О сложности алгоритмов умножения полиномов

Валеев Ю.Д., Малашонок Г.И. (Тамбов)

В работах [1,2] предлагается новый подход к оценке вычислительной сложности алгебраических алгоритмов с разреженными входными данными. Он состоит в анализе степени разреженности данных в течение всего вычислительного процесса и получении точных выражений для математического ожидания числа всех арифметических операций.

В настоящей работе развивается этот подход для сравнения алгоритмов умножения полиномов над коммутативными областями. Такие алгоритмы часто применяются во многих приложениях теории управляющих систем.

Рассматриваются области двух видов: 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.

Алгоритмы умножения полиномов в области $\mathbb{W}[x]$

Определение 1. Назовем *полиномом типа* (m, α_i) случайный полином $\sum_{i=1}^m c_i x^{i-1}$ из $\mathbb{W}[x]$ коэффициент c_i которого отличен от нуля с вероятностью α_i $(1 \le i \le m)$.

Обозначим $\mathcal{E}(m, \alpha_i)$ математическое ожидание числа ненулевых коэффициентов полинома типа (m, α_i): $\mathcal{E}(m, \alpha_i) = \sum_{i=1}^m \alpha_i$. Если $\alpha_i = \alpha$ для всех i, то будем записывать тип полинома в виде (m, α), а число α будем называть *плотностью полинома.*

Нетрудно проверить, что тип результата операций сложения и умножения определяется типом операндов. Для области характеристики 0 справедливы следующие равенства:

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

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

Здесь и далее используются обозначения

$$t_i^m = i, \text{ при } 1 \le i \le m, \ t_i^m = 2m - i, \text{ при } m \le i \le 2m-1, \tag{3}$$

$$\pi_i^m = 1 - (1-\alpha\beta)^{t_i^m} \text{ при } 1 \le i \le 2m-1. \tag{4}$$

Будем обозначать, соответственно, $\mathcal{EA}$ и $\mathcal{EM}$ математические ожидания числа операций сложения и числа операций умножения в алгоритме.

Число операций сложения коэффициентов при сложении двух полиномов – это число ненулевых коэффициентов суммы. Поэтому для суммы полиномов (1) получим $\mathcal{EA} = m(1-(1-\alpha)(1-\beta))$.Для стандартного алгоритма умножения полиномов (2) получим $\mathcal{EM} = \mathcal{EA} = m^2\alpha\beta$.

Оценим сложность алгоритма Карацубы для умножения полиномов.

Пусть f и g – полиномы, имеющие типы (m, β) и (m, γ), $m = 2l$, $0 < \beta, \gamma \le 1$. Алгоритм Карацубы для вычисления произведения этих полиномов состоит в рекурсивном вычислении по формуле

$$fg = ac + (ac + bd - (a-b)(c-d))x^l + bdx^{2l}, \tag{5}$$

где $f = a + bx^l$, $g = c + dx^l$, a, b – полиномы типа (l, β), c, d – типа (l, γ). Обозначим

$$\mu_s = (1-\alpha)^{2^s}, \quad \sigma(s) = 1 - \mu_s, \tag{6}$$

$$\pi_i^l(r,s) = 1 - (1-\sigma(r)\sigma(s))^{t_i^l}, \ \rho_i^{l,h}(r,s) = 1 - (1-\pi_i^l(r,s))^h, \ \nu_{r,s} = \mu_r + \mu_s - \mu_r\mu_s,$$

для всех неотрицательных целых i, r, s и натуральных h, l, а t_i^l определено в (3).

Тогда $\sigma(0) = \alpha$, $\pi_i^l(r,s) = 1 - (\nu_{r,s})^{t_i^l}$, $\rho_i^{l,h}(r,s) = 1 - (\nu_{r,s})^{ht_i^l}$ и из (1) и (2) для всех неотрицательных целых i, r, s и натуральных h, l следуют равенства:

$$(l, \sigma(r)) + (l, \sigma(r)) = (l, \sigma(r+1)), \quad (l, \sigma(r)) \times (l, \sigma(s)) = (2l-1, \pi_i^l(r,s)), \tag{7}$$

$$\sum_{j=1}^h (2l-1, \pi_i^l(r,s)) = (2l-1, \rho_i^{l,h}(r,s)). \tag{8}$$

Рассмотрим алгоритм Карацубы (5) для случая, когда $m = 2^M$, $\beta = \sigma(r)$, $\gamma = \sigma(s)$, где r и s – могут быть любыми неотрицательными целыми.

Отметим, что из трех произведений в выражении (5) в двух случаях вычисляются произведения полиномов, имеющих типы $(l, \sigma(r))$ и $(l, \sigma(s))$ и в одном случае,как следует из равенства (7), произведение полиномов, имеющих типы $(l, \sigma(r + 1))$ и $(l, \sigma(s + 1))$.

Следовательно, на k-том рекурсивном шаге нужно вычислять произведения полиномов, имеющих типы $(2^{M-k}, \sigma(r + i))$ и $(2^{M-k}, \sigma(s + i))$, $i = 0, 1, \ldots, k$. Если обозначить d_i^k – число таких произведений на k-том шаге, то легко показать, что $(2 + z)^k = \sum_{i=0}^k d_i^k z^i$ является производящей функцией последовательности d_i^k, при этом $d_i^k = \binom{k}{i} 2^{k-i}$.

Предложение 1. При вычислении произведения полиномов типов $(m, \sigma(r))$ и $(m, \sigma(s))$, $r, s \geq 0$, с помощью алгоритма Карацубы на k-том рекурсивном шаге ($k = 1, \ldots, M$) выполняется 3^k умножений коэффициентов, из них в $\binom{k}{i} 2^{k-i}$ случаях сомножители будут иметь типы $(2^{M-k}, \sigma(r + i))$ и $(2^{M-k}, \sigma(s + i))$, $i = 0, 1, \ldots, k$.

Предложение 2. При вычислении произведения полиномов типов $(m, \sigma(r))$ и $(m, \sigma(s))$, $r, s \geq 0$, с помощью алгоритма Карацубы имеем:

$$\mathcal{EM}_{m,r,s}^{PK} = \sum_{i=0}^{M} \binom{M}{i} 2^{M-i} \sigma(r + i)\sigma(s + i). \tag{9}$$

В частности, при $r = s = 0$ получим $\mathcal{EM}$ для произведения полиномов типа (m, α), а для плотных полиномов при $\alpha = 1$ получим $\mathcal{EM} = m^{\log_2 3}$.

Перейдем к подсчету числа сложений. Рассмотрим один шаг алгоритма (5) и каждое из сложений, которое здесь выполняется.

1. Полиномы $a-b$ и $c-d$ имеют типы $(l, \sigma(r+1))$ и $(l, \sigma(s+1))$. Следовательно, для их вычисления $\mathcal{EA}_1 = l(\sigma(r + 1) + \sigma(s + 1))= l(2 - \mu_{r+1} - \mu_{s+1})$.

2. Полиномы ac и bd имеют тип $(2l - 1, \pi_i^l(r, s))$. Их сумма имеет тип $(2l - 1, \rho_i^{l,2}(r, s))$. Так как $\rho_i^{l,2}(r, s) = 1 - \nu_{r,s}^{2t_i^l}$, то для вычисления суммы $ac+bd$ получим $\mathcal{EA}_2 = \sum_{i=1}^{2l-1} \rho_i^{l,2}(r, s) = 2l-1-F_l(\nu_{r,s}^2)$.

3. Полином $(a - b)(c - d)$ имеет тип $(2l - 1, \pi_i^l(r + 1, s + 1))$. Следовательно, результат вычитания его из полинома $(ac + bd)$ имеет тип $(2l - 1, \psi_i)$, где $\psi_i = 1 - (1 - \rho_i^{l,2}(r, s))(1 - \pi_i^l(r + 1, s + 1)) = 1-(\nu_{r,s}^2 \nu_{r+1,s+1})^{t_i^l}$. Для вычисления этой разности получим $\mathcal{EA}_3 = \sum_{i=1}^{2l-1} \psi_i = 2l-1-F_l(\nu_{r,s}^2 \nu_{r+1,s+1})$.

4. Последнее сложение в (5) – это сложение среднего полинома $(ac + bd - (a - b)(c - d))x^l$ с полиномами ac и bdx^{2l}. При этом его маладшие $l - 1$ коэффициенты складываются со старшими коэффициентами полинома ac, а старшие $l - 1$ коэффициенты складываются с младшими коэффициентами полинома bdx^{2l}. Для каждого из этих сложений $\mathcal{EA}_4 = \sum_{i=1}^{l-1}(1 - (1 - \psi_i)(1 - \pi_{l-i}^l(r, s)) = \sum_{i=1}^{l-1} 1 - (\nu_{r,s}^2 \nu_{r+1,s+1})^i (\nu_{r,s})^{l-i} = l - 1 - (\nu_{r,s})^l G_l(\nu_{r,s} \nu_{r+1,s+1})$.

5. Учитывая все сложения на одном шаге рекурсивного алгоритма $2\mathcal{EA}_1 + \mathcal{EA}_2 + \mathcal{EA}_3 + 2\mathcal{EA}_4$ (п.1 – п.4), получим:

$$CP(l, r, s) = 8l - 4 - l(\mu_{r+1} + \mu_{s+1}) - F_l(\nu_{r,s}^2) - F_l(\nu_{r,s}^2 \nu_{r+1,s+1}) - 2(\nu_{r,s})^l G_l(\nu_{r,s} \nu_{r+1,s+1}).$$

Предложение 3. *При вычислении произведения полиномов типа $(m, \sigma(r))$ и $(m, \sigma(s))$, $r, s \geq 0$, $m = 2^M$ с помощью алгоритма Карацубы имеем:*

$$\mathcal{EA}_{m,r,s}^{PK} = \sum_{k=0}^{M-1} \sum_{i=0}^{k} \binom{k}{i} 2^{k-i} CP(2^{M-k-1}, r + i, s + i). \tag{10}$$

В частности, для произведения плотных полиномов, когда $\alpha = 1$, $r = s = 0$, получим:
$\mathcal{EA} = 6m^{\log_2 3} - 8m + 2$.

Теперь можно найти математическое ожидание отношения числа всех операций в стандартном алгоритме умножения полиномов типа (m, α) и в алгоритме Карацубы. Результаты представлены в правой части Табл.1.

Алгоритмы умножения полиномов в области $\mathbb{Z}[x]$

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 f и g – числа типа (w), $w = 2l$. Алгоритм Карацубы для вычисления произведения этих чисел состоит в рекурсивном вычислении по формуле

$$fg = ac + (ac + bd - (a - b)(c - d))p^l + bdp^{2l}, \tag{11}$$

где $f = a + bx^l$, $g = c + dx^l$, a, b, c, d – числа типа (w), $p = 2^P$, P – число двоичных цифр, которые хранятся в одном машинном слове, .

Так же как при доказательстве Предложения 3 заметим, что при вычислении по формуле (11) необходимо выполнить следующие аддитивные действия: два действия $a - b$ и $c - d$ над числами типа (l) и четыре действия над числами типа $(2l)$. Это следующие действия: $ac + bd$, $(ac + bd) - ((a - b)(c - d))$, сложение с младшей частью (ac) и сложение со старшей частью (bdx^{2l}).

Рассматривая случай, когда $w = 2^s$, получим следующие оценки. Число операций умножения равно $N_w^{mK} = w^{\log_2 3}$.Число операций сложения равно $N_w^{aK} = \sum_{i=0}^{s-1} 3^i(2\cdot2^{s-1-i}+4\cdot2^{s-i}) = 10(w^{\log_2 3} - w)$.

Для стандартного умножения чисел типа (w) число операций сложения и умножения обозначим, соответственно, $N_w^{aS} = w^2$ и $N_w^{mS} = w^2$.Сравнение общего числа операций сложения и умножения алгоритма Карацубы с общим числом операций в стандартном алгоритме показывает, что алгоритм Карацубы начинает выигрывать при $w > 47$. А выигрыш в 2 раза начинается при $w > 298$.

Определение 2. Назовем *полиномом типа* (m, α_i, w) случайный полином $\sum_{i=1}^m c_i x^{i-1}$ из $\mathbb{W}[x]$ коэффициент c_i которого отличен от нуля с вероятностью α_i $(1 \le i \le m)$ и все ненулевые коэффициенты имеют тип (w).

Перейдем к оценке числа операций. 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 $(m, \sigma(j), w)$. Стандартный алгоритм и алгоритм Карацубы будем различать по верхнему индексу S или K, соответственно.

Из Предложений 1 – 3 следуют предложения о математическом ожидании числа операций в стандартном алгоритме и в алгоритме Карацубы для умножения полиномов в $\mathbb{Z}[x]$.

Предложение 4. При вычислении произведения полиномов типов $(m, \sigma(r), w)$ и $(m, \sigma(s), w)$, $r, s \ge 0$, с помощью стандартного алгоритма умножения полиномов, получим

$$\mathcal{EM}^{PS}_{m,r,s,w} = m^2\sigma(r)\sigma(s)N^m_w, \tag{12}$$

$$\mathcal{EA}^{PS}_{m,r,s,w} = m^2\sigma(r)\sigma(s)(N^a_w + 2w). \tag{13}$$

Предложение 5. При вычислении произведения полиномов типов $(m, \sigma(r), w)$ и $(m, \sigma(s), w)$, $r, s \ge 0$, $m = 2^M$ с помощью алгоритма Карацубы имеем:

$$\mathcal{EM}^{PK}_{m,r,s,w} = N^m_w \mathcal{EM}^{PK}_{m,r,s}, \tag{14}$$

$$\mathcal{EA}^{PK}_{m,r,s,w} = N^a_w \mathcal{EM}^{PK}_{m,r,s} + \sum_{k=0}^{M-1}\sum_{i=0}^{k}\binom{k}{i}2^{k-i}CP^{r+i,s+i}_{2^{M-k-1},w}, \tag{15}$$

где

$$CP^{r,s}_{l,w} = w(14l - 8 - l(\mu_{r+1} + \mu_{s+1}) - 2F_l(\nu^2_{r,s}) - 2F_l(\nu^2_{r,s}\nu_{r+1,s+1}) - 4(\nu_{r,s})^l G_l(\nu_{r,s}\nu_{r+1,s+1}), \tag{16}$$

и $\mathcal{EM}^{PK}_{m,r,s}$ определено в (10).

В частности, для произведения плотных полиномов, типа $(m, 1, w)$, когда $\alpha = 1$, $r = s = 0$ и алгоритм Карацубы применяется и для полиномов, и для чисел, получим $\mathcal{EM} = (mw)^{\log_2 3}$.

В правой части таблицы Табл.1 приведены результаты сравнения четырех алгоритмов умножения полиномов из $\mathbb{Z}[x]$:

0. Стандартный алгоритм умножения чисел и полиномов.
1. Алгоритм Карацубы для умножения чисел и стандартный алгоритм умножения полиномов.
2. Стандартный алгоритм умножения чисел и Алгоритм Карацубы для умножения полиномов.
3. Алгоритм Карацубы для умножения и чисел и полиномов.

Алгоритмы сравнивались по общему числу операций умножения и сложения. Плотность полиномов α приведена в процентах. Для каждого типа полинома (m, α, w) в таблице указан номер лучшего алгоритма и коэффициент ускорения – математическое ожидание отношения числа операций в стандартном алгоритме к числу операций в лучшем алгоритме.

Сравнение алгоритмов умножения в $\mathbb{W}[x]$										
m\%	10	20	30	40	50	60	70	80	90	100
4	0.09	0.16	0.22	0.29	0.37	0.46	0.56	0.68	0.81	0.97
8	0.07	0.13	0.18	0.25	0.33	0.43	0.55	0.68	0.83	1.01
16	0.06	0.11	0.18	0.26	0.35	0.47	0.61	0.77	0.95	1.16
32	0.05	0.11	0.19	0.29	0.41	0.55	0.73	0.93	1.16	1.42
64	0.05	0.12	0.21	0.34	0.49	0.68	0.90	1.16	1.45	1.78
128	0.05	0.14	0.26	0.42	0.62	0.86	1.15	1.48	1.86	2.29
256	0.06	0.16	0.32	0.53	0.79	1.11	1.49	1.93	2.43	2.99
512	0.07	0.20	0.40	0.67	1.02	1.44	1.94	2.52	3.18	3.92
2^{10}	0.08	0.25	0.51	0.87	1.33	1.89	2.56	3.33	4.20	5.18
2^{11}	0.10	0.32	0.66	1.14	1.75	2.50	3.38	4.40	5.56	6.86
2^{12}	0.12	0.41	0.87	1.50	2.31	3.30	4.48	5.83	7.38	9.10
2^{13}	0.15	0.53	1.14	1.98	3.06	4.38	5.95	7.75	9.80	12.1
2^{14}	0.19	0.69	1.50	2.62	4.06	5.82	7.91	10.3	13.0	16.1
2^{15}	0.25	0.90	1.98	3.47	5.39	7.74	10.5	13.7	17.4	21.4
2^{16}	0.32	1.19	2.62	4.61	7.17	10.3	14.0	18.3	23.1	28.6

Сравнение алгоритмов умножения в $\mathbb{Z}[x]$												
m	w=4			w=16			w=64			w=256		
%	10	50	100	10	50	100	10	50	100	10	50	100
4	0	0	2	0	0	2	1	1	3	1	1	3
			1.5			1.7	1.1	1.1	1.9	1.9	1.9	3.3
16	0	0	2	0	2	2	1	3	3	1	3	3
			2.1		1.	2.7	1.1	1.3	3.4	1.9	2.2	5.8
64	0	0	2	0	2	2	1	3	3	1	3	3
			3.3		4	4.7	1.1	1.9	5.9	1.9	3.3	10
256	0	2	2	0	2	2	1	3	3	1	3	3
		1.6	5.7		2.3	8.2	1.1	3.	10	1.9	5.2	18
2^{10}	0	2	2	0	2	2	1	3	3	1	3	3
		2.6	10		3.9	14	1.1	5.	18	1.9	8.8	32
2^{12}	0	2	2	0	2	2	1	3	3	1	3	3
		4.5	18		6.6	26	1.1	8.5	33	1.9	15	58
2^{14}	0	2	2	0	2	2	1	3	3	1	3	3
		7.9	31		12	46	1.1	15	58	1.9	26	102
2^{16}	0	2	2	0	2	2	3	3	3	3	3	3
		14	56		20	81	1.3	26	104	2.3	46	182

Табл. 1. Сравнение алгоритмов умножения полиномов в $\mathbb{W}[x]$ (слева) и в $\mathbb{Z}[x]$ (справа).

Работа выполнена при частичной поддержке грантов Минобразования (проект Е02-2.0-98), 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.

Данная работа опубликована в: Труды 6-ой Международной конференции "Дискретные модели в теории управляющих систем", ВМиК МГУ им. М.В.Ломоносова, 2004, 13–19.