О сложности алгоритмов умножения полиномиальных матриц

Зуев М.С., Малашонок Г.И. (Тамбов)

В настоящей работе развивается новый подход к оценкам вычислительной сложности алгебраических алгоритмов для разреженных входных данных, предложенный в работах [1–2]. Получены характеристики сложности алгоритмов умножения полиномиальных матриц над над коммутативными областями. Работа опирается на результаты работы [3] настоящего сборника по исследованию сложности полиномиальных алгоритмов.

Рассматриваются полиномиальные матрицы для двух типов коммутативных областей: область $\mathbb{Z}$ - целые числа, для записи которых нужно несколько машинных слов и область $\mathbb{W}$ - область, все элементы которой могут быть записаны в одном машинном слове, например, числа с плавающей точкой или конечные кольца.

1. Алгоритмы умножения матриц над $\mathbb{W}[x]$. Назовем *полиномом типа* (m, α_i) случайный полином $\sum_{i=1}^{m} c_i x^{i-1}$ из $\mathbb{W}[x]$, у которого вероятность того, что коэффициент c_i отличен от нуля равна α_i $(1 \le i \le m)$. Назовем *матрицей типа* (n, m, α_i) случайную матрицу размера $n \times n$ над $\mathbb{W}[x]$, у которой каждый элемент – это полином типа (m, α_i). Если $\alpha_i = \alpha$ для всех i, то будем записывать тип матрицы в виде (n, m, α), а число α будем называть *плотностью матрицы.* Нетрудно проверить, что тип результата операций сложения и умножения определяется типом операндов. Для области характеристики 0 справедливы следующие равенства:

$$(n, m, \alpha) + (n, m, \beta) = (n, m, 1 - (1 - \alpha)(1 - \beta)), \tag{1}$$

$$(n, m, \alpha) \times (n, m, \beta) = (2m - 1, \rho_i^m). \tag{2}$$

Здесь и далее используются обозначения $t_i^m = i$ при $1 \le i \le m$, $t_i^m = 2m - i$ при $m \le i \le 2m - 1$, $\pi_i^m = 1 - (1 - \alpha\beta)^{t_i^m}$ при $1 \le i \le 2m - 1$, $\rho_i^m = 1 - (1 - \pi_i^m)^n$ при $1 \le i \le 2m - 1$, $\mu_s = (1 - \alpha)^{2^s}$, $\sigma(s) = 1 - \mu_s$, $\pi_i^l(r, s) = 1 - (1 - \sigma(r)\sigma(s))^{t_i^l}$, $\rho_i^{l,h}(r, s) = 1 - (1 - \pi_i^l(r, s))^h$, $\nu_{r,s} = \mu_r + \mu_s - \mu_r\mu_s$ для всех неотрицательных целых i, r, s и натуральных h, l.

1.1. Стандартный алгоритм. Будем обозначать, соответственно, $\mathcal{EA}$ и $\mathcal{EM}$ математические ожидания числа операций сложения/вычитания и числа операций умножения в алгоритме. Число операций сложения коэффициентов при сложении двух матриц – это число ненулевых коэффициентов суммы. Поэтому для суммы матриц (1) получим $\mathcal{EA} = n^2 m(1-(1-\alpha)(1-\beta))$. Для стандартного алгоритма умножения матриц (2) получим: $\mathcal{EM} = n^3 m^2 \alpha\beta$, $\mathcal{EA} = n^3 m^2 \alpha\beta + n^2 \sum_{i=1}^{2m-1} \sum_{s=2}^{n} (1 - (1 - \pi_i^m)^s) = n^3 m^2 \alpha\beta + n^2(n-1)(2m-1) - n^2 \sum_{s=2}^{n} F_m((1-\alpha\beta)^s)$. Здесь обозначено $F_m(\lambda) = \sum_{i=1}^{2m-1} \lambda^{t_i^m} = (\lambda^{m+1} + \lambda^m - 2\lambda)/(\lambda - 1)$, при $\lambda \ne 1$, и $F_m(1) = 2m - 1$.

1.2. Алгоритм Штрассена. Формула Штрассена для произведения матриц второго порядка $A = (a_{ij})$ и $B = (b_{ij})$ имеет вид: $AB = \begin{pmatrix} t_1 + t_4 - t_5 + t_7 & t_3 + t_5 \\ t_2 + t_4 & t_1 + t_3 - t_2 + t_6 \end{pmatrix}$ где $t_1 = (a_{11} + a_{22})(b_{11} + b_{22})$, $t_2 = (a_{21} + a_{22})b_{11}$, $t_3 = a_{11}(b_{12} - b_{22})$, $t_4 = a_{22}(b_{21} - b_{11})$, $t_5 = (a_{11} + a_{12})b_{22}$, $t_6 = (a_{21} - a_{11})(b_{11} + b_{12})$, $t_7 = (a_{12} - a_{22})(b_{21} + b_{22})$. Так как здесь всего 7 умножений, то эта формула позволяет получить рекурсивный алгоритм для произведения плотных матриц порядка $n = 2^N$, в котором $n^{\log_2 7}$ операций умножения.

Пусть матрицы A и B имеют тип (n, m, α), $n = 2^N$, $m = 2^M$. Тогда из 7-ми произведений в 3-х случаях оба сомножителя имеют тип $(n/2, m, \alpha)$, а в 4-х случаях – один из сомножителей имеет тип $(n/2, m, \alpha)$, а другой – $(n/2, m, \sigma(1))$. Следовательно на k-том рекурсивном шаге в 7^k умножениях будут участвовать матрицы типа $(n/2^k, m, \sigma(j))$, $j = 0, 1, 2, \ldots, k$.

Обозначим $a_{i,j}^k$ – число произведений, в которых участвуют матрицы типа $(2^{N-k}, m, \sigma(i))$ и $(2^{N-k}, m, \sigma(j))$. Так как в двух случаях (t_2, t_5) возрастает плотность первого сомножителя, в двух случаях (t_3, t_4) возрастает плотность второго сомножителя и в трех случаях (t_1, t_6, t_7) возрастают плотности обоих сомножителей, то производящая функция последовательности $a_{i,j}^k$ имеет вид $(2y + 2z + 3yz)^k = \sum_{i=0}^{k} \sum_{j=0}^{k} a_{i,j}^k y^i z^j$. Следовательно, $a_{i,j}^k = \binom{k}{i}\binom{i}{i+j-k} 2^{2k-i-j} 3^{i+j-k}$, $i, j \le k$, $i + j \ge k$.

Предложение 1. При вычислении произведения матриц типа $(2^N, m, \alpha)$ с помощью алгоритма Штрассена на k-том рекурсивном шаге $(k = 1, \ldots, N)$ выполняется 7^k умножений матриц, из них в $\binom{k}{i}\binom{i}{i+j-k} 2^{2k-i-j} 3^{i+j-k}$ случаях типы первого и второго сомножителей будут, соответственно, $(2^{N-k}, m, \sigma(i))$ и $(2^{N-k}, m, \sigma(j))$, $i, j \le k$, $i + j \ge k$.

Предложение 2. При вычислении произведения матриц типа $(2^N, m, \alpha)$ с помощью алгоритма Штрассена имеем $\mathcal{EM} = \sum_{i=0}^{N}\sum_{j=N-i}^{N}\binom{N}{i}\binom{i}{i+j-N}2^{2N-i-j}3^{i+j-N}\mathcal{EM}^P_{m,i,j}$, где $\mathcal{EM}^P_{m,i,j}$ математическое ожидание числа умножений при вычислении произведения полиномов типа $(m,\sigma(i))$ и $(m,\sigma(j))$, (см.[3]). В частности, при $\alpha = 1$ $\mathcal{EM} = n^{\log_2 7}\mathcal{EM}^P_{m,0,0}$.

Подсчитаем число сложений. Рассмотрим один шаг алгоритма и каждое из сложений, которые здесь выполняются. Пусть матрица A имеет тип $(2l, m, \sigma(r))$, а матрица B имеет тип $(2l, m, \sigma(s))$, $a_{i,j}$ $b_{i,j}$ – их блоки порядка l.

1. При вычислении $t_1, \ldots, t_7$ выполняется 5 сложений матриц типа $(l, m, \sigma(r))$ и столько же – типа $(l, m, \sigma(s))$. При этом $\mathcal{EM}_1 = 5l^2m(\sigma(r+1) + \sigma(s+1))$.

2. Матрицы t_1, t_6, t_7 имеют тип $(l, 2m-1, \rho_i^{m,l}(r+1, s+1))$, матрицы t_2 и t_5 имеют тип $(l, 2m-1, \rho_i^{m,l}(r+1, s))$, матрицы t_3, t_4 имеют тип $(l, 2m-1, \rho_i^{m,l}(r, s+1))$. Следовательно: при вычислении каждой из сумм $t_2 + t_4$ и $t_3 + t_5$ и каждой из разностей $t_4 - t_5$ и $t_3 - t_2$ будет получена матрица типа $(l, 2m-1, \phi_i)$, $\phi_i = 1 - (1 - \rho_i^{m,l}(r, s+1))(1 - \rho_i^{m,l}(r+1, s))$; при вычислении каждой из сумм $t_1 + t_7$ и $t_1 + t_6$ будет получена матрица типа $(l, 2m-1, \chi_i)$, $\chi_i = 1 - (1 - \rho_i^{m,l}(r+1, s+1))^2$; при вычислении каждой из сумм $t_1 + t_4 - t_5 + t_7$ и $t_1 + t_3 - t_2 + t_6$ будет получена матрица типа $(l, 2m-1, \eta_i)$, $\eta_i = 1 - (1 - \chi_i)(1 - \phi_i)$.

Для всех этих действий получим $\mathcal{EM}_2 = l^2\sum_{i=1}^{2m-1}(4\phi_i + 2\chi_i + 2\eta_i) = l^2(8(2m-1) - 4F_m(\phi^l_{r,s}) - 2F_m(\chi^l_{r,s}) - 2F_m(\eta^l_{r,s}))$, где $\phi^l_{r,s} = (\mu_r + \mu_{s+1} - \mu_r\mu_{s+1})^l(\mu_{r+1} + \mu_s - \mu_{r+1}\mu_s)^l$, $\chi^l_{r,s} = (\mu_{r+1} + \mu_{s+1} - \mu_{r+1}\mu_{s+1})^{2l}$, $\eta^l_{r,s} = \phi^l_{r,s}\chi^l_{r,s}$. При этом имеют место равенства $\phi_i = 1 - (\phi^l_{r,s})^{t_i^m}$, $\chi_i = 1 - (\chi^l_{r,s})^{t_i^m}$, $\eta_i = 1 - (\eta^l_{r,s})^{t_i^m}$, $(i = 1, \ldots, 2m-1)$.

3. Учитывая все вычисления в п.1 и п.2, получим математическое ожидание общего числа операций сложения равное $C^{m,l}_{r,s} = l^2(26m - 8 - 5m(\mu_{r+1} + \mu_{s+1}) - 4F_m(\phi^l_{r,s}) - 2F_m(\chi^l_{r,s}) - 2F_m(\eta^l_{r,s}))$.

Предложение 3. В алгоритме Штрассена для произведения матриц типа $(2^N, m, \alpha)$ получим $\mathcal{EA} = \sum_{k=0}^{N-1}\sum_{i=0}^{k}\sum_{j=k-i}^{k}\binom{k}{i}\binom{i}{i+j-k}2^{2k-i-j}3^{i+j-k}C^{m,2^{N-1-k}}_{i,j} + \sum_{i=0}^{N}\sum_{j=N-i}^{N}\binom{N}{i}\binom{i}{i+j-N}\times$ $\times 2^{2N-i-j}3^{i+j-N}\mathcal{EA}^P_{m,i,j}$.

Здесь $\mathcal{EA}^P_{m,i,j}$ обозначает математическое ожидание числа сложений при вычислении произведения полиномов типа $(m,\sigma(i))$ и $(m,\sigma(j))$ (см.[3]).

В частности, при $\alpha = 1$ имеем $\mathcal{EA} = (1/3)(26m - 8)(n^{\log_2 7} - n^2) + n^{\log_2 7}\mathcal{EA}^P_{m,0,0}$.

1.3. Модулярные алгоритмы умножения. Модулярные алгоритмы основаны на китайской теореме об остатках для полиномов. При перемножении матриц типа (n, m, α) максимальная степень элементов у произведения равна $2m - 2$. Следовательно, необходимо $2m - 1$ различных модулей первой степени.

Вычисление пары матриц-сомножителей по каждому модулю требует всего $(2m-1)\cdot mn^2$ умножений и столько же сложений. Произведение двух таких матриц требует n^3 операций умножения и столько же операций сложения в случае стандартного алгоритма умножения, а в случае применения алгоритма Штрассена – $n^{\log_2 7}$ операций умножения и $6(n^{\log_2 7} - n^2)$ операций сложения.

Для восстановления каждого из n^2 полиномов по $2m - 1$ модулям первого порядка при использовании схемы Ньютона с предварительно вычисленными всеми необходимыми коэффициентами требуется $(2m-1)^2$ операций умножения и вдвое большее число операций сложения. Найдем общее число операций.

Предложение 4. В модулярном алгоритме, когда применяется стандартный алгоритм умножения матриц для каждого модуля, число операций сложения равно $\mathcal{A}_{n,m} = n^2(2m-1)(n+5m-2)$, и число операций умножения равно $\mathcal{M}_{n,m} = n^2(2m-1)(n+3m-1)$. Если применяется алгоритм Штрассена для умножения матриц по каждому модулю, то число операций сложения равно $\mathcal{STA} = (2m-1)(6n^{\log_2 7} + 5mn^2 - 8n^2)$, а число операций умножения равно $\mathcal{STM}_{n,m} = (2m-1)(n^{\log_2 7} + 3mn^2 - n^2)$.

1.4. Сравнение алгоритмов умножения матриц над $\mathbb{W}[x]$. Будем предполагать, что среднее время выполнения операций умножения и сложения одинаковое.

Приведем результаты сравнения следующих шести алгоритмов: $(0)M^SP^S$, $(1)M^SP^K$, $(2)M^{St}P^S$, $(3)M^{St}P^K$, $(4)ModM^S$, $(5)Mod\ M^{St}$. Здесь обозначено M^S и M^{St} – стандартный алгоритм умножения матриц и алгоритм Штрассена, P^S и P^K стандартный алгоритм умножения полиномов и алгоритм Карацубы для полиномов, Mod – модулярный алгоритм. В приведенных ниже таблицах для заданных значений n, m, α указан номер лучшего из шести алгоритмов и коэффициент ускорения – МО отношения числа операций в стандартном алгоритме (0) к числу операций в лучшем алгоритме. Плотность α приведена в процентах.

m	n=4				n=16				n=64			
%	1	10	50	100	1	10	50	100	1	10	50	100
4	0	0	0	0	0	0	0	4 1.4	0	0	0	4 2.3
16	0	0	0	3 1.3	0	0	0	4 1.8	0	0	4 1.3	4 4.4
64	0	0	0	3 2.2	0	0	0	3 2.8	0	0	4 1.7	4 6.6
256	0	0	0	3 3.8	0	0	3 1.2	3 4.9	0	0	4 1.9	4 7.6
1024	0	0	3 1.7	3 6.7	0	0	3 2.2	3 8.7	0	0	3 2.8	3 11
4096	0	0	3 3.	3 12	0	0	3 3.9	3 15	0	0	3 5.	3 20
16384	0	0	3 5.3	3 21	0	0	3 6.8	3 27	0	0	3 8.9	3 36
65536	0	0	3 9.3	3 37	0	0	3 12	3 49	0	0	3 16	3 64

m	n=256				n=1024				n=4096			
%	1	10	50	100	1	10	50	100	1	10	50	100
4	0	0	4 1.	4 2.6	0	0	5 1.1	5 3.	0	0	5 1.5	5 3.9
16	0	0	4 2.1	4 7.	0	0	5 2.6	5 8.9	0	0	5 3.6	5 12
64	0	0	4 4.3	4 16	0	0	5 7.3	5 28	0	5 1.1	5 11	5 43
256	0	0	4 6.5	4 26	0	0	5 17	5 67	0	5 1.9	5 34	5 135
1024	0	0	4 7.6	4 30	0	5 1.1	5 26	5 104	0	5 3.3	5 76	5 301
4096	0	0	4 7.9	4 32	0	5 1.2	5 30	5 121	0	5 4.5	5 109	5 436
16384	0	0	3 12	3 47	0	5 1.3	5 32	5 126	0	5 4.9	5 123	5 490
65536	0	0	3 21	3 83	0	5 1.3	5 32	5 128	0	5 5.1	5 127	5 506

Табл. 1. Лучшие алгоритмы для умножения матриц типа (n, m, α) над $\mathbb{W}[x]$ и их коэффициенты ускорения по отношению к стандартному алгоритму.

2. Алгоритмы умножения матриц над $\mathbb{Z}[x]$. Будем предполагать, что коэффициенты полиномов – это целые числа, занимающие несколько машинных слов и будем говорить, что целое число имеет тип (w), если оно хранится в w машинных словах. Примем следующую модель вычислителя: $(w) + (v) = (max(v, w))$, $(w) \times (v) = (w + v)$.

Для алгоритма суммирования типа $(w) + (w)$ число сложений положим равным w, а для стандартного алгоритма умножения $(w) \times (v)$ количество умножений и количество сложений положим равными vw. В качестве альтернативного умножения рассмотрим умножение по алгоритму Карацубы.

Пусть $w = 2^s$, тогда число операций умножения в алгоритме Карацубы для умножения чисел типа (w) равно $N_w^{mK} = w^{\log_2 3}$, а число операций сложения равно $N_w^{aK} = 10(w^{\log_2 3} - w)$. Для стандартного умножения чисел типа (w) число операций сложения и умножения обозначим, соответственно, $N_w^{aS} = w^2$ и $N_w^{mS} = w^2$.

2.1. Стандартный алгоритм умножения матриц. Назовем *полиномом типа* (m, α_i, w) случайный полином $\sum_{i=1}^{m} c_i x^{i-1}$ из $\mathbb{Z}[x]$, у которого коэффициент c_i отличен от нуля с вероятностью α_i $(1 \le i \le m)$ и все ненулевые коэффициенты имеют тип (w). Назовем *матрицей типа* (n, m, α_i, w) случайную матрицу размера $n \times n$ над $\mathbb{Z}[x]$, у которой каждый элемент – это полином типа (m, α_i, w).

Будем обозначать $\mathcal{EA}^P_{m,i,j,w}$ и $\mathcal{EM}^P_{m,i,j,w}$ – математическое ожидание числа сложений и умножений при вычислении произведения полиномов типа $(m, \sigma(i), w)$ и $(m, \sigma(j), w)$ (см.[3]). Стандартный алгоритм и алгоритм Карацубы будем различать по верхнему индексу S или K, соответственно.

Предложение 6. Для стандартного алгоритма умножения матриц типа (n, m, α, w) получим:
$\mathcal{EM} = n^3 \mathcal{EM}^P_{m,0,0,w}$, $\mathcal{EA} = n^3 \mathcal{EA}^P_{m,0,0,w} + 2wn^2(n-1)(2m-1) - 2wn^2 \sum_{s=2}^{n} F_m((1-\alpha^2)^s)$.

2.2. Алгоритм Штрассена умножения матриц.

Предложение 5. При вычислении произведения матриц типа $(2^N, m, \alpha, w)$ с помощью алгоритма Штрассена получим $\mathcal{EM} = \sum_{i=0}^{N} \sum_{j=N-i}^{N} \binom{N}{i} \binom{i}{i+j-N} 2^{2N-i-j} 3^{i+j-N} \mathcal{EM}^P_{m,i,j,w}$,
$\mathcal{EA} = \sum_{k=0}^{N-1} \sum_{i=0}^{k} \sum_{j=k-i}^{k} \binom{k}{i} \binom{i}{i+j-k} 2^{2k-i-j} 3^{i+j-k} C^{m,2^{N-1-k}}_{i,j,w} + \sum_{i=0}^{N} \sum_{j=N-i}^{N} \binom{N}{i} \binom{i}{i+j-N} 2^{2N-i-j} \times$
$\times 3^{i+j-N} \mathcal{EA}^P_{m,i,j,w}$, где $C^{m,l}_{r,s,w} = wl^2(42m - 16 - 5m(\mu_{r+1} + \mu_{s+1}) - 8F_m(\phi^l_{r,s}) - 4F_m(\chi^l_{r,s}) - 4F_m(\eta^l_{r,s}))$.

В выражении $C^{m,l}_{r,s,w}$ учтено, что в матрицах $t_1, \ldots, t_7$ коэффициенты полиномов имеют тип $(2w)$, а в матрицых $a_{i,j}$ и $b_{i,j}$ – тип (w). В частности, при $\alpha = 1$, когда n, m, w – степени двойки и алгоритм Карацубы применяется и для полиномов и для чисел, получим $\mathcal{EM} = n^{\log_2 7}(mw)^{\log_2 3}$.

2.3. Модулярные алгоритмы умножения матриц. При умножении матриц типа (n, m, α, w) в произведении будет получена матрица полиномов над числами типа $(2w)$. Будем полагать, что достаточно $2w+1$ простых модулей $p_1, \ldots, p_{2w+1}$, размеры которых не превышают одного машинного слова, для восстановления коэффициентов в произведении матриц. Для каждого из них необходимо

$2m-1$ различных модулей первой степени для восстановления полиномов. Следовательно, всего необходимо $(2m-1)(2w+1)$ модулей.

Деление числа типа (w) на число, занимающее одно машинное слово требует w операций деления с остатком и столько же вычитаний. Для математического ожидания числа делений $(\mathcal{ED})$ и вычитаний $(\mathcal{EA})$, при нахождения остатков по простым модулям p_i для двух матриц, получим $\mathcal{ED} = \mathcal{EA} = 2n^2 m\alpha w(2w+1)$. Для вычисления остатков по модулям $x-q_i$ для этих $2(2w+1)$ матриц получим $\mathcal{EM} = \mathcal{EA} = 2n^2(2m-1)m(2w+1)$.

Для вычисления произведения каждой из $(2m-1)(2w+1)$ пар матриц для стандартного алгоритма умножения нужно n^3 операций сложения и умножения и для алгоритма Штрассена – $n^{\log_2 7}$ операций умножения и $6(n^{\log_2 7}-n^2)$ операций сложения.

Для восстановления каждого из $n^2(2w+1)$ полиномов по $2m-1$ модулям первого порядка $x-q_i$ при использовании схемы Ньютона с предварительно вычисленными всеми необходимыми коэффициентами требуется $(2m-1)^2$ операций умножения и вдвое большее число операций сложения.

Для восстановления в $\mathbb{Z}$ коэффициентов каждого из n^2 полиномов по $2w+1$ простым модулям p_i по схеме Ньютона требуется $(2w+1)^2$ операций умножения и вдвое большее число операций сложения. Найдем общее число операций.

Предложение 6. В модулярном алгоритме $\mathcal{ED} = 2n^2 m\alpha w(2w+1)$. При чем, когда применяется стандартный алгоритм умножения матриц, то $\mathcal{EM} = n^2(2w+1)(2m-1)(4m+n+2w)$, $\mathcal{EA} = n^2(2w+1)(2m\alpha w + (2m-1)(6m+n+4w))$, а когда применяется алгоритм Штрассена, то $\mathcal{EM} = n^2(2w+1)(2m-1)(4m+n^{\log_2 7-2}+2w)$, $\mathcal{EA} = n^2(2w+1)(2m\alpha w + (2m-1)(6m+6n^{\log_2 7-2}+4w-6))$.

2.4. Сравнение алгоритмов умножения матриц над $\mathbb{Z}[x]$. Будем предполагать, что среднее время выполнения операций умножения и сложения одинаковое, а деление выполняется в 10 раз дольше. Приведем результаты сравнения следующих десяти алгоритмов (0)$M^S P^S N^S$, (1)$M^S P^S N^K$, (2)$M^S P^K N^S$, (3)$M^S P^K N^K$, (4)$M^{St} P^S N^S$, (5)$M^{St} P^S N^K$, (6)$M^{St} P^K N^S$, (7)$M^{St} P^K N^K$, (8)$ModM^S$, (9)$ModM^{St}$. Здесь N^S и N^K обозначают стандартный алгоритм умножения чисел и алгоритм Карацубы для умножения чисел. Остальные обозначения такие же, как и в п.1.4.

В приведенных ниже таблицах для заданных значений n, m, α указан номер лучшего алгоритма и коэффициент ускорения – математическое ожидание отношения числа операций в стандартном алгоритме (0) к числу операций в лучшем алгоритме. Плотность α приведена в процентах.

n=4	w=4				w=16				w=64			
m \%	1	10	50	100	1	10	50	100	1	10	50	100
4	0	0	0	6 1.5	0	0	0	6 2.	1 1.1	1 1.1	1 1.1	7 2.5
16	0	0	0	6 2.5	0	0	2 1.	6 3.4	1 1.1	1 1.1	3 1.3	7 4.3
64	0	0	6 1.1	6 4.2	0	0	6 1.6	6 6.	1 1.1	1 1.1	7 2.	7 7.6
256	0	0	6 1.9	6 7.3	0	0	6 2.7	6 11	1 1.1	1 1.1	7 3.5	7 14
1024	0	0	6 3.3	6 13	0	0	6 4.8	6 19	1 1.1	1 1.1	7 6.1	7 24
4096	0	0	6 5.8	6 23	0	0	6 8.4	6 33	1 1.1	1 1.1	7 11	7 43

n=16	w=4				w=16				w=64			
m \%	1	10	50	100	1	10	50	100	1	10	50	100
4	0	0	0	6 1.9	0	0	0	6 2.6	1 1.1	1 1.1	1 1.1	7 3.2
16	0	0	0	6 3.1	0	0	8 1.5	8 4.7	1 1.1	1 1.1	8 2.3	8 6.6
64	0	0	6 1.4	6 5.4	0	0	8 2.5	8 9.	1 1.1	1 1.1	8 5.9	8 19
256	0	0	6 2.4	6 9.5	0	0	6 3.5	6 14	1 1.1	1 1.1	8 9.9	8 36
1024	0	0	6 4.2	6 17	0	0	6 6.2	6 24	1 1.1	1 1.1	8 12	8 46
4096	0	0	6 7.5	6 30	0	0	6 11	6 44	1 1.1	1 1.1	7 14	7 56

n=64	w=4				w=16				w=64			
m\%	1	10	50	100	1	10	50	100	1	10	50	100
4	0	0	8	8	0	0	8	8	1	1	8	8
			1.	2.9			1.8	5.3	1.1	1.1	2.5	7.
16	0	0	8	8	0	0	8	8	1	1	8	8
			1.9	6.7			4.7	16	1.1	1.1	8.3	24
64	0	0	8	8	0	0	8	8	1	8	8	8
			2.9	11			9.	33	1.1	1.1	22	72
256	0	0	8	8	0	0	8	8	1	8	8	8
			3.4	13			12	46	1.1	1.7	39	140
1024	0	0	6	6	0	0	8	8	1	8	8	8
			5.5	22			13	51	1.1	2.	48	185
4096	0	0	6	6	0	0	6	6	1	8	8	8
			9.8	39			14	57	1.1	2.	50	200

n=256	w=4				w=16				w=64			
m\%	1	10	50	100	1	10	50	100	1	10	50	100
4	0	0	8	8	0	0	8	8	1	1	8	8
			1.5	4.5			3.6	12	1.	1.1	7.2	22
16	0	0	8	8	0	0	8	8	1	8	8	8
			3.6	13			10	37	1.	1.4	24	77
64	0	0	8	8	0	8	8	8	1	8	8	8
			7.8	30		1.3	26	96	1.	3.5	70	237
256	0	0	8	8	0	8	8	8	1	8	8	8
			12	46		1.8	42	162	1.1	6.1	139	509
1024	0	0	8	8	0	8	8	8	1	8	8	8
			14	54		2.	49	196	1.1	7.6	184	714
4096	0	0	8	8	0	8	8	8	1	8	8	8
			14	56		2.1	52	207	1.1	8.1	200	795

n=1024	w=4				w=16			w=64		
m \%	1	10	50	100	1	10	100	1	10	100
4	0	0	9	9	0	0	9	1	1	9
			1.8	5.7			18	1.	1.1	49
16	0	0	9	9	0	9	9	1	9	9
			4.9	18		1.1	61	1.	2.6	173
64	0	0	9	9	0	9	9	1	9	9
			15	57		2.4	195	1.	7.5	590
256	0	9	9	9	0	9	9	1	9	9
		1.5	33	130		5.	460	1.1	18	1532
1024	0	9	9	9	0	9	9	1	9	9
		2.	48	191		7.1	698	1.1	27	2562
4096	0	9	9	9	0	9	9	1	9	9
		2.2	54	217		8.1	802	1.1	31	3080

n=4096	w=4				w=16			w=64		
m \%	1	10	50	100	1	10	100	1	10	100
4	0	0	9	9	0	0	9	1	9	9
			2.4	7.7			26	1.	1.6	87
16	0	0	9	9	0	9	9	1	9	9
			6.9	26		23	90	1.	82	310
64	0	9	9	9	0	9	9	1	9	9
		1.5	23	91		3.9	326	1.	13	1136
256	0	9	9	9	0	9	9	1	9	9
		3.2	70	278		11	1007	1.	39	3598
1024	0	9	9	9	0	9	9	1	9	9
		6.	145	580		22	2125	1.1	82	7915
4096	0	9	9	9	0	9	9	9	9	9
		8.1	199	797		30	2943	1.2	115	11316

Табл. 2. Лучшие алгоритмы для умножения матриц типа (n, m, α, w) над $\mathbb{Z}[x]$ и их коэффициенты ускорения по отношению к стандартному алгоритму.

Работа выполнена при частичной поддержке грантов Минобразования (проект E02-2.0-98), Университеты России (проект 04.01.051), РФФИ (проект 04-07-90268) и Human Capital Foundation (проект 23-03-24).

Литература

1. G.I. Malaschonok, Complexity Considerations in Computer Algebra. — Computer Algebra in Scientific Computing, CASC 2004. — Techn. Univ. Munchen, Garching, Germany, 2004. C.325—332

2. Г.И.Малашонок, Сложность быстрого умножения на разреженных структурах. — Сб. Алгебра, логика и кибернетика /Материалы международной конференции/ — Иркутск, Изд-во ГОУ ВПО "ИГПУ", 2004, С. 175-177.

3. Ю.Д.Валеев, Г.И.Малашонок, О сложности алгоритмов умножения полиномов. — Настоящий сборник.

Данная работа опубликована в: Труды 6-ой Международной конференции "Дискретные модели в теории управляющих систем", ВМиК МГУ им. М.В.Ломоносова, 2004, 32-40.