12 Kraty. Równania liniowe z ustaloną liczbą zmiennych.

12.1 Kraty

Przypuśćmy, że mamy dane wektory $\vec{a}_1, \ldots, \vec{a}_n \in Q^m$. Niech

$$L(\vec{a}_1, \ldots, \vec{a}_n) = \{\sum_{i=1}^{n} c_i \vec{a}_i \in R^m : c_i \in Z \text{ dla } i = 1, \ldots, n\}.$$

Zbiór $L(\vec{a}_1, \ldots, \vec{a}_n)$ jest podgrupą grupy addytywnej R^m (a więc jest zamknięty ze względu na dodawanie wektorów i zmianę znaku (mnożenie przez -1)). Zbiór ten jest także modułem nad pierścieniem liczb całkowitych Z (a więc jest zamknięty ze względu na dodawanie wektorów i mnożenie przez liczby całkowite). Czasem zbiory tej postaci są nazywane kratami (lattice). Zbiory te – jako grupy – są przemienne i skończenie generowalne.

Lemat 12.1 *Dla dowolnej kraty $L = L(\vec{a}_1, \ldots, \vec{a}_n)$ generowanej przez wektory o współrzędnych wymiernych istnieje liczba $\varepsilon > 0$ taka, że niezerowe wektory o długości mniejszej niż ε nie należą do kraty L.*

Dowód. Ponieważ wszystkie współrzędne wektorów generujących kratę L są wymierne, możemy sprowadzić je do wspólnego mianownika q. Nietrudno zauważyć, że wszystkie współrzędne każdego wektora z kraty L dają się przedstawić w postaci ilorazu pewnej liczby całkowitej i liczby q. Niech $\varepsilon = \frac{1}{q}$. Każdy niezerowy wektor należący do L ma przynajmniej jedną współrzędną co do wartości bezwzględnej większą od ε, w konsekwencji jego długość jest większa od ε. □

Lemat 12.2 *Jeżeli L jest kratą, to każdy ograniczony podzbiór L jest skończony.*

Dowód. Przypuśćmy, że pewien ograniczony (a więc zawarty w pewnej kuli domkniętej) podzbiór L jest nieskończony. Wtedy istnieje różnowartościowy i ograniczony ciąg elementów L. Ponieważ jest to ciąg ograniczony, więc zawiera podciąg zbieżny. Korzystając np. z warunku Cauchy'ego, w tym ciągu znajdujemy dwa (różne) wyrazy odległe o mniej niż liczba ε z lematu 12.1. Ponieważ zbiór L jest zamknięty ze względu na odejmowanie, więc przeczy to lematowi 12.1. □

Twierdzenie 12.3 *Jeżeli L jest addytywną grupą zawartą w przestrzeni R^m mającą własność podaną w lemacie 12.2, to istnieją liniowo niezależne wektory $\vec{b}_1, \ldots, \vec{b}_k \in R^m$ takie, że $L = L(\vec{b}_1, \ldots, \vec{b}_k)$, i liczba k tych wektorów jest liczbą wektorów w maksymalnym podzbiorze kraty L złożonym z wektorów liniowo niezależnych.*

Dowód. Twierdzenie będziemy dowodzić przez indukcję ze względu na liczbę elementów maksymalnego, liniowo niezależnego (w sensie R^m) zbioru wektorów, zawartego w zbiorze L.

Przypuśćmy, że wektory $\vec{v}_1, \ldots, \vec{v}_k$ tworzą maksymalny, liniowo niezależny (w sensie R^m) podzbiór L. Załóżmy najpierw, że $k > 1$ i rozważmy podprzestrzeń liniową P przestrzeni

R^m generowaną przez wektory $\vec{v}_1, \ldots, \vec{v}_{k-1}$. Przekrój $L \cap P$ jest podgrupą addytywnej grupy R^m i nie zawiera więcej niż $k-1$ liniowo niezależnych wektorów. Z założenia indukcyjnego otrzymujemy, że

$$L \cap P = L(\vec{b}_1, \ldots, \vec{b}_{k-1})$$

dla pewnych liniowo niezależnych wektorów $\vec{b}_1, \ldots, \vec{b}_{k-1}$. Oczywiście, $\vec{v}_1, \ldots, \vec{v}_{k-1} \in L \cap P$ oraz $\vec{v}_k \notin P$.

Rozważmy zbiór

$$S = \{\sum_{i=1}^{k} a_i \vec{v}_i \in L : 0 \leqslant a_i < 1 \text{ dla } i = 1, \ldots, k-1 \wedge 0 \leqslant a_k \leqslant 1\}.$$

Oczywiście, w S jest wektor, który ma stosowne przedstawienie z liczbą $a_k > 0$. Takim wektorem jest np. $\vec{v}_k$. Zbiór S jest zbiorem ograniczonym (współrzędne wektorów $\vec{v}_i$ można ograniczyć (jest ich skończenie wiele), współczynniki a_i są ograniczone). Jest więc zbiorem skończonym. Zauważmy, że współczynniki a_i w przedstawieniu elementów zbioru S są wyznaczone jednoznacznie przez te elementy. Weźmy więc

$$\vec{b}_k = \sum_{i=1}^{k} \beta_i \vec{v}_i \in S,$$

dla którego współczynnik β_k jest dodatni i najmniejszy z możliwych. Udowodnimy, że $L = L(\vec{b}_1, \ldots, \vec{b}_k)$, oraz że wektory $\vec{b}_1, \ldots, \vec{b}_k$ są liniowo niezależne.

Zawieranie $L(\vec{b}_1, \ldots, \vec{b}_k) \subseteq L$ jest oczywiste. Aby dowieść zawieranie przeciwne, weźmy $\vec{x} \in L$ i najpierw dołączmy go do wektorów $\vec{v}_1, \ldots, \vec{v}_k$. Otrzymany w ten sposób układ jest liniowo zależny (wynika to z maksymalności układu $\vec{v}_1, \ldots, \vec{v}_k$). Wobec tego

$$\vec{x} = \sum_{i=1}^{k} \alpha_i \vec{v}_i$$

dla pewnych α_i. Niech

$$\vec{y} = \vec{x} - \left\lfloor \frac{\alpha_k}{\beta_k} \right\rfloor \cdot \vec{b}_k = \sum_{i=1}^{k} (\alpha_i - \left\lfloor \frac{\alpha_k}{\beta_k} \right\rfloor \beta_i) \vec{v}_i.$$

Przyjmując, że

$$\gamma_i = \alpha_i - \left\lfloor \frac{\alpha_k}{\beta_k} \right\rfloor \beta_i$$

otrzymujemy, że

$$\vec{y} = \sum_{i=1}^{k} \gamma_i \vec{v}_i.$$

Zauważmy, że $\vec{y} \in L$ i weźmy

$$\vec{z} = \vec{y} - \sum_{i=1}^{k-1} \lfloor \gamma_i \rfloor \vec{v}_i = \sum_{i=1}^{k-1} (\gamma_i - \lfloor \gamma_i \rfloor) \vec{v}_i + \gamma_k \vec{v}_k.$$

Nietrudno sprawdzić, że $\vec{y} \in S$ oraz

$$\gamma_k = \alpha_k - \left\lfloor \frac{\alpha_k}{\beta_k} \right\rfloor \cdot \beta_k < \beta_k.$$

Gdyby liczba γ_k była większa od 0, to z definicji $\vec{b}_k$ otrzymalibyśmy sprzeczność. Wobec tego $\gamma_k = 0$. Rozważmy jeszcze raz wektor

$$\vec{y} = \vec{x} - \left\lfloor \frac{\alpha_k}{\beta_k} \right\rfloor \cdot \vec{b}_k = \sum_{i=1}^{k} \gamma_i \vec{v}_i = \sum_{i=1}^{k-1} \gamma_i \vec{v}_i.$$

Należy on do $L \cap P = L(\vec{b}_1, \ldots, \vec{b}_{k-1})$. Wobec tego

$$\vec{x} = \vec{y} + \left\lfloor \frac{\alpha_k}{\beta_k} \right\rfloor \cdot \vec{b}_k \in L(\vec{b}_1, \ldots, \vec{b}_k).$$

Wektory $\vec{b}_1, \ldots, \vec{b}_{k-1}$ są liniowo niezależne. Gdyby wektory $\vec{b}_1, \ldots, \vec{b}_k$ były liniowo zależne, to

$$\vec{b}_k = \sum_{i=1}^{k-1} \delta_i \vec{b}_i$$

dla pewnych liczb δ_i. Wtedy

$$\beta_k \vec{v}_k = \vec{b}_k - \sum_{i=1}^{k-1} \beta_i \vec{v}_i = \sum_{i=1}^{k-1} \delta_i \vec{b}_i - \sum_{i=1}^{k-1} \beta_i \vec{v}_i \in P.$$

Przeczy to liniowej niezależności wektorów $\vec{v}_1, \ldots, \vec{v}_k$.

Pozostał do rozważenia przypadek $k = 1$ (pierwszy krok indukcyjny). Weźmy dowolny niezerowy wektor $\vec{v}_1 \in L$. W tym przypadku każdy inny wektor należący do L jest postaci $\alpha \vec{v}_1$. Weźmy najmniejszą dodatnią liczbę β taką, że $\beta \vec{v}_1 \in L$ (taka liczba istnieje na podstawie lematu 12.2). Jest oczywiste, że $L(\beta \vec{v}_1) \subseteq L$. Jeżeli $\vec{x} \in L$, to $\vec{x} = \alpha \vec{v}_1$. Weźmy

$$\vec{y} = \vec{x} - \left\lfloor \frac{\alpha}{\beta} \right\rfloor \beta \vec{v}_1 = (\alpha - \left\lfloor \frac{\alpha}{\beta} \right\rfloor \beta) \vec{v}_1.$$

Oczywiście $\vec{y} \in L$ oraz

$$0 \leqslant \alpha - \left\lfloor \frac{\alpha}{\beta} \right\rfloor \beta < \beta,$$

a gdyby środkowa liczba była większa od 0, to otrzymalibyśmy sprzeczność z definicją β. Wobec tego

$$\vec{x} = \alpha \vec{v}_1 = (\left\lfloor \frac{\alpha}{\beta} \right\rfloor \beta) \vec{v}_1 = \left\lfloor \frac{\alpha}{\beta} \right\rfloor (\beta \vec{v}_1) \in L(\beta \vec{v}_1).$$

□

12.2 Kraty dualne

Będziemy teraz rozważać kratę $L(\vec{a}_1, \ldots, \vec{a}_n)$ generowaną przez bazę $\vec{a}_1, \ldots, \vec{a}_n$ przestrzeni R^n. Dla takiej kraty L, kratą dualną do L nazywamy zbiór

$$L^* = \{\vec{x} \in R^n : \forall \vec{y} \in L \; \vec{x}^T \vec{y} \in Z\}.$$

Najpierw pokażemy, że zbiór ten rzeczywiście jest kratą.

Lemat 12.4 *Jeżeli wektory $\vec{a}_1, \ldots, \vec{a}_n$ są bazą przestrzeni R^n, a wektory $\vec{b}_1, \ldots, \vec{b}_n$ spełniają równości*

$$\vec{b}_i^T \vec{a}_j = \begin{cases} 1 & \text{jeżeli } i = j \\ 0 & \text{w przeciwnym razie,} \end{cases}$$

to $(L(\vec{a}_1, \ldots, \vec{a}_n))^* = L(\vec{b}_1, \ldots, \vec{b}_n)$.

Dowód. Przypuśćmy, że $\vec{x} \in L(\vec{b}_1, \ldots, \vec{b}_n)$ i weźmy dowolny $\vec{y} \in L(\vec{a}_1, \ldots, \vec{a}_n)$. Niech

$$\vec{x} = \sum_{i=1}^{n} x_i \vec{b}_i \quad \text{oraz} \quad \vec{y} = \sum_{i=1}^{n} y_i \vec{a}_i$$

dla pewnych całkowitych współczynników x_i oraz y_i. Wtedy

$$\vec{x}^T \vec{y} = (\sum_{i=1}^{n} x_i \vec{b}_i)^T (\sum_{i=1}^{n} y_i \vec{a}_i) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i y_j \vec{b}_i^T \vec{a}_j = \sum_{i=1}^{n} x_i y_i \in Z.$$

Wobec tego $\vec{x} \in (L(\vec{a}_1, \ldots, \vec{a}_n))^*$.

Załóżmy teraz, że $\vec{x} \in (L(\vec{a}_1, \ldots, \vec{a}_n))^*$ i weźmy wektor

$$\vec{y} = \sum_{i=1}^{n} (\vec{x}^T \vec{a}_i) \vec{b}_i.$$

Ponieważ $\vec{x}$ należy do wskazanej kraty dualnej, więc współczynniki kombinacji liniowej definiującej $\vec{y}$ są liczbami calkowitymi i w konsekwencji $\vec{y} \in L(\vec{b}_1, \ldots, \vec{b}_n)$. Zauważmy, że

$$\vec{y}^T \vec{a}_j = (\sum_{i=1}^{n} (\vec{x}^T \vec{a}_i) \vec{b}_i)^T \vec{a}_j = \sum_{i=1}^{n} (\vec{x}^T \vec{a}_i) \vec{b}_i^T \vec{a}_j = \vec{x}^T \vec{a}_j.$$

Oznacza to, że wektor $\vec{x} - \vec{y}$ spełnia układ równań liniowych

$$(\vec{x} - \vec{y})^T \vec{a}_j = \vec{0}.$$

Jest to układ jednorodny i wierszami macierzy głównej A tego układu są wektory $\vec{a}_j$. Ponieważ wektory $\vec{a}_j$ są liniowo niezależne, więc wyznacznik macierzy A jest różny od 0 i rozważamy układ ma dokładnie jedno rozwiązanie. Ponieważ jest to układ jednorodny, więc jego rozwiązaniem jest wektor zerowy, czyli $\vec{x} - \vec{y} = \vec{0}$. Stąd wynika, że $\vec{x} = \vec{y} \in L(\vec{b}_1, \ldots, \vec{b}_n)$. $\square$

Wniosek 12.5 *Jeżeli wektory* $\vec{a}_1, \ldots, \vec{a}_n$ *są bazą przestrzeni* R^n *i* $L = L(\vec{a}_1, \ldots, \vec{a}_n)$*, to zbiór* L^* *(nazywany kratą dualną) jest kratą.*

Dowód. Wystarczy pokazać, że dla dowolnej bazy $\vec{a}_1, \ldots, \vec{a}_n$ istnieją wektory $\vec{b}_i$ spełniające równości podane w tezie lematu 12.4. Utwórzmy macierz A, której kolumnami są wektory $\vec{a}_i$ dla $i = 1, \ldots, n$. Ponieważ wektory te są liniowo niezależne, więc wyznacznik macierzy A jest różny od 0. Macierz o wyznaczniku różnym od 0 ma macierz odwrotną. Niech $B = A^{-1}$. Nietrudno zauważyć, że wiersze macierzy B mają żądane własności. □

Wniosek 12.6 *Jeżeli wektory* $\vec{a}_1, \ldots, \vec{a}_n$ *są bazą przestrzeni* R^n *i* $L = L(\vec{a}_1, \ldots, \vec{a}_n)$*, to* $(L^*)^* = L$*.*

Dowód. Dla wektorów $\vec{a}_1, \ldots, \vec{a}_n$ weźmy wektory $\vec{b}_1, \ldots, \vec{b}_n$ spełniające własności podane w tezie lematu 12.4 (korzystając z poprzedniego wniosku). Zauważmy, że $\vec{b}_i^T \vec{a}_j = \vec{a}_j^T \vec{b}_i$. Wobec tego z lematu 12.4 wynika nie tylko równość

$$L^* = (L(\vec{a}_1, \ldots, \vec{a}_n))^* = L(\vec{b}_1, \ldots, \vec{b}_n),$$

ale także

$$(L(\vec{b}_1, \ldots, \vec{b}_n))^* = L(\vec{a}_1, \ldots, \vec{a}_n) = L.$$

Łącząc te dwie równości otrzymujemy tezę. □

12.3 Zastosowanie krat dualnych

Niech $\mathcal{A}$ będzie układem n równań liniowych

$$\begin{gathered}
a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,m}x_m = c_1, \\
a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,m}x_m = c_2, \\
\vdots \\
a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,m}x_m = c_n
\end{gathered}$$

z m niewiadomymi i z całkowitymi (lub wymiernymi) współczynnikami. Niech $\vec{a}_i = (a_{1,i}, a_{2,i}, \ldots, a_{n,i})$ (tak więc $\vec{a}_i$ są kolumnami macierzy głównej układu $\mathcal{A}$) oraz niech $\vec{c} = (c_1, \ldots, c_n)$. Będziemy zakładać, że wiersze macierzy głównej układu $\mathcal{A}$ (wektory postaci $(a_{i,1}, a_{i,2}, \ldots, a_{i,m})$) są liniowo niezależne. Implikuje to, że $n \leqslant m$ oraz, że wektory $\vec{a}_1, \ldots, \vec{a}_m$ generują przestrzeń R^n (i można z nich wybrać układ n wektorów liniowo niezależnych). Niech

$$L = L(\vec{a}_1, \ldots, \vec{a}_m)$$

będzie kratą generowaną przez wspomniane wektory. Zauważmy, że z twierdzenia 12.3 i lematu 12.1 wynika, że krata L jest generowana przez pewną bazę przestrzeni R^n i wobec tego w takiej sytuacji możemy rozważać kratę dualną L^* (patrz też lemat 12.4). Przyjmijmy, że

$$L^* = L(\vec{b}_1, \ldots, \vec{b}_n).$$

Wprowadzone oznaczenia wykorzystamy w następującym lemacie.

Lemat 12.7 *Układ $\mathcal{A}$ ma całkowite rozwiązanie wtedy i tylko wtedy, gdy $\vec{b}_i^T\vec{c} \in Z$ dla $i = 1, \dots, n$.*

Dowód. Układowi $\mathcal{A}$ można nadać postać wektorową

$$\sum_{i=1}^{m} x_i\vec{a}_i = \vec{c}.$$

Stąd oczywiście wynika, że układ $\mathcal{A}$ ma rozwiązanie całkowite wtedy i tylko wtedy, gdy $\vec{c} \in L = L(\vec{a}_1, \dots, \vec{a}_m)$. Wystarczy więc dowieść, że warunek podany w tezie lematu jest równoważny warunkowi $\vec{c} \in L$.

Jeżeli $\vec{c} \in L$, to $\vec{b}_i^T\vec{c} \in Z$ dla $i = 1, \dots, n$, ponieważ $\vec{b}_i \in L^*$ i wobec tego spełniają warunek podany w definicji L^*.

Jeżeli natomiast dla $i = 1, \dots, n$ zachodzi $\vec{b}_i^T\vec{c} = \vec{c}^T\vec{b}_i \in Z$, to także $\vec{c}^T\vec{y} \in Z$ dla dowolnej kombinacji $\vec{y}$ wektorów $\vec{b}_i$ o współczynnikach całkowitych, a więc dla dowolnego wektora $\vec{y} \in L^*$. To oznacza, że $\vec{c} \in (L^*)^* = L$. □

Powyższy lemat sugeruje następujący algorytm sprawdzania, czy dany układ $\mathcal{A}$ równań liniowych ma rozwiązanie całkowite: tworzymy kratę $L = L(\vec{a}_1, \dots, \vec{a}_m)$, znajdujemy wektory $\vec{b}_1, \dots, \vec{b}_k$ generujące kratę dualną i sprawdzamy warunek podany w tezie lematu.

12.4 Wyrocznie i maszyny z wyroczniami

Niech L będzie taką kratą w R^n, dla której istnieje krata dualna. Mówimy, że krata L jest opisana przez wyrocznię, jeżeli istnieje maszyna Turinga (algorytm), która dla danego wektora $\vec{x} \in R^n$ zwraca informację, czy $\vec{x} \in L$, a w przypadku, gdy nie jest to prawdą, zwraca także wektor $\vec{y} \in L^*$ taki, że $\vec{y}^T\vec{x} \notin Z$. Maszynę Turinga (algorytm) o podanych własnościach będziemy czasem nazywać wyrocznią.

Mówimy, że krata L złożona z wektorów o współrzędnych wymiernych jest dobrze opisana przez wyrocznię, jeżeli

1) krata L jest opisana przez wyrocznię,

2) mamy daną liczbę n taką, że $L \subseteq R^n$,

3) mamy daną liczbę T taką, że każda współrzędna każdego wektora należącego do $L \cup L^*$ daje się przedstawić w postaci $\frac{p}{q}$, gdzie p jest liczbą całkowitą, a q jest dodatnią liczbą naturalną $\leqslant T$,

4) rozmiar wyników zwracanych przez wyrocznię z punktu 1) uruchomioną ze słowem s nie przekracza wartości $w(|\, s\,|)$ pewnego wielomianu w dla rozmiaru słowa s.

Lemat 12.8 *Jeżeli wektory $\vec{a}_1, \dots, \vec{a}_m$ o wymiernych współrzędnych zawierają bazę przestrzeni R^n i $L = L(\vec{a}_1, \dots, \vec{a}_m)$, to krata L^* jest dobrze opisana przez wyrocznię. Wyrocznia ta po uruchomieniu z daną s działa w czasie $w(\langle s\rangle, \langle\vec{a}_1\rangle + \ldots + \langle\vec{a}_m\rangle)$ dla pewnego wielomianu w i zwraca słowo rozmiaru $\leqslant \max\{\langle\vec{a}_i\rangle : i = 1, \dots, m\}$. Ponadto, mając dane wektory $\vec{a}_1, \dots, \vec{a}_m$ można (posługując się maszyną Turinga) w czasie wielomianowym obliczyć liczby n i T wymagane w definicji kraty dobrze opisanej.*

Dowód. Szukana wyrocznia działa zgodnie z następującym algorytmem: dany wektor $\vec{x}$ mnoży kolejno przez wektory $\vec{a}_1, \ldots, \vec{a}_m$ i sprawdza, czy $\vec{x}^T\vec{a}_i \in Z$. Jeżeli wszystkie wyliczone iloczyny skalarne należą do Z, to zwraca informację, że $\vec{x} \in L^*$. W przeciwnym razie zwraca informację, że $\vec{x} \notin L^*$ i wektor $\vec{a}_i$ taki, że $\vec{x}^T\vec{a}_i \notin Z$.

Kilka uwag poświęcimy jeszcze obliczaniu liczby T. Łatwo ustalić mianowniki wszystkich współrzędnych wektorów $\vec{a}_1, \ldots, \vec{a}_m$, a następnie wspólny mianownik q tych liczb (wystarczy pomnożyć mianowniki). Nietrudno zauważyć, że współrzędne wektorów należących do L można przedstawić w postaci ilorazu odpowiedniej liczby całkowitej i liczby q. Aby oszacować mianowniki współczynników wektorów z L^* możemy wzorować się na dowodzie istnienia bazy w L^*. Możemy wybrać bazę złożoną z wektorów $\vec{a}_1, \ldots, \vec{a}_m$, utworzyć z wybranych wektorów macierz A i przyjrzeć się macierzy B odwrotnej do A. Wiersze macierzy B generują L^*, wystarczy więc oszacować mianowniki elementów B. Zgodnie z wzorami Cramera, elementy macierzy B są ilorazami wyznaczników. W liczniku znajduje się wyznacznik macierzy wypełnionej współrzędnymi wektorów $\vec{a}_1, \ldots, \vec{a}_m$, zerami i jedynkami a w mianowniku – wyznacznik macierzy A. Oba wyznaczniki po pomnożeniu przez q^n stają się liczbami całkowitymi, gdyż są wyznacznikami macierzy o elementach postaci $\frac{p}{q}$, gdzie $p \in Z$. Wobec tego, krata L^* jest generowana przez wektory o współrzędnych postaci $\frac{p}{q^n|\,A\,|}$ dla całkowitych p. W tej sytuacji liczbę T można zdefiniować jako $\max\{q, q^n|\,A\,|\}$. $\square$

Będziemy konstruować maszynę Turinga (algorytm), która dla kraty dobrze opisanej przez wyrocznię pozwala w czasie wielomianym obliczyć bazę generującą tę kratę. Będzie to maszyna Turinga z wyrocznią. Taką maszynę możemy wyobrażać sobie jako zwykłą maszynę Turinga z wyróżnioną taśmą i wyróżnionym stanem. Maszyna z wyrocznią wykonuje zwykłe ruchy lub zadaje pytania wyroczni. Zadawanie pytania jest traktowane jako specjalny, pojedyńczy ruch maszyny. Ruch ten jest wykonywany, jeżeli maszyna znajduje się w wyróżnionym stanie. Ten ruch polega na zmianie napisu na wyróżnionej taśmie (mimo tego, jest liczony jako pojedyńczy ruch) i przejściu do odpowiedniego stanu. Innymi słowami, algorytm z wyrocznią możemy interpretować jako algorytm z wyróżnioną procedurą, (daną, ale o nieznanej treści). Złożoność czasową takiego algorytmu definiujemy przyjmując, że wykonanie wyróżnionej procedury zajmuje jednostkę czasu. Będziemy korzystać z tego, że jeżeli w wielomianowym algorytmie z wyrocznią zapytania do wyroczni zastąpimy wykonaniem odpowiednich, wielomianowych obliczeń, to otrzymamy algorytm wielomianowy. Własność ta wymaga jeszcze pewnego uściślenia (zostanie to zrobione w interesującym nas przypadku), a jej dowód zostanie pominięty.

12.5 Wielomianowy algorytm obliczający bazę kraty

Twierdzenie 12.9 *Istnieje wielomianowy algorytm z wyrocznią, który dla kraty L dobrze opisanej przez wyrocznię znajduje bazę generującą kratę L.*

Dowód. Niech L będzie kratą dobrze opisaną przez wyrocznię. Znamy więc liczbę n taką, że $L \subseteq R^n$ i liczbę T pozwalającą na szacowanie mianowników elementów $L \cup L^*$ (patrz str. 90). Złożoność czasowa algorytmu, który zdefiniujemy, będzie $\leqslant W(n + \langle T\rangle)$ dla pewnego wielomianu W (złożoność możemy rozumieć jako liczbę ruchów maszyny Turinga z wyrocznią).

Algorytm będzie korzystać ze zmiennej C pamiętającej zbiór liniowo niezależnych wektorów należących do L^*. Zbiór ten będziemy stopniowo rozszerzać tak, aby w końcu był bazą przestrzeni R^n. Przyjmijmy, że $C = \{\vec{c}_1, \ldots, \vec{c}_k\}$. Algorytm będzie iterować pewien zespoł czynności. Będziemy przyjmować, że ma postać **while true do ...** i czynności wykonywane w pętli powodują w odpowiednim momencie przerwanie działania algorytmu. Taki algorytm będzie będzie mógł się zapętlić najwyżej wtedy, gdy zostanie uruchomiony z niepoprawną wyrocznią (można podać warunek zakończenia pętli, który będzie powodować, że realizacja algorytmu będzie kończyć się także dla niepoprawanych wyroczni). Wykonywanie algorytmu będzie składać się z dwóch faz. Pierwsza faza będzie trwać tak długo, dopóki będzie prawdziwa nierówność $k < n$, w drugiej będzie prawdziwa równość $k = n$. W każdej fazie zbiór C będzie „zmieniany” (bez zmiany liczby elementów), w pierwszej fazie zbiór C będzie mógł być też „rozszerzany”. Zmiana zbioru C (ale nie rozszerzanie) będzie zawsze połączona z przynajmniej czterokrotnym zmniejszeniem wyznacznika macierzy Grama

$$\mathcal{G}_k(\vec{c}_1, \ldots, \vec{c}_k)$$

(znaczenie wyznacznika Grama dla krat wynika z lematu 13.9). Możemy przerywać działanie algorytmu, jeżeli ten wyznacznik stanie się zbyt mały (zostanie sprecyzowane, jak to należy rozumieć). Początkowo zbiór C jest pusty.

Przypuśćmy, że algorytm rozpoczyna wykonywanie czynności z kolejnej pętli. Opiszemy teraz czynności wykonywane w pierwszej fazie algorytmu. Najpierw algorytm oblicza niezerowy wektor $\vec{b} = (\beta_1, \ldots, \beta_n) \in Q^n$ taki, że $\vec{b}^T\vec{c}_j = 0$ dla $j = 1, \ldots, k$ oraz $\vec{b} \notin L$. Aby obliczyć $\vec{b}$ znajdujemy wektor o współczynnikach całkowitych, spełniający podane równości, a następnie dzielimy go przez taką potęgę 2, aby pewna jego współrzędna wymagała przedstawienia w postaci ułamka $\frac{p}{M}$ dla liczby M spełniającej nierówność $T < M \leqslant 2T$.

Niech q będzie wspólnym mianownikiem współrzędnych wektorów należących do C. Przyjmijmy, że $\vec{d} = (\delta_1, \ldots, \delta_n)$, przy czym

$$\delta_i = \beta_i - q \cdot \left\lfloor \frac{\beta_i}{q} \right\rfloor .$$

Współrzędne wektorów $\vec{b}$ i $\vec{d}$ różnią się o liczby całkowite. Jeżeli jedna ze współrzędnych $\vec{b}$ jest nieskracalnym ułamkiem o mianowniku $M > T$, to tę samą własność ma odpowiednia współrządna $\vec{d}$. Wobec tego $\vec{d} \notin L$.

Obliczmy jeszcze $\vec{d}^T\vec{c}_j$ przyjmując, że $\vec{c}_j = (c_{1,j}, \ldots, c_{n,j})$:

$$\vec{d}^T\vec{c}_j = \vec{b}^T\vec{c}_j - \sum_{i=1}^{n} c_{i,j} q \cdot \left\lfloor \frac{\beta_i}{q} \right\rfloor = - \sum_{i=1}^{n} c_{i,j} q \cdot \left\lfloor \frac{\beta_i}{q} \right\rfloor \in Z. \tag{13}$$

Uruchamiamy teraz z wektorem $\vec{d}$ wyrocznię sprawdzającą, czy dany wektor należy do L. Wyrocznia musi stwierdzić, że $\vec{d} \notin L$ i dodatkowo zwróci wektor $\vec{c} \in L^*$ taki, że $\vec{d}^T\vec{c} \notin Z$. Dalsze działanie algorytmu zależy od wektora $\vec{c}$.

Jeżeli zbiór $C \cup \{\vec{c}\}$ jest liniowo niezależny, to zbiór C jest zastępowany przez $C \cup \{\vec{c}\}$ (określamy to jako rozszerzanie zbioru C).

W przeciwnym razie zbiór C jest zmieniany (wykonujemy operację określaną jako zmiana C). Wtedy

$$\vec{c} = \sum_{i=1}^{k} \lambda_i \vec{c}_i \tag{14}$$

dla pewnych liczb wymiernych λ_i. Rozważmy wektor

$$\vec{c}\,' = \sum_{i=1}^{k}(\lambda_i - \lceil\lambda_i\rfloor)\vec{c}_i = \vec{c} - \sum_{i=1}^{k}\lceil\lambda_i\rfloor\,\vec{c}_i, \tag{15}$$

gdzie $\lceil x\rfloor$ oznacza liczbę całkowitą, która różni się najmniej od x (zaokrąglamy w górę, jeżeli podana definicja nie jest jednoznaczna). Wektory $\vec{c}$ i $\vec{c}\,'$ różnią się o element L^*. Wobec tego $\vec{c}\,' \in L^*$. Co więcej, korzystając z faktu ze wzoru (13) otrzymujemy, że

$$\vec{d}^T\vec{c} - \vec{d}^T\vec{c}\,' = \sum_{i=1}^{k}\lceil\lambda_i\rfloor\,\vec{d}^T\vec{c}_i \in Z.$$

Wobec tego $\vec{d}^T\vec{c}\,' \notin Z$ i w konsekwencji λ_i z wzoru (14) dla pewnej liczby i nie jest całkowite. Niech i_0 będzie największą liczbą o tej własności. Mamy więc $\lambda_{i_0} - \lceil\lambda_{i_0}\rfloor \neq 0$. Implikuje to, że $(C\setminus\{\vec{c}_{i_0}\})\cup\{\vec{c}\,'\}$ jest zbiorem liniowo niezależnych wektorów. Zmiana C polega na zastąpieniu C przez $(C\setminus\{\vec{c}_{i_0}\})\cup\{\vec{c}\,'\}$. Zauważmy jeszcze, że podczas zmiany C wyznacznik macierzy Grama wyznaczonej przez wektory ze zbioru C zmniejsza przynajmniej o połowę. Mamy bowiem

$$|\,\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_{i_0-1},\vec{c}\,',\vec{c}_{i_0+1},\ldots,\vec{c}_k)\,| = |\,\lambda_{i_0} - \lceil\lambda_{i_0}\rfloor\,|^2|\,\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)\,| \leqslant \frac{1}{4}\cdot|\,\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)\,|.$$

W fazie drugiej, a więc gdy $k = n$, na początku pętli znajdujemy bazę dualnę do C, a więc znajdujemy wektory $\vec{b}_i$ takie, że

$$\vec{b}_i^T\vec{c}_j = \begin{cases} 1 & \text{jeżeli } i = j\\ 0 & \text{w przeciwnym razie,}\end{cases}$$

Następnie sprawdzamy uruchamiając wyrocznię, czy $\vec{b}_i$ wektory należą do L. Mogą zajść dwa przypadki.

Jeżeli $\vec{b}_i \in L$ dla $i = 1,\ldots,n$, to algorytm kończy pracę i zwraca wektory $\vec{b}_1,\ldots,\vec{b}_n$. W tym przypadku pokażemy jeszcze, że $L = L(\vec{b}_1,\ldots,\vec{b}_n)$. Zawieranie $L(\vec{b}_1,\ldots,\vec{b}_n) \subseteq L$ jest oczywiste, gdyż wektory $\vec{b}_i \in L$. Aby dowieść zawieranie przeciwne weźmy $\vec{a} \in L$ i przedstawmy go (jako element przestrzeni R^n) w postaci kombinacji liniowej wektorów $\vec{b}_i$, np.

$$\vec{a} = \sum_{i=1}^{n}\alpha_i\vec{b}_i.$$

Wobec tego

$$\vec{a}^T\vec{c}_j = \sum_{i=1}^{n}\alpha_i\vec{b}_i^T\vec{c}_j = \alpha_j.$$

Ponieważ $\vec{a} \in L$ i $\vec{c}_j \in L^*$, więc $\alpha_j \in Z$. To oznacza, że $\vec{a} \in L(\vec{b}_1,\ldots,\vec{b}_n)$.

Jeżeli $\vec{b}_i \notin L$ dla pewnego i, to wyrocznia zwróci tę informację oraz wektor $\vec{c} \in L^*$ taki, że $\vec{b}_i^T\vec{c} \notin Z$. W tym przypadku dalej postępujemy tak, jak podczas zmiany C w fazie pierwszej.

Powinniśmy pokazać, że opisany algorytm nie zapętla się. Najpierw zauważmy, że własność „C jest zbiorem liniowo niezależnych wektorów" jest niezmiennikiem pętli algorytmu i jest stale prawdziwa. Implikuje to, że

$$|\,\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)\,| > 0$$

(jest to konsekwencja lematu 13.3). Z lematu 13.3 wynika także, że jeżeli wszystkie wektory z C mają współrzędne o mianownikach $\leqslant T$, to wyznacznik macierzy $\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)$ daje się przedstawić w postaci ułamka o mianowniku $\leqslant T^{2nk^2}$ (wspólny mianownik współrzędnych elementów C jest $\leqslant T^{nk}$). Wobec tego

$$|\,\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)\,| \geqslant T^{-2nk^2} \geqslant T^{-2n^3}.$$

Będziemy jeszcze analizować liczbę operacji zmieniania zbioru C, które można wykonać nie wykonując operacji rozszerzenia.

Przypuśćmy, że po ostatnim rozszerzeniu powstał zbiór C taki, że

$$|\,\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)\,| \leqslant s.$$

Przypuśćmy, że po wykonaniu t zmian zbioru C otrzymujemy zbiór $C' = \{\vec{c}_1^{\,\prime},\ldots,\vec{c}_k^{\,\prime}\}$. Ponieważ zmiana C jest związana z przynajmniej czterokrotnym zmniejszeniem wyznacznika, więc dla zbioru C' prawdziwa jest nierówność

$$|\,\mathcal{G}_k(\vec{c}_1^{\,\prime},\ldots,\vec{c}_k^{\,\prime})\,| \leqslant \frac{s}{4^t}.$$

Nietrudno zauważyć, że algorytm nie może wykonać $t > \log_4(sT^{2n^3})$ zmian zbioru C, gdyż w przeciwnym razie otrzymalibyśmy zbiór C', dla którego

$$T^{-2n^3} > \frac{s}{4^t} \geqslant |\,\mathcal{G}_k(\vec{c}_1^{\,\prime},\ldots,\vec{c}_k^{\,\prime})\,| \geqslant T^{-2n^3},$$

a to nie jest możliwe. Może więc zostać wykonane najwyżej $\log_4(sT^{2n^3})$ zmian C bez wykonywania rozszerzania.

Stąd łatwo wywnioskować, że algorytm nie zapętla się. Operacja rozszerzania może zostać wykonana najwyżej n razy, a po ostatniej operacji rozszerzania może zostać wykonane najwyżej skończenie wiele operacji zmieniania zbioru C.

Podobne argumenty pozwalają oszacować, ile razy była wykonywana pętla algorytmu. Wymaga to oszacowania wyznaczników macierzy $\mathcal{G}_k(\vec{c}_1,\ldots,\vec{c}_k)$ z góry. Najpierw oszacujemy wektor $\vec{d}$ konstruowany na początku pętli podczas wykonywania algorytmu w fazie pierwszej. Współrzędne δ_i tego wektora spełniają nierówność

$$|\,\delta_i\,| \leqslant q \leqslant T^{n^2}$$

(q to wspólny mianownik współrzędnych elementów C). Liczba δ_i ma przedstawienie w postaci ułamka z mianownikiem $\leqslant 2T$, licznik tego przedstawienia jest więc $\leqslant 2T \cdot T^{n^2}$. Wobec tego

$$\langle \delta_i \rangle \leqslant \langle 2T \rangle + \langle 2T \cdot T^{n^2} \rangle < 2n^2 \langle T \rangle$$

oraz

$$\langle \vec{d} \rangle \leqslant 2n^3 \langle T \rangle.$$

Wyrocznia opisująca kratę L, po otrzymaniu wektora $\vec{d}$ i stwierdzeniu, że $\vec{d} \notin L$ zwraca wektor $\vec{c}$ o rozmiarze $\leqslant w(\langle \vec{d} \rangle)$ dla pewnego wielomianu w. Wobec tego zbiór C jest zawsze rozszerzany o wektor o rozmiarze $\leqslant w(2n^3\langle T \rangle)$. Wektor o takim rozmiarze ma długość

$$\leqslant 2^{w(2n^3\langle T \rangle)} \tag{16}$$

(patrz lemat 7.2). Stąd wynika, że jeżeli podczas wykonania programu powstaje zbiór $C = \{\vec{c}_1, \ldots, \vec{c}_k\}$, to

$$|\, \mathcal{G}_k(\vec{c}_1, \ldots, \vec{c}_k) \,| \leqslant 2^{2k \cdot w(2n^3\langle T \rangle)}.$$

Dowodzimy to pokazując, że fakt ten jest niezmiennikiem wykonywanej pętli. Jest to oczywiste, gdy zbiór C jest zmieniany (wtedy interesujący nas wyznacznik maleje). Jeżeli zbiór C został rozszerzony o element $\vec{c}_{k+1}$, to (na podstawie wniosku 13.7)

$$|\, \mathcal{G}_k(\vec{c}_1, \ldots, \vec{c}_k, \vec{c}_{k+1}) \,| \leqslant |\, \mathcal{G}_k(\vec{c}_1, \ldots, \vec{c}_k) \,| \cdot |\, \vec{c}_{k+1} \,|^2 \leqslant 2^{2k \cdot w(2n^3\langle T \rangle)} \cdot 2^{2w(2n^3\langle T \rangle)} = 2^{2(k+1) \cdot w(2n^3\langle T \rangle)}.$$

Możemy już oszacować liczbę pętli wykonywanych podczas realizacji rozważanego algorytmu. Przyjmując dodatkowo, że $w(x) \geqslant x$ dla dowolnego x, otrzymujemy, że liczba ta nie jest większa niż

$$\sum_{k=1}^{n} (\log_4(2^{2k \cdot w(2n^3\langle T \rangle)} \cdot T^{2n^3}) + 1) \leqslant \sum_{k=1}^{n} (k \cdot w(2n^3\langle T \rangle) + n^3 \log_2 T + 1) \leqslant 2n^2 \cdot w(2n^3\langle T \rangle). \tag{17}$$

Otrzymane oszacowanie pozwala stwierdzić, że opisany algorytm wykonuje wielomianowo wiele (w sensie podanym na początku dowodu) operacji arytmetycznych. Jego wielomianowość wynika z twierdzenia 7.8. Aby się o tym przekonać, wystarczy wykazać, że algorytm wykorzystuje wielomianową pamięć. Wymaga to jeszcze sprawdzenia, że przedstawienia wektorów ze zbioru C mają wielomianowy rozmiar, zwłaszcza, gdy zmieniamy zbiór C (prawdziwość tego faktu podczas rozszerzania już została sprawdzona).

Zmieniając C konstruujemy (patrz (15)) wektor

$$\vec{c}\,' = \sum_{i=1}^{k} (\lambda_i - \lceil \lambda_i \rfloor) \vec{c}_i.$$

Zauważmy, że

$$|\, \vec{c}\,' \,| \leqslant \sum_{i=1}^{k} (\lambda_i - \lceil \lambda_i \rfloor) |\, \vec{c}_i \,| \leqslant n \cdot \max\{|\, \vec{c}_i \,| : 1 \leqslant i \leqslant k\}.$$

Oznacza to, że maksimum długości wektorów ze zbioru C w każdym kolejnym kroku algorytmu zwiększa się najwyżej n-krotnie. Wobec tego, po t krokach algorytmu (po t zmianach lub rozszerzaniach C) mamy

$$|\, \vec{c}\,' \,| \leqslant n^t \cdot 2^{w(2n^3\langle T \rangle)}$$

(sprawdzamy to łatwo przez indukcję korzystając z (16)). Uwzględniając oszacowanie (17) liczby wykonywanych kroków (pętli) otrzymujemy, że

$$| \vec{c}\,' | \leqslant n^{2n^2 \cdot w(2n^3\langle T\rangle)} \cdot 2^{w(2n^3\langle T\rangle)}.$$

Wektor $\vec{c}\,'$ należy do L^*, więc mianowniki jego współrzędnych są $\leqslant T$, a liczniki są $\leqslant | \vec{c}\,' | \cdot T$. Rozmiar $\vec{c}\,'$ możemy oszacować w następujący sposób

$$\begin{aligned} \langle \vec{c}\,' \rangle &\leqslant n \cdot (\langle T\rangle + \langle T \cdot n^{2n^2 \cdot w(2n^3\langle T\rangle)} \cdot 2^{w(2n^3\langle T\rangle)}\rangle) \\ &\leqslant 2n\langle T\rangle + 2n^3 \cdot w(2n^3\langle T\rangle) \cdot \log n + n \cdot w(2n^3\langle T\rangle) \\ &\leqslant 2n\langle T\rangle + n \cdot (2n^3 + 1) \cdot w(2n^3\langle T\rangle). \end{aligned}$$

□

Wniosek 12.10 *Istnieje wielomianowy algorytm sprawdzający, czy dany układ liniowych równań o współczynnikach całkowitych na całkowite rozwiązanie.*

Dowód. Z danego układu równań najpierw usuwamy równania liniowo zależne od pozostałych stosując np. metodę macierzy wierszowo równoważnych, a następnie stosujemy algorytm opisany w rozdz. 12.3 i 12.4 i w dowodzie twierdzenia 12.9. □

Lemat 12.11 *Zbiór całkowitych rozwiązań jednorodnego układu równań liniowych o współczynnikach wymiernych jest kratą spełniającą tezę lematu 12.1.* □

Wniosek 12.12 *Istnieje wielomianowy algorytm znajdujący kratę całkowitych rozwiązań jednorodnego układu równań liniowych o współczynnikach wymiernych.*

Dowód.

Przedstawione metody można rozbudować i wykorzystać do skonstruowania wielomianowego algorytmu, który bada, czy dany układ nierówności liniowych z ustaloną liczbą zmiennych ma całkowite rozwiązanie. Opis tego algorytmu można znaleźć w książce *Geometric Algorithms and Combinatorial Optimization* napisanej przez Martina Grötschela, László Lovásza i Alexandra Schrijvera (w tej książce jest opisany m.in. algorytm badający, czy układ równań liniowych o współczynnikach wymiernych ma całkowite rozwiązanie i metoda elipsoid).