dla $j = 1, \ldots, k$ wtedy i tylko wtedy, gdy istnieje wektor $\vec{h}$ o całkowitych współrzędnych, których wartości bezwzględne nie przekraczają M, i taki, że $\vec{h}\vec{v}_j \geqslant 1$ dla $j = 1, \ldots, k$.*

Dowód. Przypuśćmy, że istnieje wektor $\vec{h} = (h_1, \ldots, h_m)$ taki, że $\vec{h}\vec{v}_j > 0$ dla $j = 1, \ldots, k$. Mnożąc ten wektor przez odpowiednią liczbę możemy spowodować, że będzie on spełniać dla $j = 1, \ldots, k$ nierównosci $\vec{h}\vec{v}_j \geqslant 1$. Dobierając odpowiednio znaki możemy spowodować, że będą spełnione także wszystkie nierówności postaci $\pm h_j \geqslant 0$. Weźmy rozwiązanie bazowe układu

$$\vec{h}\vec{v}_j \geqslant 1 \ \text{ dla } \ j = 1, \ldots, k$$

oraz

$$\pm h_j \geqslant 0 \ \text{ dla } \ j = 1, \ldots, m.$$

Dalej postępujemy tak, jak w poprzednim dowodzie, i znajdujemy rozwiązanie o współczynnikach całkowitych spełniające oszacowania podane w tezie lematu. □

9.2 Oszacowanie pewnego rozwiązania układu diofantycznego

Twierdzenie 9.4 (Papadimitriou) *Niech A będzie macierzą o wymiarach $n \times m$ o wyrazach całkowitych i niech $\vec{b} \in R^m$ będzie wektorem o współrzędnych całkowitych. Załóżmy, że elementy A i b mają wartości bezwzględne $\leqslant a$. Jeżeli układ m równań $A\vec{x} = \vec{b}$ z n niewiadomymi ma rozwiązanie złożone z liczb naturalnych, to ma także rozwiązanie złożone z liczb naturalnych nie przekraczających $(n+1)(ma)^{2m+1}$.*

Dowód. Niech $M = m!a^m$. Weźmy naturalne rozwiązanie układu $A\vec{x} = \vec{b}$ o najmniejszej sumie jego składowych. Jeżeli składowe rozwiązania $\vec{x}$ nie przekraczają M, to zachodzi teza twierdzenia. W przeciwnym razie możemy założyć, że $x_j \geqslant M$ dla $j = 1, \ldots, k$. Będziemy rozważać k pierwszych kolumn macierzy A, powiedzmy, że kolumnami A są wektory $\vec{v}_1, \ldots, \vec{v}_n \in R^m$.

Przypadek 1: rzypuśćmy, że istnieją liczby naturalne $\alpha_1, \ldots, \alpha_k$ nie wszystkie równe 0 i nie przekraczające M takie, że $\sum_{j=1}^{k} \alpha_j \vec{v}_j = 0$. Wtedy wektor $\vec{x}' = (x_1 - \alpha_1, \ldots, x_k - \alpha_k, x_{k+1}, \ldots, x_n)$ jest rozwiązaniem układu $A\vec{x} = \vec{b}$ i przeczy to minimalności (w podanym sensie) rozwiązania $\vec{x}$.

Przypadek 2: przeciwnym razie, na podstawie wniosku 8.7 oraz lematów 9.2 i 9.3 stwierdzamy, że istnieje wektor $\vec{h} \in R^m$ o całkowitych współrzednych, których wartości bezwzględne są $\leqslant M$, spełniający nierówności postaci $\vec{h}\vec{v}_j \geqslant 1$ dla $j = 1, \ldots, k$. Pomnóżmy równość $A\vec{x} = \vec{b}$ przez $\vec{h}$. W ten sposób otrzymujemy, że

$$\vec{h}\vec{b} = \vec{h}A\vec{x} = (\vec{h}\vec{v}_1, \ldots, \vec{h}\vec{v}_n)\vec{x} = \sum_{j=1}^{k} \vec{h}\vec{v}_j x_j + \sum_{j=k+1}^{n} \vec{h}\vec{v}_j x_j.$$

Wobec tego

$$\sum_{j=1}^{k} x_j \leqslant \sum_{j=1}^{k} \vec{h}\vec{v}_j x_j = \vec{h}\vec{b} - \sum_{j=k+1}^{n} \vec{h}\vec{v}_j x_j \leqslant maM + nmaM^2 \leqslant (n+1)(ma)^{2m+1}.$$

□

9.3 Wnioski z twierdzenia Papadimitriou

Wniosek 9.5 *Problem niesprzeczności układu liniowych równań diofantycznych (problem 7.3) należy do klasy NP.*

Dowód. O tym, że problem niesprzeczności układu liniowych równań diofantycznych należy do klasy NP świadczy następujący algorytm:

Algorytm 9.1 niedeterministyczny algorytm rozwiązujący problem 7.3
Dane: układ równań $A\vec{x} = \vec{b}$.

1) ustalamy liczbę m równań i liczbę n zmiennych danego układu,

2) obliczamy liczbę a, która jest największą liczbą spośród wartości bezwzględnych elementów macierzy A i wyrazów wektora $\vec{b}$,

3) obliczamy liczbę $B = (n+1)(ma)^{2m+1}$,

4) niedeterministycznie zgadujemy wektor $\vec{x} = (x_1, \ldots, x_n)$ o współrzędnych $x_i \leqslant B$ dla $i = 1, \ldots, n$,

5) obliczamy wektor $A\vec{x}$ i porównujemy go z wektorem $\vec{b}$; jeżeli są równe, to przekazujemy, że dany układ ma rozwiązanie, a w przeciwnym razie – że jest sprzeczny.

Nietrudno zauważyć, że liczbę operacji wykonywanych przez podany algorytm szacuje pewien wielomian zależący od n i m. Największymi liczbami, które obliczamy podczas wykonywania tego algorytmu są współrzędne wektora $A\vec{x}$. Co do wartości bezwzględnej są to liczby $\leqslant n \cdot a \cdot B$. Rozmiar tych liczb jest $\leqslant 2 \cdot n \cdot \langle a \rangle \cdot (2m+1)(\langle a \rangle + m)$, a więc daje się oszacować za pomocą wielomianu zależącego od n, m i rozmiaru $\langle a \rangle$ liczby a. Ponieważ liczby n, m i $\langle a \rangle$ są mniejsze od rozmiaru danych, więc podany algorytm jest wielomianowy. $\Box$

Wniosek 9.6 *Problem niesprzeczności układu m liniowych równań diofantycznych (problem 7.2) należy do klasy NP.* $\Box$

Wniosek 9.7 *Istnieje pseudowielomianowy algorytm rozwiązujący problem 7.2 niesprzeczności układu m liniowych równań diofantycznych.*

Dowód. Rozważmy następujący algorytm posługujący się dwoma listami S i S_p wektorów o m współrzędnych.

Algorytm 9.2 rozwiązujący problem 7.2.
Dane: układ $A\vec{x} = \vec{b}$ złożony z m równań liniowych.

1) ustalamy liczbę n zmiennych danego układu;

2) znajdujemy liczbę a, największą co do wartości bezwzględnej spośród elementów macierzy A i wyrazów wektora $\vec{b}$;

3) obliczamy liczbę $B = (n+1)(ma)^{2m+1}$;

4) zmiennej S przypisujemy listę złożoną z wektora zerowego o m współrzędnych, zmiennej (pomocniczej) S_p – listę pustą, znajdujemy kolumny $\vec{v}_1, \ldots, \vec{v}_n \in R^m$ macierzy A;

5) dla wszystkich i od 1 do n
{lista S zawiera wszystkie kombinacje wektorów $\vec{v}_1, \ldots, \vec{v}_{i-1}$ o naturalnych współczynnikach $\leqslant B$ i jest listą bez powtórzeń}

   (a) dla wszystkich j od 0 do B
   i dla każdego elementu s listy S

      obliczamy $s_1 = s + j \cdot \vec{v}_i$;

sprawdzamy, czy s_1 występuje na liście S_p; jeżeli nie występuje, to dopisujemy s_1 do listy S_p;

(b) listę S_p zapamiętuje w zmiennej S, a następnie powodujemy, że S_p staje się pusta;

6) sprawdzamy, czy $\vec{b}$ znajduje się na liście S; Jeżeli tak, to stwierdzamy, że dany układ ma rozwiązanie, a w przeciwnym razie – że jest sprzeczny.

Poprawność przedstawionego algorytmu jest konsekwencją tego, że informacja podana w komentarzu do punktu 5) jest niezmiennikiem pętli z tego punktu. Jeżeli jest to niezmiennik, to po zakończeniu wykonywania pętli z punktu 5) wartością zmiennej S jest lista zawierająca wszystkie wektory postaci $\sum_{i=1}^{n} x_i \vec{v}_i$, gdzie $x_i \leqslant B$ dla $i = 1, \ldots, n$. Jeżeli $(\alpha_1, \ldots, \alpha_n)$ jest rozwiązaniem danego równania, to oczywiście $\sum_{i=1}^{n} \alpha_i \vec{v}_i = \vec{b}$.

Przypuśćmy, że dane równanie ma rozwiązanie w liczbach naturalnych. Z twierdzenia Papadimitriou 9.4 wynika, że ma także rozwiązanie naturalne $(\alpha_1, \ldots, \alpha_n)$ takie, że $\alpha_i \leqslant B$ dla $i = 1, \ldots, n$. Dla tego rozwiązania wektor $\sum_{i=1}^{n} \alpha_i \vec{v}_i$ znajdzie się na liście S. Ponieważ ten wektor jest równy $\vec{b}$, więc w ostatniej fazie algorytm 9.2 znajdzie na liście S wektor $\vec{b}$ i stwierdzi, że dane równanie ma rozwiązanie. Jeżeli natomiast dane równanie nie ma naturalnego rozwiązania, to dla dowolnych liczb naturalnych x_i suma $\sum_{i=1}^{n} x_i \vec{v}_i$ nie jest równa $\vec{b}$ i wektor $\vec{b}$ nie występuje na liście S. Wobec tego, algorytm 9.2 nie znajdzie tego wektora na liście S i stwierdzi, że dane równanie nie ma rozwiązania diofantycznego.

Aby ocenić złożoność algorytmu 9.2 musimy oszacować długość list ze zmiennych S i S_p. Listy te zawsze zawierają wektory postaci $\sum_{i=1}^{k} x_i \vec{v}_i$ dla ustalonego $k \leqslant n$ i naturalnych współczynników $x_i \leqslant B$. Współrzędne takich wektorów są liczbami całkowitymi, mają bezwzględne wartości nie przekraczające $k \cdot a \cdot B \leqslant n \cdot a \cdot B$ i w konsekwencji mogą przyjmować $2 \cdot n \cdot a \cdot B + 1$ różnych wartości. Wektorów o m takich współrzędnych jest $(n \cdot a \cdot B + 1)^m$. W pętli z punktu 5) algorytm najwyżej

$$n \cdot B \cdot (2 \cdot n \cdot a \cdot B + 1)^m \cdot (2 \cdot n \cdot a \cdot B + 1)^m$$

razy wykonuje pewną stałą (zależną od m) liczbę czynności. Pętla z punktu 6) jest wykonywana najwyżej $(n \cdot a \cdot B + 1)^m$ razy. Tak więc złożoność algorytmu 9.2 nie przekracza

$$c \cdot n \cdot (n+1) \cdot (ma)^{2m+1} \cdot (2 \cdot n \cdot a \cdot (n+1) \cdot (ma)^{2m+1} + 1)^{2 \cdot m}$$

i wyraża się wielomianem zależącym od n i a, którego stopień i współczynniki wyrażają się w pewien sposób przez stałą m.

Nietrudno zauważyć, że liczby pojawiające się podczas realizacji algorytmu 9.2 mają wartości bezwzględne $\leqslant n \cdot a \cdot B$, a ich rozmiar można oszacować za pomocą wielomianu zależącego od n i $\langle a \rangle$ (a także od stałej m). Tak więc algorytm 9.2 korzysta z wielomianowej pamięci.

Ostatecznie, algorytm 9.2 rozwiązuje problem 7.2 i jest pseudowielomianowy. □