7 Metoda Biniego i współaut. konstruowania algorytmów

Przedstawimy teraz sposób konstruowania algorytmów mnożenia macierzy, którego autorami są Bini, Capovati, Lotti i Romani.

7.1 Pewien iloczyn macierzy

Rozważmy funkcję $\mathcal{F} : k^3 \times k^{2\times 2} \to k^{3\times 2}$, która jest „częściowym" mnożeniem macierzy, zdefiniowaną wzorem

$$\mathcal{F}\left((x_{1,1}, x_{1,2}, x_{2,1}), \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{2,1} & y_{2,2} \end{pmatrix}\right) = \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{2,1} & y_{2,2} \end{pmatrix}.$$

Jeżeli argumenty $\mathcal{F}$ w powyższym zbiorze oznaczymy przez X i Y, to otrzymamy

$$\begin{aligned}
\mathcal{F}(X, Y) &= \begin{pmatrix} x_{1,1}y_{1,1} + x_{1,2}y_{2,1} & x_{1,1}y_{1,2} + x_{1,2}y_{2,2} \\ x_{2,1}y_{1,1} & x_{2,1}y_{1,2} \\ 0 & 0 \end{pmatrix} = \\
&= x_{1,1}y_{1,1}E_{1,1} + x_{1,2}y_{2,1}E_{1,1} + x_{1,1}y_{1,2}E_{1,2} + x_{1,2}y_{2,2}E_{1,2} + x_{2,1}y_{1,1}E_{2,1} + x_{2,1}y_{1,2}E_{2,2} = \\
&= \delta_{1,1}(X)\Delta_{1,1}(Y)E_{1,1} + \delta_{1,2}(X)\Delta_{2,1}(Y)E_{1,1} + \delta_{1,1}(X)\Delta_{1,2}(Y)E_{1,2} + \\
&\quad + \delta_{1,2}(X)\Delta_{2,2}(Y)E_{1,2} + \delta_{2,1}(X)\Delta_{1,1}(Y)E_{2,1} + \delta_{2,1}(X)\Delta_{1,2}(Y)E_{2,2},
\end{aligned}$$

gdzie funkcje $\Delta_{i,j}$ są zdefiniowane wzorem (12) (lub (1)), a $\delta_{i,j}$ są analogicznymi funkcjonałami dla przestrzeni k^3 (zauważmy, że ze względu na związki k^3 z przestrzenią macierzy, współrzędne, elementy bazy itp. w tej przestrzeni identyfikujemy za pomocą indeksów $(1,1)$, $(1,2)$ i $(2,1)$).

Funkcja $\mathcal{F}$ jest oczywiście dwuliniowa i należy do $Bil(k^3, k^{2\times 2}, k^{3\times 2})$. Z udowodnionego wzoru wynika, że jako element tej przestrzeni ma następujące przedstawienie:

$$\mathcal{F} = \delta_{1,1}\Delta_{1,1}E_{1,1} + \delta_{1,2}\Delta_{2,1}E_{1,1} + \delta_{1,1}\Delta_{1,2}E_{1,2} + \delta_{1,2}\Delta_{2,2}E_{1,2} + \delta_{2,1}\Delta_{1,1}E_{2,1} + \delta_{2,1}\Delta_{1,2}E_{2,2}.$$

Oczywiście, algorytm obliczający $\mathcal{F}$ zgodnie z definicją wymaga wykonia 6 istotnych mnożeń.

7.2 Przestrzenie $k[\varepsilon]^{m\times n}$ i $Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$

Struktury takiej postaci są bardzo podobne do przestrzeni liniowych, ale nazywają się modułami. Dokładniej, są to $k[\varepsilon]$-moduły, albo moduły nad pierścieniem $k[\varepsilon]$. Moduły nad pierścieniem A mają wszystkie własności wymagane od przestrzeni liniowych, zakładamy jednak, że A jest tylko pierścieniem przemiennym z jednością, a nie ciałem jak w przypadku przestrzeni liniowych.

Pojęcie bazy dla modułów definiujemy tak, jak dla przestrzeni liniowych: bazami są liniowo niezależne zbiory generatorów. Dla modułów pozostają prawdziwe wszystkie własności przedstawione w rozdziałe 3, a w szczególności twierdzenia o definiowaniu przekształceń liniowych i dwuliniowych, i o jednoznaczności takich definicji (patrz fakty i lematy 3.1, 3.2, 3.3 i 3.4). Różnice między modułami i przestrzeniami liniowymi pojawiają się, gdy chcemy konstruować szczególne bazy, np. gdy dowodzimy twierdzenie o możliwości rozszerzenia do bazy dowolnego zbioru liniowo niezależnego. Na przykład, w dowolnej przestrzeni liniowej każdy jednoelementowy układ nie zawierający 0 jest liniowo niezależny i daje się rozszerzyć do bazy. W przestrzeni wymiaru 1 każdy taki układ jest bazą. Podobnie, w zbiorze Z liczb całkowitych (oczywiście, Z jezt Z-modułem) każda różna od 0 liczba całkowita tworzy układ liniowo niezależny. Zauważmy jednak, że podzbiór Z o przynajmniej dwóch elementach jest liniowo zależny, a zbiór jednoelementowy generuje Z wtedy i tylko wtedy, gdy jego elementem jest 1 lub -1. Wobec tego, zbiór $\{2\}$ nie daje się rozszerzyć do bazy modułu Z, mimo że jest liniowo niezależny, a jedynymi bazami w Z są zbiory $\{1\}$ i $\{-1\}$.

Zbiór $k[\varepsilon]^{m\times n}$ macierzy o wymiarach $m \times n$ i o wyrazach będących wielomianami z $k[\varepsilon]$ jest $k[\varepsilon]$-modułem. Jest też przestrzenią liniową (nieskończonego wymiaru!) nad ciałem k. Macierze $E_{i,j}$ dla $i = 1,\dots,m$, $j = 1,\dots,n$ tworzą bazę zarówno modułu $k[\varepsilon]^{m\times n}$ (nad pierścieniem $k[\varepsilon]$), jak i przestrzeni $k^{m\times n}$ (nad ciałem k). Przestrzeń $k^{m\times n}$ jest podprzestrzenią liniową przestrzeni $k[\varepsilon]^{m\times n}$.

Nieco inaczej jest w przypadku $k[\varepsilon]$-modułu $Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$. Oczywiście, jest to także przestrzeń nad ciałem k, ale nie zawiera przestrzeni $Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$. Zawiera ją dopiero po stosownych utożsamieniach.

Przypuśćmy, że mamy $f \in Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$. Możemy zdefiniować przekształcenie $\tilde{f} \in Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$ przyjmując, że spełnia równości

$$\tilde{f}(E_{i,j}, E_{p,q}) = f(E_{i,j}, E_{p,q})$$

dla $i = 1,\dots,m$, $j = 1,\dots,n$. Funkcje f i $\tilde{f}$ są oczywiście różne: dziedzina funkcji f jest właściwym podzbiorem dziedziny $\tilde{f}$. Funkcja $\tilde{f}$ jest jednorodna nad pierścieniem $k[\varepsilon]$, a f – tylko nad ciałem k. Zauważmy, że na produkcie $k^{m\times n} \times k^{n\times k}$ obie funkcje są definiowane tymi samymi wzorami. Obcinając funkcję $\tilde{f}$ do dziedziny f otrzymujemy więc funkcję f, czyli $\tilde{f}$ jest rozszrzeniem f.

Przyporządkowanie funkcji f rozszerzenia $\tilde{f}$ pozwala utożsamiać $Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$ z podprzestrzenią modułu $Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$. Przyporządkowanie to zachowuje dodawanie i mnożenie przez elementy z k, jest więc funkcją liniową nad k. Jest też różnowartościowe (znając $\tilde{f}$ potrafimy odtwotrzyć f). Mówiąc naczej, rozszerzenie to jest monomorfizmem (włożeniem) przestrzeni liniowych nad k.

W przestrzeni $Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$ mamy bazę standardową złożoną z przekształceń $\Delta_{i,j,p,q,s,t}$. Tak samo, jak o tym, możemy przekonać się, że przekształcenia $\tilde{\Delta}_{i,j,p,q,s,t}$ tworzą bazę $k[\varepsilon]$-modułu $Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$. Dla dowolnej funkcji $f \in Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$ mamy zależność

$$f = \sum_{i,j,p,q,s,t} \Delta_{s,t}(f(E_{i,j}, E_{p,q}))\Delta_{i,j,p,q,s,t},$$

gdzie $\Delta_{s,t}(f(E_{i,j}, E_{p,q}))$ oznacza współrzędną o indeksach t, s macierzy $f(E_{i,j}, E_{p,q})$ (patrz wzóry (7) i (15)). Ponieważ współrzędne $\Delta_{s,t}(f(E_{i,j}, E_{p,q}))$ należą do k i $\tilde{}$ jest homomorfizmem, więc także

$$\tilde{f} = \sum_{i,j,p,q,s,t} \Delta_{s,t}(f(E_{i,j}, E_{p,q}))\tilde{\Delta}_{i,j,p,q,s,t}.$$

Zauważmy więc, że jeżeli będziemy pomijać znak $\tilde{}$, to funkcje f i $\tilde{f}$ będą miały identyczne przedstawienia w postaci kombinacji liniowych odpowiednich przekształceń bazowych. W dalszym ciągu najczęściej będziemy utożsamiać f i $\tilde{f}$, a także będziemy we wzorach pomijać znak $\tilde{}$.

Dowolne przekształcenie $F \in Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$ można przedstawić w postaci kombinacji liniowej przekształceń bazowych

$$F = \sum_{i,j,p,q,s,t} w_{i,j,p,q,s,t}\tilde{\Delta}_{i,j,p,q,s,t}$$

dla pewnych wielomianów $w_{i,j,p,q,s,t} \in k[\varepsilon]$. Przedstawiając te wielomiany w postaci kombinacji potęg zmiennej ε otrzymujemy, że

$$F = \sum_{i,j,p,q,s,t} w_{i,j,p,q,s,t}\tilde{\Delta}_{i,j,p,q,s,t} = \sum_{i,j,p,q,s,t}\sum_{l} a_{i,j,p,q,s,t}\varepsilon^l\tilde{\Delta}_{i,j,p,q,s,t} =$$
$$= \sum_l \left(\sum_{i,j,p,q,s,t} a_{i,j,p,q,s,t}\tilde{\Delta}_{i,j,p,q,s,t}\right)\varepsilon^l = \sum_l \tilde{f}_l\varepsilon^l$$

dla odpoweidnich przekształceń $f_l \in Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$. Tak więc każde takie F jest z dokładnością do przyjętych utożsamień wielomianem o współczynnikach ze zbioru $Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$.

Dla takich wielomianów funkcyjnych też zachodzi twierdzenie o jednoznaczności: równe wielomiany mają identyczne współczynniki. Łatwo się o tym przekonać porównując wartości obu wielomianów funkcyjnych dla dowolnych argumentów i korzystając z jednoznaczności przedstawień wielomianów o współczynnikach z k.

7.3 Przekształcenie $\mathcal{F}'$, rząd $\tilde{R}_q$

Niech $\mathcal{F}' : k[\varepsilon]^3 \times k[\varepsilon]^{2\times 2} \to k[\varepsilon]^{3\times 2}$ będzie przekształceniem zdefiniowanym wzorem

$$\begin{aligned}\mathcal{F}' = &(\delta_{1,2} + \varepsilon\delta_{1,1})(\Delta_{1,2} + \varepsilon\Delta_{2,2})E_{1,2} + \\ &+(\delta_{2,1} + \varepsilon\delta_{1,1})\Delta_{1,1}(E_{1,1} + \varepsilon E_{2,1}) - \\ &-\delta_{1,2}\Delta_{1,2}(E_{1,1} + E_{1,2} + \varepsilon E_{2,2}) - \\ &-\delta_{2,1}(\Delta_{1,1} + \Delta_{1,2} + \varepsilon\Delta_{2,1})E_{1,1} + \\ &+(\delta_{1,2} + \delta_{2,1})(\Delta_{1,2} + \varepsilon\Delta_{2,1})(E_{1,1} + \varepsilon E_{2,2}).\end{aligned}$$

Obliczając $\mathcal{F}'(X,Y)$ wartość X podstawiamy w miejsce argumentów funkcjonałów $\delta_{i,j}$, a wartość Y – w miejsce argumentów funkcjonałów $\Delta_{i,j}$, i wykonujemy wyżej opisane obliczenia. Oczywiście, rząd $R(\mathcal{F}')$ (nad pierścieniem $k[\varepsilon]$) jest ≤ 5, a więc obliczenie $\mathcal{F}'(X,Y)$ wymaga w pierścieniu wielomianów $k[\varepsilon]$ wykonania ≤ 5 istotnych mnożeń.

Zauważmy, że

$$\begin{aligned}\mathcal{F}' \;=\; &\delta_{1,2}\Delta_{1,2}E_{1,2} + \varepsilon\delta_{1,2}\Delta_{2,2}E_{1,2} + \varepsilon\delta_{1,1}\Delta_{1,2}E_{1,2} + \varepsilon^2\delta_{1,1}\Delta_{2,2}E_{1,2} + \\ &+\delta_{2,1}\Delta_{1,1}E_{1,1} + \varepsilon\delta_{2,1}\Delta_{1,1}E_{2,1} + \varepsilon\delta_{1,1}\Delta_{1,1}E_{1,1} + \varepsilon^2\delta_{1,1}\Delta_{1,1}E_{2,1} - \\ &-\delta_{1,2}\Delta_{1,2}E_{1,1} - \delta_{1,2}\Delta_{1,2}E_{1,2} - \varepsilon\delta_{1,2}\Delta_{1,2}E_{2,2} - \\ &-\delta_{2,1}\Delta_{1,1}E_{1,1} - \delta_{2,1}\Delta_{1,2}E_{1,1} - \varepsilon\delta_{2,1}\Delta_{2,1}E_{1,1} + \\ &+\delta_{1,2}\Delta_{1,2}E_{1,1} + \delta_{2,1}\Delta_{1,2}E_{1,1} + \varepsilon(\delta_{1,2} + \delta_{2,1})\Delta_{1,2}E_{2,2}) + \\ &\quad +\varepsilon(\delta_{1,2} + \delta_{2,1})\Delta_{2,1}E_{1,1} + \varepsilon^2\delta_{1,2}\Delta_{2,1}E_{2,2} + \delta_{2,1}\Delta_{2,1}E_{2,2} = \\ =\; &\varepsilon\left[(\delta_{1,2}\Delta_{2,2}E_{1,2} + \delta_{1,1}\Delta_{1,2}E_{1,2}) + (\delta_{2,1}\Delta_{1,1}E_{2,1} + \delta_{1,1}\Delta_{1,1}E_{1,1}) - (\delta_{1,2}\Delta_{1,2}E_{2,2}) - \right. \\ &\quad \left. - (\delta_{2,1}\Delta_{2,1}E_{1,1}) + ((\delta_{1,2} + \delta_{2,1})\Delta_{1,2}E_{2,2} + (\delta_{1,2} + \delta_{2,1})\Delta_{2,1}E_{1,1})\right] + \\ &+\varepsilon^2\left(\delta_{1,1}\Delta_{2,2}E_{1,2} + \delta_{1,1}\Delta_{1,1}E_{2,1} + \delta_{1,2}\Delta_{2,1}E_{2,2} + \delta_{2,1}\Delta_{2,1}E_{2,2}\right) = \\ =\; &\varepsilon\mathcal{F} + \varepsilon^2\mathcal{G}\end{aligned}$$

dla odpowiedniego przekształcenia $\mathcal{G}$. W czterech pierwszych linijkach oraz w linijkach piątej i szóstej jest rozpisane 5 iloczynów z wzoru definiującego $\mathcal{F}'$. W kolejnych linijkach składniki poszczególnych iloczynów mnożone przez ε są ujęta w dodatkowe nawiasy. Składniki mnożone przez ε w sumie są równe $\mathcal{F}$. Przedstawione wzory będą interpretowane jako pewien sposób obliczania $\mathcal{F}$ wymagający co prawda 8 mnożeń, ale podzielonych na 5 grup składających się ≤ 2 mnożeń.

O przekształceniu $\mathcal{F} \in Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$ będziemy mówić, że jest rzędu granicznego $\leq r$ wtedy i tylko wtedy, gdy istnieją liczba naturalna q i przekształcenie $\mathcal{F}' \in Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$ takie, że $R(\mathcal{F}') \leq r$ oraz $\mathcal{F}' = \varepsilon^{q-1}\mathcal{F} + \varepsilon^q \mathcal{G}$ dla pewnego $\mathcal{G} \in Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$. Fakt, że $\mathcal{F}$ jest rzędu granicznego $\leq r$ będziemy zapisywać wzorem $\tilde{R}(\mathcal{F}) \leq r$, lub wzorem $\tilde{R}_q(\mathcal{F}) \leq r$, gdy będziemy chcieli jawnie podać także paremetr q. Tak więc warunek $\tilde{R}(\mathcal{F}) \leq r$ jest równoważny istnieniu liczby naturalnej q takiej, że $\tilde{R}_q(\mathcal{F}) \leq r$.

Z powyższych wzorów wynika, że $\tilde{R}_2(\mathcal{F}) \leq 5$.

7.4 Iloczyn $\langle 3, 2, 2\rangle$

Przekształcenie $\mathcal{F}$ zdefiniowane w rozdziale 7.1 będziemy teraz oznaczać symbolem $\mathcal{F}_1$ i dodatkowo zdefiniujemy przekształcenie $\mathcal{F}_2 : k^3 \times k^{2\times 2} \to k^{3\times 2}$ zdefiniowane wzorem

$$\mathcal{F}\left((x_{2,2}, x_{3,1}, x_{3,2}), \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{2,1} & y_{2,2} \end{pmatrix}\right) = \begin{pmatrix} 0 & 0 \\ 0 & x_{2,2} \\ x_{3,1} & x_{3,2} \end{pmatrix} \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{2,1} & y_{2,2} \end{pmatrix}.$$

Przekształcenia clf_1 i $\mathcal{F}_2$ obliczamy właściwie w taki sam sposób: mając wartość jednego z tych przekształceń, wystarczy odpowiednio przestawiać współrzędne argumentów i wartości, aby otrzymać wartość drugiego. Stąd wynika, że oba przekształcenia mają takie same rzędy graniczne (można też powtórzyć rachunki z poprzedniego rozdziału). Tak więc $\tilde{R}_2(\mathcal{F}_2) \leq 5$.

Dla macierzy $X \in K^{3\times 2}$ i $Y \in K^{2\times 2}$ zachodzą następujące wzory:

$$XY = \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \\ x_{3,1} & x_{3,2} \end{pmatrix} Y = \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & 0 \\ 0 & 0 \end{pmatrix} Y + \begin{pmatrix} 0 & 0 \\ 0 & x_{2,2} \\ x_{3,1} & x_{3,2} \end{pmatrix} Y = \mathcal{F}_1(X, Y) + \mathcal{F}_2(X, Y).$$

Stąd otrzymujemy, że $\langle 3, 2, 2\rangle$ jest sumą prostą $\mathcal{F}_1 \oplus \mathcal{F}_2$.

7.5 Rząd sumy prostej przekształceń dwuliniowych

Lemat 7.1 *Jeżeli f_1 i f_2 są przekształceniami dwuliniowymi oraz $R(f_1) \leq r_1$ i $R(f_2) \leq r_2$, to $R(f_1 \oplus f_2) \leq r_1 + r_2$.*

Dowód. Przypuśćmy, że

$$f_1(u_1, v_1) = \sum_{i=1}^{r_1} f_{1,i}(u_1) g_{1,i}(v_1) w_{1,i} \quad \text{oraz} \quad f_2(u_2, v_2) = \sum_{i=1}^{r_2} f_{2,i}(u_2) g_{2,i}(v_2) w_{2,i}.$$

Wtedy

$$(f_1 \oplus f_2)((u_1, u_2), (v_1, v_2)) = (f_1(u_1, v_1), 0) + (0, f_2(u_2, v_2)) =$$
$$= \sum_{i=1}^{r_1} f_{1,i}(u_1) g_{1,i}(v_1)(w_{1,i}, 0) + \sum_{i=1}^{r_2} f_{2,i}(u_2) g_{2,i}(v_2)(0, w_{2,i}). \ \square$$

7.6 Własności rzędu $\tilde{R}_q$

Lemat 7.2 *Jeżeli $\mathcal{F}$ jest przekształceniem dwuliniowym i $\tilde{R}_q(\mathcal{F}) \leq r$, to $R(\mathcal{F}) \leq \frac{q(q+1)}{2} \cdot r$.*

Dowód. Jeżeli $\tilde{R}_q(\mathcal{F}) \leq r$ i $\mathcal{F} \in Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$, to istnieją przekształcenia dwuliniowe $\mathcal{F}', \mathcal{G} \in Bil(k^{m\times n}, k^{n\times k}, k^{m\times k})$ takie, że $\mathcal{F}' = \varepsilon^{q-1}\mathcal{F} + \varepsilon^q\mathcal{G}$ i przy tym rząd $\mathcal{F}'$ jest $\leq r$. Wobec tego, dla pewnych funkcjonałów $f_i \in (k[\varepsilon]^{m\times n})^*$ oraz $g_i \in (k[\varepsilon]^{n\times k})^*$, i dla macierzy $M_i \in k^{m\times k}$ zachodzi wzór

$$\mathcal{F}'(X,Y) = \sum_{i=1}^{r} f_i(X)g_i(Y)M_i.$$

Każdy z funkcjonałów f_i oraz g_i przedstawimy w postaci kombinacji liniowych wektorów ze standardowej bazy. Dla pewnych wielomianów $\sum_j a_{i,j,s,t}\varepsilon^j$ o współczynnikach $a_{i,j,s,t}$ z ciała k i dla odpowiednich funkcjonałów $f_{i,j} \in (k^{m\times n})^*$ zachodzą więc równości

$$f_i(X) = \sum_{s,t=1}^{m,n}\left(\sum_j a_{i,j,s,t}\varepsilon^j\right)\delta_{s,t}(X) = \sum_j\left(\sum_{s,t=1}^{m,n} a_{i,j,s,t}\delta_{s,t}(X)\right)\varepsilon^j = \sum_j f_{i,j}(X)\varepsilon^j.$$

Podobnie, funkcjonały g_i przedstawiamy w postaci

$$g_i(Y) = \sum_j g_{i,j}(Y)\varepsilon^j$$

dla pewnych funkcjonałów $g_{i,j} \in (k^{n\times k})^*$. Postępując analogicznie macierze M_i przedstawiamy w postaci

$$M_i = \sum_j M_{i,j}\varepsilon^j$$

dla pewnych macierzy $M_{i,j} \in k^{m\times k}$. Korzystając z podanych przedstawień otrzymujemy, że

$$\mathcal{F}'(X,Y) = \sum_{i=1}^{r}\left(\sum_u f_{i,u}(X)\varepsilon^u\right)\left(\sum_v g_{i,v}(Y)\varepsilon^v\right)\left(\sum_w M_{i,w}\varepsilon^w\right) =$$
$$= \sum_s\left(\sum_{i=1}^{r}\sum_{u+v+w=s} f_{i,u}(X)g_{i,v}(Y)M_{i,w}\right)\varepsilon^s = \mathcal{F}(X,Y)\varepsilon^{q-1} + \mathcal{G}(X,Y)\varepsilon^q.$$

Stąd i z jednoznaczności przedstawienia wynika, że

$$\mathcal{F}(X,Y) = \sum_{i=1}^{r}\sum_{u+v+w=q-1} f_{i,u}(X)g_{i,v}(Y)M_{i,w} \tag{31}$$

i teraz wystarczy policzyć liczbę składników drugiej sumy w tym wzorze. Indeks u może przyjmować wartości od 0 do $q-1$, jeżeli przyjmuje on wartość u, to v przyjmuje wartości od 0 do $q-1-u$, a więc przyjmuje $q-u$ różnych wartości. Wartości u i v jednoznacznie wyznaczają wartość w. Ostatecznie, suma ta ma

$$\sum_{u=0}^{q-1}(q-u) = \sum_{u=1}^{q} u = \frac{q(q+1)}{2}$$

składników, a we wzorze (31) jest $\leq \frac{q(q+1)}{2}r$ składników. To kończy dowód lematu. □

Lemat 7.3 *Jeżeli* $\tilde{R}_p(\mathcal{F}_1) \le r_1$ *i* $\tilde{R}_q(\mathcal{F}_2) \le r_2$*, to* $\tilde{R}_{\max(p,q)}(\mathcal{F}_1 \oplus \mathcal{F}_2) \le r_1 + r_2$.

Dowód. Dla pewnych przekształceń dwuliniowych $\mathcal{F}_1'$ i $\mathcal{F}_2'$ rzędów r_1 i r_2, o współczynnikach wielomianowych mamy równości

$$\mathcal{F}_1' = \varepsilon^{p-1}\mathcal{F}_1 + \varepsilon^p \mathcal{G}_1 \ \text{ oraz } \ \mathcal{F}_2' = \varepsilon^{q-1}\mathcal{F}_2 + \varepsilon^q \mathcal{G}_2.$$

Wobec tego, jeżeli $p \le q$, to

$$(\varepsilon^{q-p}\mathcal{F}_1') \oplus \mathcal{F}_2' = (\varepsilon^{q-1}\mathcal{F}_1 + \varepsilon^q \mathcal{G}_1) \oplus (\varepsilon^{q-1}\mathcal{F}_2 + \varepsilon^q \mathcal{G}_2) = \varepsilon^{q-1}(\mathcal{F}_1 \oplus \mathcal{F}_2) + \varepsilon^q(\mathcal{G}_1 \oplus \mathcal{G}_2).$$

Aby zakończyć dowód, zauważymy, że z lematu 7.1 wynika nierówność $R(\varepsilon^{q-p}\mathcal{F}_1' \oplus \mathcal{F}_2') \le r_1 + r_2$. □

Wniosek 7.4 *Rząd graniczny iloczynu* $\langle 3,2,2\rangle$ *jest* ≤ 10*, a dokładniej,* $\tilde{R}_2(\langle 3,2,2\rangle) \le 10$.

Dowód. Jest to konsekwencja rozważań zawartych w rozdziale 7.4. □

Lemat 7.5 *Jeżeli* $\tilde{R}_p(\mathcal{F}_1) \le r_1$ *i* $\tilde{R}_q(\mathcal{F}_2) \le r_2$*, to* $\tilde{R}_{p+q-1}(\mathcal{F}_1 \otimes \mathcal{F}_2) \le r_1 r_2$.

Dowód. Z założenia wynika, że dla pewnych przekształceń dwuliniowych $\mathcal{F}_1'$ i $\mathcal{F}_2'$ rzędów r_1 i r_2, o współczynnikach wielomianowych zachodzą równości

$$\mathcal{F}_1' = \varepsilon^{p-1}\mathcal{F}_1 + \varepsilon^p \mathcal{G}_1 \ \text{ oraz } \ \mathcal{F}_2' = \varepsilon^{q-1}\mathcal{F}_2 + \varepsilon^q \mathcal{G}_2.$$

Zauważmy, że stąd wynika równość

$$\mathcal{F}_1' \otimes \mathcal{F}_2' = (\varepsilon^{p-1}\mathcal{F}_1 + \varepsilon^p \mathcal{G}_1) \otimes (\varepsilon^{q-1}\mathcal{F}_2 + \varepsilon^q \mathcal{G}_2) = \varepsilon^{(p+q-1)-1}\mathcal{F}_1 \otimes \mathcal{F}_2 + \varepsilon^{p+q-1}(\mathcal{F}_1\mathcal{G}_2 + \varepsilon\mathcal{G}_1\mathcal{G}_2 + \mathcal{F}_2\mathcal{G}_1).$$

Aby zakończyć dowód, wystarczy zauważyć, że lemat 6.4 implikuje nierówność $R(\mathcal{F}_1' \otimes \mathcal{F}_2') \le r_1 r_2$. □

Lemat 7.6 *Jeżeli* $\tilde{R}_q(\langle m,n,k\rangle) \le r$*, to* $\tilde{R}_q(\langle n,k,m\rangle) \le r$.

Dowód. Rozważania prowadzone w rozdziale 4.4 pozostają prawdziwe, jeżeli zamiast ciała k weźmiemy pierścień wielomianów $k[\varepsilon]$. Tak jak w rozdziale 4.4, konstruujemy izomorfizm

$$\Phi : Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k}) \to Bil(k[\varepsilon]^{n\times k}, k[\varepsilon]^{k\times m}, k[\varepsilon]^{n\times m})$$

taki, że

$$\Phi(\langle m,n,k\rangle) = \langle n,k,m\rangle.$$

Jeżeli $\tilde{R}_q(\langle m,n,k\rangle) \le r$, to istnieją $\mathcal{F}', \mathcal{G} \in Bil(k[\varepsilon]^{m\times n}, k[\varepsilon]^{n\times k}, k[\varepsilon]^{m\times k})$ takie, że $R(\mathcal{F}') \le r$ oraz

$$\mathcal{F}' = \varepsilon^{q-1}\langle m,n,k\rangle + \varepsilon^q \mathcal{G}.$$

Wobec tego

$$\Phi(\mathcal{F}') = \Phi(\varepsilon^{q-1}\langle m,n,k\rangle + \varepsilon^q\mathcal{G}) = \varepsilon^{q-1}\Phi(\langle m,n,k\rangle) + \varepsilon^q\Phi(\mathcal{G}) = \varepsilon^{q-1}\langle n,k,m\rangle + \varepsilon^q\Phi(\mathcal{G}).$$

Ponieważ $R(\Phi(\mathcal{F}')) = R(\mathcal{F}') \le r$, więc rząd graniczny $\langle n,k,m\rangle$ jest $\le r$, a także $\tilde{R}_q(\langle n,k,m\rangle) \le r$. □

Wniosek 7.7 *Rząd graniczny iloczynu* $\langle 12,12,12\rangle$ *jest* ≤ 1000*, a dokładniej,* $\tilde{R}_4(\langle 12,12,12\rangle) \le 1000$.

Dowód. Z wzoru (21) wynika, że $\langle 12,12,12\rangle = \langle 3,2,2\rangle \otimes \langle 2,3,2\rangle \otimes \langle 2,2,3\rangle$, a z lematu 7.6 i oszacowania $\tilde{R}_2(\langle 3,2,2\rangle) \le 5$ otrzymujemy, że także $\tilde{R}_2(\langle 2,3,2\rangle), \tilde{R}_2(\langle 2,2,3\rangle) \le 5$. Teraz wystarczy powołać się na lemat 7.5. □

7.7 Twierdzenie Biniego

Twierdzenie 7.8 (Bini i współaut.) *Jeżeli* $\tilde{R}_q(\langle m, n, k\rangle) \le r$, *to* $(mnk)^{\omega/3} \le r$.

Dowód. Weźmy N-tą potęgę tensorową przekształcenia $(\langle m, n, k\rangle \otimes \langle n, k, m\rangle \otimes \langle k, m, n\rangle)$. Z wzoru (21) otrzymujemy, że jest to iloczyn $\langle (mnk)^N, (mnk)^N, (mnk)^N\rangle$. Z lematów 7.5 i 6.10 wynika, że

$$\tilde{R}_{3N(q-1)+1}(\langle (mnk)^N, (mnk)^N, (mnk)^N\rangle) \le r^{3N}.$$

Wobec tego i lematu 7.2

$$R(\langle (mnk)^N, (mnk)^N, (mnk)^N\rangle) \le \frac{(3N(q-1)+1)(3N(q-1)+2)}{2} \cdot r^{3N}.$$

Stąd i z wniosku 6.8 otrzymujemy, że

$$(mnk)^{N\omega} \le \frac{(3N(q-1)+1)(3N(q-1)+2)}{2} \cdot r^{3N},$$

a po spierwiastkowaniu

$$(mnk)^{\omega/3} \le \sqrt[3N]{\frac{(3N(q-1)+1)(3N(q-1)+2)}{2}} \cdot r.$$

po przejściu z N do granicy w ∞ dostajemy, że

$$(mnk)^{\omega/3} \le \lim_{N\to\infty} \sqrt[3N]{\frac{(3N(q-1)+1)(3N(q-1)+2)}{2}} \cdot r = r. \quad \square$$

Wniosek 7.9 *Współczynnik* ω *jest* $\le \log_{12} 1000 < \log_2 7$.