17 Wielomianowość problemu niesprzeczności układu równań liniowych

17.1 Algorytm pomocniczy

Dana jest całkowita tablica A o m wierszach długości n. Niech $\mathcal{A}_1$ będzie następującym algorytmem.

$I := \varepsilon$; $J := \varepsilon$;

$L := A$;

dla wszystkich $i = 1, \ldots, m$

$M_i := 1$;

dopóki istnieją $i \notin I$ **oraz** $j \notin J$ **takie, że** $L_{i,j} \neq 0$

wybierz $i_0 \notin I$ **oraz** $j_0 \notin J$ **takie, że** $L_{i_0,j_0} \neq 0$;

dla wszystkich $i \notin I, i_0$

dla wszystkich $j \notin J, j_0$

$L_{i,j} := (-1)^{p(I,i_0)+p(J,j_0)} \left[(L_{i,j}L_{i_0,j_0} - L_{i,j_0}L_{i_0,j}) \text{ div } M_i\right]$;

$L_{i,j_0} := 0$;

$M_i := (-1)^{p(I,i_0)+p(J,j_0)} L_{i_0,j_0}$;

$I := I, i_0$; $J := J, j_0$

Lemat 17.1 *Następujące własności są niezmiennikami pętli w algorytmie* $\mathcal{A}_1$*:*

1) *jeżeli* $i \notin I$ *oraz* $j \notin J$*, to* $L_{i,j} = (-1)^{p(I,i)+p(J,j)} | A^{I,i;J,j} |$,

2) *jeżeli* $i \notin I$*, to* $M_i = | A^{I,J} |$,

3) *jeżeli* $i \notin I$ *oraz* $j \in J$*, to* $L_{i,j} = 0$,

4) $M_i \neq 0$ *dla* $i = 1, \ldots, m$,

5) $| L^{I,\vec{x};J,\vec{y}} | = | A^{I,\vec{x};J,\vec{y}} | \cdot \prod_{i \in I,\vec{x}} M_i$,

6) *wiersze macierzy* L *i* A *generują tę samą przestrzeń.*

Dowód. Jest oczywiste, że wymienione własności są prawdziwe przed rozpoczęciem wykonywania pętli po raz pierwszy.

Zakładamy, że zatrzymaliśmy wykonywanie algorytmu $\mathcal{A}_1$ w momencie, w którym algorytm rozpoczyna kolejne wykonanie pętli. Mamy więc dane macierze L i M, ciągi I oraz J, a także indeksy i_0 oraz j_0 takie, że $i_0 \notin I$, $j_0 \notin J$ oraz $L_{i_0,j_0} \neq 0$. Załóżmy, że wtedy zachodzą podane własności. Przypuśćmy, że w wyniku podstawiania podczas wykonywania pętli otrzymaliśmy macierze $\mathcal{L}$ oraz $\mathcal{M}$ i ciągi $\mathcal{I}$ oraz $\mathcal{J}$. W razie potrzeby, symbolem ε_0 będziemy oznaczać liczbę $(-1)^{p(I,i_0)+p(J,j_0)}$. Będziemy też symbolem $M_{(i_1,\ldots,i_k)}$ oznaczać iloczyn $\prod_{i=1}^{k} M_i$, a także będziemy stosować analogiczne oznaczenie dla macierzy $\mathcal{M}$.

Rozważmy macierz $L^{I,i_0,i;J,j_0,j}$ dla $i \notin I, i_0$ oraz $j \notin J, j_0$. Rozwińmy wyznacznik tej macierzy wzdłuż wiersza i. Wobec własności 3) mamy

$$| L^{I,i_0,i;J,j_0,j} | =$$
$$= (-1)^{p((I,i_0),i)+p((J,j_0),j)} L_{i,j} | L^{I,i_0;J,j_0} | + (-1)^{p((I,i_0),i)+p((J,j),j_0)} L_{i,j_0} | L^{I,i_0;J,j} |.$$

Zauważmy jeszcze, że

$$(-1)^{p((I,i_0),i)} = (-1)^{p(I,i)+p(i,i_0)}.$$

Stąd wynika, że

$$(-1)^{p((I,j_0),j)+p((I,j),j_0)} = (-1)^{p(I,j)+p(j,j_0)+p(I,j_0)+p(j_0,j)} = -(-1)^{p(I,j)+p(I,j_0)}.$$

Korzystając z powyższych wzorów obliczmy część wzoru na $\mathcal{L}_{i,j}$. Mamy

$$(-1)^{p(I,i_0)+p(J,j_0)}(L_{i,j}L_{i_0,j_0} - L_{i,j_0}L_{i_0,j})$$

$$= (-1)^{p(I,i_0)+p(J,j_0)}$$

$$\cdot((-1)^{p(I,i_0)+p(J,j_0)}L_{i,j}|\ A^{I,i_0;J,j_0}\ | - (-1)^{p(I,i_0)+p(J,j)}L_{i,j_0}|\ A^{I,i_0;J,j}\ |)$$

$$= L_{i,j}\frac{|\ L^{I,i_0;J,j_0}\ |}{M_I M_{i_0}} - (-1)^{p(J,j_0)+p(J,j)}L_{i,j_0}\frac{|\ L^{I,i_0;J,j}\ |}{M_I M_{i_0}}$$

$$= \frac{(-1)^{p((I,i_0),i)+p((J,j_0),j)}}{M_I M_{i_0}}((-1)^{p((I,i_0),i)+p((J,j_0),j)}L_{i,j}|\ L^{I,i_0;J,j_0}\ |$$

$$-(-1)^{p((I,i_0),i)+p((J,j_0),j)+p(J,j_0)+p(J,j)}L_{i,j_0}|\ L^{I,i_0;J,j}\ |)$$

$$= \frac{(-1)^{p((I,i_0),i)+p((J,j_0),j)}}{M_I M_{i_0}}((-1)^{p((I,i_0),i)+p((J,j_0),j)}L_{i,j}|\ L^{I,i_0;J,j_0}\ |$$

$$+(-1)^{p((I,i_0),i)+p((J,j_0),j)}L_{i,j_0}|\ L^{I,i_0;J,j}\ |)$$

$$= \frac{(-1)^{p((I,i_0),i)+p((J,j_0),j)}}{M_I M_{i_0}}(|\ L^{I,i_0,i;J,j_0,j}\ |)$$

$$= \frac{(-1)^{p((I,i_0),i)+p((J,j_0),j)}}{M_I M_{i_0}}|\ A^{I,i_0,i;J,j_0,j}\ | \cdot M_I M_{i_0} M_i$$

$$= (-1)^{p((I,i_0),i)+p((J,j_0),j)}|\ A^{I,i_0,i;J,j_0,j}\ | \cdot M_i$$

$$= (-1)^{p(\mathcal{I},i)+p(\mathcal{J},j)}|\ A^{\mathcal{I},i;\mathcal{J},j}\ | \cdot M_i.$$

Tak więc analizowany fragment wzoru na $\mathcal{L}_{i,j}$ okazał się wielokrotnością M_i, a to implikuje, że

$$\mathcal{L}_{i,j} = \left[(-1)^{p(\mathcal{I},i)+p(\mathcal{J},j)}|\ A^{\mathcal{I},i;\mathcal{J},j}\ | \cdot M_i\right] \textbf{ div } M_i = (-1)^{p(\mathcal{I},i)+p(\mathcal{J},j)}|\ A^{\mathcal{I},i;\mathcal{J},j}\ |.$$

Tym samym zostało dowiedzione, że własność 1) jest niezmiennikiem.

Aby dowieść, że własność 2) jest niezmiennikiem zauważmy, że dla $i \notin I, i_0$

$$\mathcal{M}_i = \varepsilon_0 L_{i_0,j_0} = \varepsilon_0^2|\ A^{I,i_0;J,j_0}\ | = |\ A^{\mathcal{I};\mathcal{J}}\ |.$$

Weźmy $i \notin \mathcal{I}$ oraz $j \in \mathcal{J}$. Oczywiście $i \notin I$, oraz są możliwe dwa przypadki: albo $j \in J$, albo $j = j_0$. W pierwszym przypadku, analizując algorytm stwierdzamy, że $\mathcal{L}_{i,j} = L_{i,j}$ i – wobec tego – $\mathcal{L}_{i,j} = 0$. W drugim przypadku mamy

$$\mathcal{L}_{i,j_0} = (-1)^{p(I,i_0)+p(J,j_0)}\left[(L_{i,j_0}L_{i_0,j_0} - L_{i,j_0}L_{i_0,j_0}) \text{ div } M_i\right] = 0.$$

Tak więc własność 3) jest niezmiennikiem.

Jest oczywiste, że własność 4) jest niezmiennikiem.

Rozważmy macierz $\mathcal{L}^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}}$. Analizowany algorytm nie zmienia wierszy o indeksach należących do $\mathcal{I} = (I, i_0)$. Oznacza to, że w tych wierszach są odpowiednie wyrazy macierzy L. Rozważmy wiersz $\mathcal{L}^{k;\mathcal{J},\vec{y}}$ o indeksie $k \in \vec{x}$. Wiersz ten rozbijamy na dwie części i korzystamy z własności 3):

$$\mathcal{L}^{k;\mathcal{J},\vec{y}} = (\mathcal{L}^{k;\mathcal{J}}, \mathcal{L}^{k;\vec{y}}) = (\vec{0}, \mathcal{L}^{k;\vec{y}}).$$

Pomnóżmy wiersze o indeksach $k \in \vec{x}$ w macierzy $\mathcal{L}^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}}$ przez M_k i wyraźmy je przez elementy macierzy L stosując zapis wektorowy. Korzystając z uwagi z dowodu niezmienniczości własnosci 1) stwierdzającej wykonalność dzielenia z definicji elementu $\mathcal{L}_{i,j}$ otrzymujemy, że

$$M_k \mathcal{L}^{k;\vec{y}} = \varepsilon_0 (L_{i_0,j_0} L^{k;\vec{y}} - L_{k,j_0} L^{i_0;\vec{y}}).$$

Wobec tego

$$M_k \mathcal{L}^{k;\mathcal{J},\vec{y}} = \varepsilon_0 L_{i_0,j_0} L^{k;\mathcal{J},\vec{y}} - \varepsilon_0 L_{k,j_0} \mathcal{L}^{i_0;\mathcal{J},\vec{y}}.$$

Dodajmy do k-tego wiersza macierzy $M_{\vec{x}} \mathcal{L}^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}}$ wektor $\varepsilon_0 L_{k,j_0} \mathcal{L}^{i_0;\mathcal{J},\vec{y}}$. Operacja ta nie zmienia wyznacznika i powoduje, że k-ty wiersz staje się równy $\varepsilon_0 L_{i_0,j_0} L^{k;\mathcal{J},\vec{y}}$. W ten sposób otrzymujemy wzór

$$\begin{aligned} M_{\vec{x}} |\, \mathcal{L}^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| &= |\, L^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| (\varepsilon_0 L_{i_0,j_0})^{|\,\vec{x}\,|} = |\, L^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| \mathcal{M}_{\vec{x}} \\ &= |\, A^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| M_{\mathcal{I}} M_{\vec{x}} \mathcal{M}_{\vec{x}}. = |\, A^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| \mathcal{M}_{\mathcal{I}} \mathcal{M}_{\vec{x}} M_{\vec{x}}. \end{aligned}$$

Stąd wynika, że

$$|\, \mathcal{L}^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| = |\, A^{\mathcal{I},\vec{x};\mathcal{J},\vec{y}} \,| \mathcal{M}_{\mathcal{I},\vec{x}}.$$

Niezmienniczość własności 6) wynika z zależnościami między macierzami L i $\mathcal{L}$ ustalonymi w dowodzie niezmienniczości własności 5). □

Lemat 17.2 *Następująca własność jest niezmiennikiem algorytmu* $\mathcal{A}_1$*:*

> *dla dowolnych ciągów* I_1, I_2, J_1, J_2 *takich, że* $|\, I_1 \,| = |\, J_1 \,|$ *oraz dla dowolnych liczb* i, j*, jeżeli* $I = I_1, i, I_2$*,* $J = J_1, j, J_2$*, to zachodzą warunki*
>
> *(a)* $L_{i,j} \neq 0$*,*
>
> *(b)* $L_{i,j'} = 0$ *dla dowolnego* $j' \in J_1$ *oraz*
>
> *(c)* $L_{i',j} = 0$ *dla dowolnego* $i' \notin (I_1, i)$*.*

Dowód. Będziemy stosować symbolikę opisaną na początku dowodu lematu 17.1. Udowodnimy, że jeżeli przed rozpoczęciem wykonania pętli wartości zmiennych I, J oraz tablica L mają wartości spełniające własności podaną w tezie lematu, to także

> dla dowolnych ciągów I_1, I_2, J_1, J_2 takich, że $|\, I_1 \,| = |\, J_1 \,|$ oraz dla dowolnych liczb i, j, jeżeli $\mathcal{I} = I_1, i, I_2$ i $\mathcal{J} = J_1, j, J_2$, to zachodzą warunki
>
> (a) $\mathcal{L}_{i,j} \neq 0$,
>
> (b) $\mathcal{L}_{i,j'} = 0$ dla dowolnego $j' \in J_1$ oraz
>
> (c) $\mathcal{L}_{i',j} = 0$ dla dowolnego $i' \notin (I_1, i)$.

Przypuśćmy, że $\mathcal{I} = I_1, i, I_2$, $\mathcal{J} = J_1, j, J_2$ oraz $\mid I_1 \mid = \mid J_1 \mid$. Najpierw załóżmy, że ciąg I_2 jest pusty. Wtedy $i = i_0$ oraz $j = j_0$, a także $I_1 = I$ oraz $J_1 = J$. Własność $L_{i,j} \neq 0$ jest oczywista i wynika z wyboru pary i_0, j_0. Analizując program stwierdzamy, że $L_{i,j} = L_{i_0,j_0} = \mathcal{L}_{i_0,j_0}$. Tak więc $\mathcal{L}_{i,j} \neq 0$. Ponadto, z własności 3) z lematu 17.1 wynika, że $\mathcal{L}_{i_0,j'} = 0$ dla $j' \in J$. Ostatnia własność ($\mathcal{L}_{i',j} = 0$ dla $i' \notin (I, i_0)$) w tym przypadku jest uzyskiwana przez stosowne podstawienia wykonywane podczas realizacji algorytmu.

Załóżmy więc, że I_1 jest niepusty. Przypuśćmy, że po usunięciu ostatnich elementów z ciągów I_2 oraz J_2 otrzymujemy ciągi I_2' oraz J_2'. Mamy $I = I_1, i, I_2'$ oraz $J = J_1, j, J_2'$ i – na podstawie podanego założenia – $L_{i,j} \neq 0$, $L_{i,j'} = 0$ dla $j' \in J_1$ oraz $L_{i',j} = 0$ dla $i' \notin (I_1, i)$. Teraz wystarczy sprawdzić, że żaden z elementów macierzy L występujących w podanych stwierdzeniach nie ulega zmianie podczas wykonywania pętli algorytmu (zmieniane są tylko inne elementy macierzy L). W ten sposób otrzymujemy, że $\mathcal{L}_{i,j} \neq 0$, $\mathcal{L}_{i,j'} = 0$ oraz $\mathcal{L}_{i',j} = 0$ dla $j' \in J_1$ oraz $i' \notin (I_1, i)$. □

Algorytm $\mathcal{A}_1$ spełnia tezę lematu 17.1 bez względu na sposób wybierania indeksów i_0 oraz j_0. Wykorzystamy to w kolejnym algorytmie. Będziemy teraz rozważać algorytm $\mathcal{A}$. Daną dla tego algorytmu, podobnie jak dla $\mathcal{A}_1$, jest macierz A o wyrazach całkowitych. Algorytm $\mathcal{A}$ będzie wykorzystywał (do różnych celów) zmienne I^m, J^m, M^m oraz L^m pamiętające wartości odpowiednich zmiennych między oboma wykonaniami algorytmu $\mathcal{A}_1$ i ma następującą postać:

uruchom algorytm $\mathcal{A}_1$;

$I^m := I$; $J^m := J$;

dla wszystkich $i = 1 \ldots, m$ **wykonaj** $M_i^m := M_i$;

$A := L$; $L^m := L$;

uruchom algorytm $\mathcal{A}_1$ **wybierając (dopóki** $\mid J \mid < \mid J^m \mid$**) jako kolejne wartości zmiennych** i_0 **oraz** j_0 **kolejne od końca wyrazy ciągów** I^m **oraz** J^m

17.2 Wielomianowość metody eliminacji Gaussa

Algorytm $\mathcal{A}_1$ zmodyfikowany tak, aby działać zgodnie z końcowym fragmentem opisem algorytmu $\mathcal{A}$ będziemy oznaczać symbolem $\mathcal{A}_1'$. Jeżeli I jest ciągiem, to symbolem I^R będziemy oznaczać ciąg odwrotny od I, a więc ciąg, w którym elementy I ustawione od ostatniego do pierwszego. Dla dwóch ciągów $I = (i_1, \ldots, i_k)$ oraz $J = (j_1, \ldots, j_k)$ symbolem (I, J) będziemy oznaczać ciąg $((i_1, j_1), \ldots, (i_k, j_k))$ par odpowiających sobie wyrazów ciągów I oraz J.

Lemat 17.3 *Przypuśćmy, że mamy macierz A, ciągi I^m oraz J^m takie, że*

dla wszystkich podziałów $I^m = (I_1, i, I_2)$ i $J^m = (J_1, j, J_2)$ tych ciągów mamy

(a) $A_{i,j} \neq 0$,

(b) $A_{i,j'} = 0$ dla $j' \in J_1$ oraz

(c) $A_{i',j} = 0$ dla $i' \notin (I_1, i)$.

Załóżmy także, że algorytm $\mathcal{A}_1'$ jest wykonywany w opisany sposób dla danych ciągów I^m oraz J^m (definicja $\mathcal{A}_1'$ wymaga wskazania dwóch pomocniczych ciągów). Wtedy własności

$$\forall i \forall j \; (j \in J^m \wedge j \notin J \Rightarrow L_{i,j} = M_i \cdot A_{i,j})$$

oraz

$$\forall (i,j) \in (I^m, J^m) \; L_{i,j} \neq 0$$

są niezmiennikami pętli z algorytmu $\mathcal{A}_1'$.

Dowód. Jak w dowodach poprzednich, podobnych lematów, przyjmujemy oznaczenia opisane na początku dowodu lematu 17.1. Zakładamy, że obie własności są prawdziwe na początku pętli. Pokażemy, że będą prawdziwe także po wykonaniu pętli. Możemy dodatkowo założyć, że J^R jest odcinkiem końcowym J^m. Gdyby bowiem J^R zawierał cały J^m, to pierwsza własność byłaby niezmiennikiem z oczywistych powodów, a druga – gdyż algorytm $\mathcal{A}_1'$ nie zmienia wierszy o numerach należących do $\mathcal{I}$ (a także $\mathcal{I}$ musiałoby zawierać I^m). W sytuacji, gdy spełnione jest założenie dodatkowe, prawdziwość drugiej z podanych własności gwarantuje, że można wybrać aktualne wartości zmiennych i_0 oraz j_0 zgodnie z wymaganiami algorytmu $\mathcal{A}_1'$ i wykonanie tego algorytmu nie zostanie w tym momencie przerwane z powodu niemożności zdefiniowania wartości tych zmiennych.

Aby dowieść lemat najpierw zakładamy, że

$$L_{i,j} = M_i \cdot A_{i,j},$$

dla wszystkich $i = 1, \dots, m$ oraz $j \in J^m \setminus J$ i dążymy do wykazania, że

$$\mathcal{L}_{i,j} = \mathcal{M}_i \cdot A_{i,j}$$

dla wszystkich i oraz $j \in J^m \setminus \mathcal{J}$.

Wiersze o numerach $i \in (I, i_0) = \mathcal{I}$ nie ulegają zmianie podczas wykonywania pętli. Dla takich i mamy także $M_i = \mathcal{M}_i$. Tak więc dla dowolnego j i dla $i \in (I, i_0) = \mathcal{I}$ mamy

$$\mathcal{L}_{i,j} = L_{i,j} = M_i \cdot A_{i,j} = \mathcal{M}_i \cdot A_{i,j}.$$

Wobec tego algorytm zachowuje w tym przypadku cały wiersz, a nie tylko opisany w tezie jego fragment.

Założmy, że $i \notin (I, i_0) = \mathcal{I}$ oraz $j \in J^m \setminus \mathcal{J}$. Element $L_{i,j}$ jest zmieniamy zgodnie ze wzorem

$$\mathcal{L}_{i,j} = (-1)^{p(I,i_0)+p(J,j_0)}(L_{i,j}L_{i_0,j_0} - L_{i,j_0}L_{i_0,j}) \text{ div } M_i.$$

Rozważmy wiersz macierzy L o numerze i_0. Oczywiście, $J_1 = J^m \setminus \mathcal{J} \subseteq J^m \setminus J$. Wobec tego, przed wykonaniem pętli prawdziwa jest równość

$$L_{i_0,j} = M_{i_0} \cdot A_{i_0,j}.$$

Z tego samego powodu i z założenia o macierzy A dla podziału $I^m = I_1, i_0, I^R$ oraz $J^m = J_1, j_0, J^R$ mamy, że $A_{i_0,j} = 0$. Tak więc

$$L_{i_0,j} = 0.$$

Stąd wynika, że

$$\mathcal{L}_{i,j} = (-1)^{p(I,i_0)+p(J,j_0)}(L_{i,j}L_{i_0,j_0}) \text{ div } M_i = (A_{i,j} \cdot M_i\mathcal{M}_i) \text{ div } M_i = \mathcal{M}_i \cdot A_{i,j},$$

i dowodzi to, że pierwsza z własności jest niezmiennikiem.

Zajmijmy się więc drugą własnością. Przyjmijmy, że $I^m = (I_1, i_0, I^R)$ dla pewnego ciągu I_1. Niech $(i,j) \in (I^m, J^m)$. Jeżeli $i \in (i_0, I^R)$, to $\mathcal{L}_{i,j} = L_{i,j} \neq 0$ (wiersze o takich numerach nie są zmieniane podczas wykonywania pętli). W przeciwnym razie $j \notin (j_0, J^R)$ (i i j odpowiadają sobie, i mają analogiczne własności), oraz $\mathcal{L}_{i,j} = \mathcal{M}_i \cdot A_{i,j}$. Z lematu 17.1 wynika, że $\mathcal{M}_i \neq 0$, a na podstawie założenia (a) ze sformułowania lematu stwierdzamy, że $A_{i,j}$ jest różna od zera. Tak więc $\mathcal{L}_{i,j} \neq 0$. □

Lemat 17.4 *Przyjmijmy wszystkie założenia o macierzy A, ciągach I^m i J^m, oraz wykonaniu algorytmu $\mathcal{A}_1'$ wymienione w sformułowaniu lematu 17.3 i ponadto, że*

$A_{i,j} = 0$ *dla dowolnego* $i \notin I^m$ *i dowolnego* j.

Wtedy następująca własność

$$\forall i, i', j \ \left[(i,j) \in (I,J) \wedge i \neq i' \ \Rightarrow \ L_{i',j} = 0\right]$$

jest niezmiennikiem pętli z algorytmu $\mathcal{A}_1'$.

Dowód. Jak w poprzednich dowodach, zakładamy, że na początku pętli zachodzi warunek

$$\forall i, i', j \ \left[(i,j) \in (I,J) \wedge i \neq i' \ \Rightarrow \ L_{i',j} = 0\right]$$

i dowodzimy, że po wykonaniu pętli zachodzi warunek

$$\forall i, i', j \ \left[(i,j) \in (\mathcal{I},\mathcal{J}) \wedge i \neq i' \ \Rightarrow \ \mathcal{L}_{i',j} = 0\right].$$

Przypuśćmy więc, że mamy parę $(i,j) \in (\mathcal{I},\mathcal{J})$. Są możliwe dwa przypadki: albo $(i,j) \in (I,J)$, albo $i = i_0$ i $j = j_0$. W pierwszym przypadku, z założenia opisującego sytuację przed wykonaniem pętli mamy $L_{i',j} = 0$ dla $i' \neq i$. Z opisu algorytmu $\mathcal{A}_1'$ wynika, że kolumna o numerze $j \in J$ nie jest zmieniana podczas wykonywania pętli, a więc dla $i' \neq i$ zachodzi $\mathcal{L}_{i',j} = L_{i',j} = 0$.

W kolumnie o numerze j_0 są zerowane elementy z wierszy o numerach $i' \notin I$ i $i' \neq i_0$. Tak więc $\mathcal{L}_{i',j_0} = 0$ dla i' spełniających podany warunek. Powinniśmy się więc zająć indeksami $i' \in I$. Oczywiście, $\mathcal{L}_{i',j_0} = L_{i',j_0}$.

Po pierwsze zauważmy, że algorytm $\mathcal{A}_1'$ nie zmienia wierszy, w których wszystkie wyrazy są równe 0 (albo nie zmienia elementów takich wierszy, albo zmienia jego zgodnie ze wzorem zamieszczonym w opisie algorytmu, a to oznacza, że do elementów takich wierszy wstawia 0). Wobec tego wiersze o indeksach $i \notin I^m$ są podczas wykonywania algorytmu stale wypełnione zerami. Stąd wynika, że I^R jest odcinkiem końcowym I^m i para $(i_0, j_0) \in (I^m, J^m)$. Skorzystamy teraz z lematu 17.3. Wynika z niego, że jest prawdziwa pierwsza z podanych tam własności (jest prawdziwa przed wykonaniem algorytmu, i jest niezmiennikiem). Wobec tego

$$\forall i \forall j \ (j \in J^m \wedge j \notin J \Rightarrow L_{i,j} = M_i \cdot A_{i,j})$$

i – w konsekwencji –

$$\mathcal{L}_{i',j_0} = L_{i',j_0} = M_{i'} \cdot A_{i',j_0}.$$

Weźmy podział ciągów I^m, J^m wyznaczony przez parę i_0, j_0. Niech $I^m = (I_1, i_0, I^R)$ i $J^m = (J_1, j_0, J^R)$. Z założonych własności macierzy A (warunek (c) ze sformułowania lematu 17.3) wynika, że $A_{i',j_0} = 0$ dla $i' \notin (I_1, i_0)$, a więc także dla $i' \in I$. Wobec tego $\mathcal{L}_{i',j_0} = 0$ również dla $i' \in I$. □

Twierdzenie 17.5 *Algorytm cla przekształca daną macierz A o wyrazach całkowitych w równoważną jej wierszowo macierzą L taką, że $L^{\{1,\ldots,m\}\setminus I^m;\{1,\ldots,n\}}$ jest macierzą wypełnioną zerami, a macierz L^{I^m,J^m} ma w każdym wierszu i w każdej kolumnie dokładnie jeden element różny od zera.* □

Lemat 17.6 *Podczas wykonywania algorytmu $\mathcal{A}_1$ uruchomiomego z daną macierzą A o wyrazach całkowitych i o wymiarach $m \times n$ wartości zmiennych co do wartości bezwzględnej są mniejsze niż $\langle A \rangle$.*

Dowód. Z lematu 17.1 wynika, że podczas wykonywania algorytmu $\mathcal{A}_1$ wszystkie zmienne (wszystkie elementy tablic M i L) przechowują liczby będące z dokładnością do znaku wyznacznikami podmacierzy danej macierzy A. Na podstawie lematu 11.5 wartości tych zmiennych szacujemy jako $\leq \langle A \rangle$. □

Twierdzenie 17.7 *Algorytm $\mathcal{A}$ jest wielomianowy i można go zrealizować na wielomianowej maszynie RAM korzystającej z wielomianowej pamięci.*

Dowód. Przypuśćmy, że algorytm $\mathcal{A}$ uruchamiamy z macierzą A o wyrazach całkowitych i o wymiarach $m \times n$. Z poprzedniego lematu otrzymujemy, że rozmiar elementów macierzy L po wykonaniu algorytmu $\mathcal{A}_1$ nie przekracza $\langle A \rangle$ Wobec tego rozmiar macierzy L spełnia nierówność $\langle L \rangle \leq mn\langle A \rangle$. Macierz ta jest daną dla drugiej części algorytmu $\mathcal{A}$. Ponieważ wtedy jest także wykonywany algorytm $\mathcal{A}_1$, więc na podstawie poprzedniego lematu stwierdzamy, że podczas wykonywania drugiej części algorytmu $\mathcal{A}$ wartości zmiennych nie przekraczają $mn\langle A \rangle$. Aby otrzymać tezę wystarczy powołać się na twierdzenie 11.8. □

Wniosek 17.8 *Istnieją algorytmy wykonywane na wielomianowych maszynach RAM korzystających z wielomianowej pamieci i*

1) *znajdujące wymierne rozwiązanie układu równań liniowych o współczynnikach wymiernych,*

2) *wyznaczające rząd macierzy o wyrazach wymiernych,*

3) *obliczające wyznacznik macierzy o wyrazach wymiernych,*

4) *obliczające macierz odwrotną do odwracalnej macierzy o wyrazach wymiernych.* □