Math-Net.Ru

Общероссийский математический портал

С. Б. Гашков, И. С. Сергеев, О построении схем логарифмической глубины для инвертирования в конечных полях, *Дискрет. матем.*, 2008, том 20, выпуск 4, 8–28

DOI: <https://doi.org/10.4213/dm1023>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 34.229.45.116

26 апреля 2023 г., 18:12:44

О построении схем логарифмической глубины для инвертирования в конечных полях

© 2008 г. С. Б. Гашков, И. С. Сергеев

Предложен метод реализации инвертирования в стандартных базисах конечных полей $GF(p^n)$ схемами над $GF(p)$ сложности $O(\varepsilon^{-1}n^{w+\varepsilon})$ и глубины $O(\varepsilon^{-1}\log n)$, где $\varepsilon > 0$, а $w < 1,667$ — экспонента умножения матриц размера $\sqrt{n} \times \sqrt{n}$ и $\sqrt{n} \times n$. Инвертирование в гауссовых нормальных базисах реализуется схемой сложности $O(\varepsilon^{-b}n^{1+c\varepsilon|\log \varepsilon|})$ и глубины $O(\varepsilon^{-1}\log n)$, где b, c — некоторые константы.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 05-01-00994, программы президента Российской Федерации поддержки ведущих научных школ, проект НШ 5400.2006.1, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики», проект «Синтез и сложность управляющих систем».

1. Введение

Интенсивно развивающаяся криптография побуждает к изучению вопросов эффективной реализации арифметики больших конечных полей, в частности, операции инвертирования, которая используется во многих криптографических алгоритмах.

Как обычно, конечное поле $GF(q^n)$ рассматривается как расширение поля $GF(q)$ степени n . Возможны различные представления элементов поля, связанные с различным выбором базиса в нем, тогда все поле порождается линейными комбинациями над $GF(q)$ базисных элементов. Наиболее употребительными являются стандартные базисы, имеющие вид $\{1, \alpha, \dots, \alpha^{n-1}\}$, где в качестве α , генератора базиса, выбирается корень неприводимого над $GF(q)$ многочлена $g(t)$ степени n , являющегося также минимальным многочленом для элемента α .

Вычисления в стандартном базисе поля можно производить, пользуясь модулярной арифметикой многочленов: элементы поля представляются многочленами степени не выше $n - 1$, а результаты выполнения операций приводятся по модулю $g(t)$. Стандартный базис позволяет эффективно реализовать операцию умножения.

Для ускорения операций возведения в степень применяются нормальные базисы вида $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$. Генератором нормального базиса служит корень неприводимого над $GF(q)$ многочлена степени n , корни которого (они же элементы базиса) образуют линейно независимую систему над $GF(q)$.

Задача реализации инвертирования в конечном поле схемами логарифмической глубины рассматривалась ранее в работах [1, 2], в которых были предложены алгоритмы, позволяющие построить такие схемы. Сложность этих схем авторами не оценивалась. В

обеих работах использовалось матричное представление элементов поля и в доказательствах применялась техника матричной алгебры, в частности, теорема Гамильтона–Кэли. В предлагаемом изложении эта техника не используется.

Для реализации операций в поле $GF(q^n)$ будем использовать схемы над $GF(q)$, которые в случае $q = 2$ являются булевыми схемами в обычном смысле (см., например, [3]). Общий случай отличается тем, что входы и выходы принимают значения в $GF(q)$, а элементы схемы реализуют функции над $GF(q)$. В качестве базиса выбирается базис всех двуместных операций в поле $GF(q)$. Построенные схемы можно превратить в булевы, если заменить указанные операции в поле $GF(q)$ реализующими их булевыми схемами. Для оценки сложности и глубины булевых схем инвертирования достаточно умножить сложность и глубину схемы инвертирования над $GF(q)$ соответственно на сложность и глубину булевой схемы для умножения в $GF(q)$ (она, очевидно, сложнее схемы для сложения).

Излагаемый далее алгоритм предназначен для полей с малым простым основанием p . Поэтому сложностью инвертирования в поле $GF(p)$ можно пренебрегать. В основном, прикладное значение имеют поля характеристики два как более удобные для реализации булевыми схемами, но в последнее время в некоторых вопросах криптографии на эллиптических кривых, например, в так называемой криптографии, основанной на спаривании, нашли применения поля нечетной характеристики, в частности, поля $GF(3^n)$ (см. [4, 5, 6]).

В разделе 2 показано, как инвертирование сводится к многократному умножению многочленов. В разделе 3 изложены методы многократного умножения многочленов. В разделе 4 приведен окончательный результат о сложности и глубине инвертирования. В разделе 5 рассмотрено приложение к некоторым типам нормальных базисов.

2. Инвертирование и возведение в степень

Для представления элементов поля мы будем использовать стандартные базисы, но будут рассмотрены также некоторые случаи применения нормальных базисов. Инвертирование в произвольном конечном поле $GF(q^n)$ может быть сведено к возведению в степень специального вида [7] (см. также 4.6.3 в [8]). Согласно малой теореме Ферма, для $x \in GF(q^n)$, $(x, q) = 1$, справедливо равенство $x^{q^n} = x$. Положим $Q = (q^n - q)/(q - 1)$. Тогда

$$x^{-1} = x^Q (x^{Q+1})^{-1}.$$

Следует заметить, что $x^{Q+1} \in GF(q)$, так как $(Q + 1)(q - 1) = q^n - 1$. Таким образом, инвертирование сведено к возведению в степень Q , умножению x^Q на x (оно выполняется проще, чем умножение вообще, поскольку известно, что результат принадлежит полю $GF(q)$, и достаточно вычислить только одну компоненту произведения) и инвертированию в поле коэффициентов $GF(q)$, сложностью которого, если n велико, фактически можно пренебречь. Если $q = 2$, то инвертирование просто совпадает с возведением в степень $Q = 2^n - 2$.

Метод аддитивных цепочек Брауэра (см. 4.6.3 в [9]) позволяет выполнять возведение в степень Q последовательностью из $O(\log n)$ умножений и возведений в степени вида q^k , что приводит к оценке глубины $O(\log^2 n)$ операций над $GF(q)$ (см. [7] или 4.6.2 в [8, 10]). При этом сложность такой схемы оценивается как $O(n^w \log n)$, если операции выполняются в произвольном стандартном базисе (здесь $O(n^w)$ — сложность выполнения операции Фробениуса методом, предложенным в [11]; как показано в [12], $w < 1,667$).

В произвольном нормальном базисе сложность схемы фактически определяется сложностью перехода к полиномиальному базису и обратно — справедлива оценка $O(n^{1,806})$, как следует из [13]. Однако, в случае оптимального нормального базиса сложность схемы инвертирования оценивается как $O(n \log^2 n \log \log n)$, поскольку переход к полиномиальному базису и обратно выполняется схемой сложности $O(n \log n)$ (см. [14], 5.2 в [8]), а умножение в стандартном базисе выполняется методом Шёнхаге–Штрассена (характеристика поля отлична от двух) или методом Шёнхаге для полей характеристики два со сложностью $O(n \log n \log \log n)$ (см. гл. 8 в [15] и [16]).

Для возведения в произвольную степень P в поле $GF(q^n)$ можно использовать разложение показателя P в q -ичной системе счисления $P = [p_k, \dots, p_1, p_0]_q$, $0 \leq p_i \leq q - 1$. Сумму разрядов p_i в обычном смысле назовем q -ичным весом числа P (обозначим его через $\rho(P)$). Схема состоит из двух частей: вычисление степеней x^{q^i} для всех $p_i \neq 0$ и перемножение $\rho(P)$ сомножителей такого вида. Таким образом, сложность (и глубина) схемы зависят от числа ненулевых разрядов числа P и его веса (в случае $q = 2$ эти понятия совпадают). Возведение в степень Q , которая определяется выше, можно свести к возведениям в степень с относительно небольшим весом при помощи следующей леммы.

Лемма 1. Пусть $m = \lceil \sqrt[r]{n-1} \rceil$, $r \in \mathbf{N}$. Тогда для операции возведения в степень $Q = (q^n - q)/(q - 1)$ в поле $GF(q^n)$ можно построить схему над $GF(q)$ сложности и глубины

$$I(n) \leq (2r - 1)E(n, m) + (r - 1)M(n),$$

$$D_I(n) \leq 2D_E(n, m) + D_M(n) + (r - 2) \max\{D_E(n, m), D_M(n)\},$$

где $M(n)$ и $D_M(n)$ — сложность и глубина умножения, а $E(n, m)$ и $D_E(n, m)$ — сложность и глубина возведения в степень с q -ичным весом m в поле $GF(q^n)$. В случае $q = 2$ построенная схема является схемой инвертирования.

Доказательство. Пусть $n - 1 = [n_r, n_{r-1}, \dots, n_1]_m$ в системе счисления с основанием m . Для $i = 1, \dots, r - 1$ положим

$$N_i = 1 + q^{m^{i-1}} + q^{2m^{i-1}} + \dots + q^{(m-1)m^{i-1}} = \frac{q^{m^i} - 1}{q^{m^{i-1}} - 1},$$

так что выполняется равенство

$$N_1 N_2 \dots N_i = q^{m^i} - 1.$$

Далее, пусть $M_i = 0$, если $n_i = 0$, и

$$M_i = q^{[n_r, \dots, n_{i+1}, 0, \dots, 0]_{m+1}} (1 + q^{m^{i-1}} + \dots + q^{(n_i-1)m^{i-1}})$$

в противном случае (в квадратных скобках записано r -разрядное число).

Вес каждого из чисел M_i , N_i не превосходит m . Суммируя тождества

$$N_1 \dots N_{i-1} M_i = (q^{m^{i-1}} - 1) M_i = q(q^{[n_r, \dots, n_i, 0, \dots, 0]} - q^{[n_r, \dots, n_{i+1}, 0, \dots, 0]})$$

по всем $i = 1, \dots, r - 1$, получаем, что

$$Q = q^{n-1} + \dots + q = M_1 + N_1(\dots(M_{r-1} + N_{r-1}M_r)\dots).$$

В соответствии с этой формулой можно построить схему для возведения в степень Q . На первом уровне x возводится в степени M_1 и N_1 ; на следующем x^{N_1} возводится в степени M_2 и N_2 ; на третьем одновременно с возведением $x^{N_1 N_2}$ в степени M_3 и N_3 можно выполнить умножение x^{M_1} на $x^{N_1 M_2}$, и так далее. На i -м уровне производится возведение $x^{N_1 \dots N_{i-1}}$ в степени M_i и N_i , и выполняется умножение $x^{N_1 \dots N_{i-2} M_{i-1}}$ на $x^{M_1 + N_1 (\dots (M_{i-3} + N_{i-3} M_{i-2}) \dots)}$. На $(r + 1)$ -м уровне вычисляется x^Q как произведение вычисленных на предыдущем уровне $x^{M_1 + N_1 (\dots (M_{r-2} + N_{r-2} M_{r-1}) \dots)}$ и $x^{N_1 \dots N_{r-1} M_r}$.

Всего в данной процедуре используется $r - 1$ умножений и $2r - 1$ возведений в степени с весами, не превосходящими m . На первых двух уровнях производятся только возведения в степень, на последнем — только умножения, а на остальных операции обоих видов выполняются параллельно. Лемма доказана.

2.1. Реализация операции Фробениуса

Возведение в степень вида q^k (или операция Фробениуса) в нормальном базисе поля $GF(q^n)$ осуществляется посредством циклического сдвига коэффициентов (что, со схемной точки зрения, реализуется просто перекоммутацией входов). При работе в стандартном базисе можно воспользоваться тем, что эта операция является линейной (более того, она является автоморфизмом поля). Методом О. Б. Лупанова (см. [3]) для произвольного линейного $n \times n$ отображения можно построить схему сложности $O(n^2 / \log_q n)$ и глубины $\log_2 n + O(1)$.

На самом деле, операция Фробениуса может рассматриваться как модулярная композиция (композиция двух многочленов по модулю третьего). Действительно, пусть $x = f(t)$ в полиномиальном представлении, $\deg f < n$. Тогда

$$f^{q^k}(t) \bmod g(t) = f(t^{q^k}) \bmod g(t) = f(t^{q^k \bmod g(t)}) \bmod g(t) = f(\xi(t)) \bmod g(t),$$

где $\xi(t) = t^{q^k} \bmod g(t)$ (напомним, что $g(t)$ — характеристический многочлен данного представления поля). Метод Брента–Кунга [11] (см. также 3.1.6 в [8]) позволяет выполнять модулярную композицию многочленов степени n с существенно меньшим порядком сложности. Более точно, справедливо следующее утверждение.

Лемма 2. Для реализации операции Фробениуса в поле $GF(q^n)$ можно построить схему над $GF(q)$ сложности и глубины

$$S(n) \leq O(n^w) + \sqrt{n}(M(n) + n), \quad D_S(n) = D_M(n) + O(\log n),$$

где w — экспонента умножения матриц размера $\sqrt{n} \times \sqrt{n}$ и $\sqrt{n} \times n$ с логарифмической глубиной.

В работе [12] показано, что $w < 1,667$, откуда, используя для схемы умножения оценки Шёнхаге и Штрассена, получаем, что

$$S(n) = O(n^{1,667}), \quad D_S(n) = O(\log n).$$

Таким образом, сложность и глубина той части схемы для возведения в степень веса m , которая выполняет необходимые операции Фробениуса, удовлетворяют оценкам $O(mn^w)$ и $O(\log n)$ соответственно.

Остается выполнить m -кратное умножение в $GF(q^n)$, которое сводится к умножению многочленов в обычном смысле и приведению их произведения (степени не выше $m(n - 1)$) по модулю $g(t)$. Последняя операция может быть выполнена со сложностью

$(m-1)(M(n)+n)$ и глубиной $D_M(n) + \lceil \log_2 m \rceil$. Действительно, многочлен $f(t)$ степени $mn-1$ можно представить в виде

$$f(t) = f_0(t) + f_1(t)t^n + \dots + f_{m-1}(t)t^{(m-1)n},$$

где $\deg f_i < n$. Тогда, если ввести обозначение $g_i(t) = t^{in} \bmod g(t)$, то

$$f(t) \bmod g(t) = f_0(t) + f_1(t)g_1(t) + \dots + f_{m-1}(t)g_{m-1}(t) \bmod g(t),$$

откуда понятно, как получаются заявленные оценки.

3. Многократное умножение многочленов

Пусть требуется вычислить произведение m многочленов $f_1(x), \dots, f_m(x)$ степени $n-1$. Очевидный способ, состоящий из попарных перемножений, позволяет построить схему сложности $O(mn \log n \log \log n)$ и глубины $O(\log m \log n)$, если для умножения многочленов использовать методы Шёнхаге и Штрассена.

Из результатов [17] следует, что для m -кратного умножения двоичных многочленов можно построить схему оптимальной по порядку глубины $O(\log(mn))$. Из [18] вытекает еще один способ умножения над $GF(2)$ с оценками сложности и глубины $O(m^3 n^2)$ и $O(\log(mn))$, основанный на идее работы [19].

Далее будут изложены модифицированные для умножения нескольких многочленов алгоритмы Шёнхаге и Штрассена. В основу изложения будет положена интерпретация Кантора–Калтофена [20]. В этих алгоритмах используется дискретное преобразование Фурье (ДПФ), поэтому напомним некоторые сведения о нем (более подробно см. [21] и гл. 8 в [8]).

Пусть K — коммутативное кольцо, $\zeta \in K$ — первообразный корень степени N из единицы в данном кольце, для которого выполнено следующее условие: для любого простого $p \mid N$ элемент $\zeta^{N/p} - 1$ не является делителем нуля в K (в таком случае ζ называется примитивным корнем). Дискретным преобразованием Фурье порядка N называется отображение, ставящее в соответствие каждому набору $\gamma_0, \gamma_1, \dots, \gamma_{N-1}$ элементов из K набор $\gamma_0^*, \gamma_1^*, \dots, \gamma_{N-1}^*$ по правилу

$$\gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij}.$$

Если в кольце K число N (сумма N единиц) обратимо, то первоначальный набор может быть восстановлен по формулам

$$\gamma_j = N^{-1} \sum_{i=0}^{N-1} \gamma_i^* \zeta^{-ij}.$$

Такое отображение называется обратным преобразованием Фурье и отличается от прямого постоянным множителем N^{-1} и выбором ζ^{-1} в качестве первообразного корня.

Если набор $\gamma_0, \gamma_1, \dots, \gamma_{N-1}$ связать с коэффициентами многочлена $F(x) = \sum \gamma_i x^i$, то прямое преобразование Фурье вычисляет набор значений многочлена $F(x)$ в точках ζ^j , $j = 0, 1, \dots, N-1$, а именно, $\gamma_j^* = F(\zeta^j)$. Обратное преобразование Фурье восстанавливает коэффициенты единственного многочлена $G(x)$ степени не выше $N-1$ такого,

что $G(\zeta^i) = \gamma_i^*$ для всех $i = 0, 1, \dots, N-1$ (такой же набор значений имеет любой многочлен, совпадающий с $G(x)$ по модулю $x^N - 1$).

В случае, когда N является степенью небольшого простого числа, ДПФ реализуется со сложностью $O(N \log N)$ операций в кольце K при помощи алгоритма, называемого быстрым преобразованием Фурье, схема которого будет понятна из доказательства лемм 3 или 6.

3.1. О применении ДПФ (характеристика 2)

Рассмотрим кольцо $R_s^{(x)} = GF(2)[x]/(x^{2 \cdot 3^{s-1}} + x^{3^{s-1}} + 1)$ двоичных многочленов по модулю $x^{2 \cdot 3^{s-1}} + x^{3^{s-1}} + 1$. В этом кольце элемент x является примитивным корнем степени 3^s из единицы, так как многочлены $x^{2 \cdot 3^{s-1}} + x^{3^{s-1}} + 1$ и $x^{3^{s-1}} - 1$ взаимно просты. Поэтому в $R_s^{(x)}$ определено ДПФ порядка 3^s , а вычисления удобно производить по модулю $x^{3^s} - 1$. Заметим также, что прямое и обратное ДПФ над $R_s^{(x)}$ с вычислительной точки зрения эквивалентны. Для обратного преобразования следует использовать разложение элементов по степеням x^{-1} , а оно отличается от обычного только порядком следования коэффициентов. Деление на N производить не нужно, так как $3^s \equiv 1 \pmod{2}$.

Если $m(n-1) < 2 \cdot 3^{s-1}$, то m -кратное умножение многочленов степени $n-1$ сводится к m -кратному умножению в $R_s^{(x)}$. В соответствии с вышеприведенным замечанием, для представления элементов из $R_s^{(x)}$ будем использовать многочлены степени не выше $3^s - 1$. Для получения однозначного представления требуется приведение по модулю $x^{2 \cdot 3^{s-1}} + x^{3^{s-1}} + 1$ (оно выполняется со сложностью $2 \cdot 3^{s-1}$ и глубиной 1).

Через $M'(m, s)$ и $D'_M(m, s)$ обозначим соответственно сложность и глубину m -кратного умножения в кольце $R_s^{(x)}$, а через $\Phi(s, r)$ и $D_\Phi(s, r)$ — сложность и глубину ДПФ порядка 3^r над $R_s^{(x)}$, $r \leq s$.

Лемма 3. Пусть $r \leq s$. Тогда ДПФ порядка 3^r над $R_s^{(y)}$ реализуется схемой сложности и глубины

$$\Phi(s, r) \leq 2r3^{r+s}, \quad D_\Phi(s, r) \leq 2r.$$

Доказательство. Выберем $z = y^{3^{s-r}}$, корень из единицы степени 3^r в $R_s^{(y)}$, и пусть $\Gamma(x) = \sum \gamma_i x^i$ — многочлен над $R_s^{(y)}$ степени не выше $3^r - 1$. Ясно, что

$$\Gamma(z^l) = \sum_{i=0}^{3^r-1} \gamma_i z^{il} = \sum_{j=0}^2 z^{jl} \sum_{i=0}^{3^{r-1}-1} \gamma_{3i+j} (z^3)^{il} = \Gamma_0(z_*^{l_1}) + z^l \Gamma_1(z_*^{l_1}) + z^{2l} \Gamma_2(z_*^{l_1}),$$

где $z_* = z^3$ — корень степени 3^{r-1} из единицы, $l_1 = l \pmod{3^{r-1}}$,

$$\Gamma_j(x) = \sum_{i=0}^{3^{r-1}-1} \gamma_{3i+j} x^i, \quad j = 0, 1, 2.$$

Пусть необходимые значения $\Gamma_j(z_*^i)$, $j = 0, 1, 2$, $i = 0, 1, \dots, 3^{r-1} - 1$, найдены при помощи трех ДПФ порядка 3^{r-1} . Умножения на степени z не требуют схемных затрат (осуществляются циклическим сдвигом коэффициентов), поэтому для вычисления каждого из 3^r значений $\Gamma(z^l)$ остается выполнить два сложения в $R_s^{(y)}$ со сложностью $2 \cdot 3^s$ и глубиной 2. Получаем рекуррентные неравенства

$$\Phi(s, r) \leq 2 \cdot 3^{s+r} + 3\Phi(s, r-1), \quad D_\Phi(s, r) \leq 2 + D_\Phi(s, r-1),$$

которые, если учесть, что $\Phi(s, 0) = D_\Phi(s, 0) = 0$, приводят к неравенствам

$$\Phi(s, r) \leq 2r3^{s+r}, \quad D_\Phi(s, r) \leq 2r.$$

При помощи следующей леммы можно свести m -кратное умножение в кольце $R_s^{(x)}$ к вычислениям в кольце меньшего порядка, ее доказательство, по существу, состоит в применении итерации метода Шёнхаге [16].

Лемма 4. Пусть $m \leq 3^{s-r}$, тогда

$$\begin{aligned} M'(m, r+s) &\leq 3^s M'(m, s) + 2(m+1)s3^{2s} + (m-1)3^{r+s}, \\ D'_M(m, r+s) &\leq D'_M(m, s) + 4s + \lceil \log_2 m \rceil. \end{aligned}$$

Доказательство. Пусть $f_i \in R_{r+s}^{(x)}$ и $f = f_1 \dots f_m$. Ясно, что

$$f_i = \sum_{j=0}^{3^{r+s}-1} f_{i,j} x^j = \sum_{j=0}^{3^r-1} \left(\sum_{l=0}^{3^s-1} f_{i,l3^r+j} x^{l3^r} \right) x^j = \sum_{j=0}^{3^r-1} \varphi_{i,j}(\tilde{y}) x^j,$$

где $\tilde{y} = x^{3^r}$ и $\deg \varphi_{i,j} < 3^s$.

Установим соответствие между многочленами $\varphi_{i,j}(\tilde{y})$ (степени не выше $3^s - 1$) и элементами $\tilde{\varphi}_{i,j} \in R_s^{(y)}$ по правилу $\tilde{\varphi}_{i,j} = \varphi_{i,j}(y)$. Оно автоматически порождает (взаимно однозначное) соответствие между элементами $R_{r+s}^{(x)}$ и многочленами из $R_s^{(y)}[x]$ степени не выше $3^r - 1$. При этом операции в $R_s^{(y)}[x]$ соответствуют операциям в $R_{r+s}^{(x)}$ с точностью до приведения по модулю $x^{3^r} - y$. Таким образом, если обозначить через $f'_i(x)$ многочлены из $R_s^{(y)}[x]$, соответствующие f_i , и положить $f'(x) = f'_1(x) \dots f'_m(x) \in R_s^{(y)}[x]$, то многочлену $f'(x) \bmod (x^{3^r} - y)$ соответствует искомый элемент $f \in R_{r+s}^{(x)}$.

Многочлен $f'(x)$ имеет степень не выше $m(3^r - 1)$, поэтому он однозначно восстанавливается по своим значениям в $3^s \geq m3^r$ точках $R_s^{(y)}$. Рассмотрим следующий алгоритм m -кратного умножения в $R_{r+s}^{(x)}$.

- (А) Вычислим значения всех многочленов $f'_i(x)$ в точках $1, y, y^2, \dots, y^{3^s-1}$, где y является примитивным корнем степени 3^s в $R_s^{(y)}$, с помощью ДПФ.
- (Б) Произведения $f'(y^j) = f'_1(y^j) \dots f'_m(y^j)$ вычисляются при помощи 3^s m -кратных умножений в $R_s^{(y)}$.
- (В) Многочлен $f'(x)$ восстанавливается по значениям в точках $1, y, y^2, \dots, y^{3^s-1}$ при помощи обратного ДПФ.
- (Г) Многочлен $f'(x)$ приводится по модулю $x^{3^r} - y$.

Для завершения доказательства остается показать, что заключительный шаг реализуется схемой сложности $(m-1)3^{r+s}$ и глубины $\lceil \log_2 m \rceil$. Рассмотрим $f'(x) = \sum \psi_i(x) x^{i3^r}$, где $\psi_i(x) \in R_s^{(y)}[x]$ и $\deg \psi_i < 3^r$. Отсюда $f'(x) \bmod (x^{3^r} - y) = \sum y^i \psi_i(x)$. Умножение на степени y в кольце $R_s^{(y)}$ осуществляется циклическим сдвигом коэффициентов. Остается просуммировать m многочленов над $R_s^{(y)}$ степени не выше $3^r - 1$, что, очевидно, может быть выполнено с заявленными оценками.

Следующее утверждение получается в результате применения нескольких итераций согласно доказанной лемме 4.

Лемма 5. Пусть $j \in \mathbf{N}$ и $m = 3^\mu$, $\mu \in \mathbf{N}$. Тогда

$$\begin{aligned} M'(m, \mu + v) &\leq m^j 3^{j+(1-2^{-j})v} M'(m, \mu + \lceil v/2^j \rceil) + O((\mu + v)3^{v+j}m^{j+2}), \\ D'_M(m, \mu + v) &< D'_M(m, \mu + \lceil v/2^j \rceil) + (4 + \log_2 3)(\mu + 1)j + v. \end{aligned}$$

Доказательство. Пусть $s_1 = \mu + \lceil v/2 \rceil$ и $r_1 = \lfloor v/2 \rfloor$. При этом $\mu + v = r_1 + s_1$, $m \leq 3^{s_1-r_1}$, и можно применять лемму 4. Ясно, что

$$\begin{aligned} M'(m, \mu + v) &\leq 3^{s_1} M'(m, s_1) + 2(m+1)s_1 3^{2s_1} + (m-1)3^{r_1+s_1}, \\ D'_M(m, \mu + v) &\leq D'_M(m, s_1) + 4s_1 + \lceil \log_2 m \rceil. \end{aligned}$$

Положим $s_1 = s_2 + r_2$, где $s_2 = \mu + \lceil (s_1 - \mu)/2 \rceil$, и далее $s_{i+1} = \mu + \lceil (s_i - \mu)/2 \rceil$. Легко проверяется, что $s_i = \mu + \lceil v/2^i \rceil$, откуда следуют неравенства

$$\begin{aligned} s_1 + \dots + s_j &\leq (\mu + 1)j + (v-1)(1-2^{-j}), \\ s_1 + \dots + s_{j-1} + 2s_j &\leq (j+1)(\mu + 1) + v - 1. \end{aligned} \quad (1)$$

Применяя j раз лемму 4, получаем неравенство

$$\begin{aligned} M'(m, \mu + v) &\leq 3^{s_1+\dots+s_j} M'(m, s_j) \\ &\quad + 2(m+1)(s_1 3^{2s_1} + s_2 3^{s_1+2s_2} + \dots + s_j 3^{s_1+\dots+s_{j-1}+2s_j}) \\ &\quad + (m-1)(3^{r_1+s_1} + 3^{2s_1} + \dots + 3^{s_1+\dots+s_{j-2}+2s_{j-1}}), \end{aligned}$$

откуда подстановкой оценок (1) получаем неравенства

$$\begin{aligned} M'(m, \mu + v) &\leq (3m)^j 3^{(1-2^{-j})v} M'(m, s_j) \\ &\quad + 2(m+1)3^v m \left((\mu + 1) \sum_{i=1}^j (3m)^i + (v-1) \sum_{i=1}^j (3m/2)^i \right) \\ &\quad + (m-1)m3^v (1 + 3m + \dots + (3m)^{j-1}) \\ &< (3m)^j 3^{(1-2^{-j})v} M'(m, s_j) \\ &\quad + 2(m+1)3^{v+1} m^2 (3m)^j \left(\frac{\mu + 1}{3m - 1} + \frac{v - 1}{(3m - 2)2^j} \right) \\ &\quad + (m-1)m3^v \frac{(3m)^j}{3m - 1}, \end{aligned}$$

где последний переход состоит в применении формул для суммы геометрической прогрессии. Очевидно, что выражение в нижней строчке имеет порядок $O((\mu + v)3^{v+j}m^{j+2})$, откуда следует утверждение, касающееся сложности. Для глубины справедлива оценка

$$D'_M(m, k) \leq D'_M(m, s_j) + 4(s_1 + \dots + s_j) + j \lceil \log_2 m \rceil,$$

которая, с учетом (1), приводится к оценке в утверждении леммы.

3.2. О применении ДПФ (нечетная характеристика)

Умножение в поле нечетной характеристики может выполняться в известной степени более простым алгоритмом, основанным на двоичном, а не на троичном преобразовании Фурье (см. [15]). Опишем аналогичный алгоритму предыдущего раздела метод многократного умножения над полем $GF(p)$.

Рассмотрим кольцо $R_s^{(x)} = GF(p)[x]/(x^{2^s} + 1)$ многочленов над $GF(p)$ по модулю $x^{2^s} + 1$. Элемент x является примитивным корнем степени 2^{s+1} из единицы в силу взаимной простоты многочленов $x^{2^s} + 1$ и $x^{2^s} - 1$. Таким образом, в кольце $R_s^{(x)}$ определено ДПФ порядка 2^{s+1} . Для обратного преобразования требуется разложение по степеням x^{-1} , которое получается изменением порядка следования коэффициентов и умножением их на -1 , так как

$$c_0 + \sum_{i=1}^{2^s-1} c_i x^i \equiv c_0 - \sum_{i=1}^{2^s-1} c_{2^s-i} (x^{-1})^i \pmod{x^{2^s} + 1},$$

при этом умножение на -1 можно совместить с умножением на $N^{-1} = 2^{-(s+1)} \pmod{p}$ в конце алгоритма. Заметим, что в случае характеристики три схемную сложность обратного ДПФ можно принять совпадающей со сложностью прямого ДПФ, поскольку сложность умножения на -1 в поле $GF(3)$ можно полагать равной 0 (если элементы $GF(3)$ записываются в двухбитовом двоичном коде $1 = [01]$, $2 = [10]$, $0 = [00]$ или $[11]$, то умножение на -1 осуществляется перестановкой разрядов).

Пусть $m(n-1) < 2^s$, тогда от m -кратного умножения многочленов над $GF(p)$ степени $n-1$ можно перейти к m -кратному умножению в $R_s^{(x)}$. Как и ранее, через $M'(m, s)$ и $D'_M(m, s)$ обозначим соответственно сложность и глубину m -кратного умножения в кольце $R_s^{(x)}$, а через $\Phi(s, r)$ и $D_\Phi(s, r)$ — сложность и глубину ДПФ порядка 2^r над $R_s^{(x)}$, $r \leq s+1$. При этом обратное ДПФ выполняется со сложностью $\Phi(s, r) + 2^s$ и глубиной $D_\Phi(s, r) + 1$.

Лемма 6. Пусть $r \leq s$. Тогда ДПФ порядка 2^r над $R_s^{(y)}$ реализуется схемой сложности и глубины

$$\Phi(s, r) \leq r2^{r+s}, \quad D_\Phi(s, r) \leq r.$$

Доказательство. Пусть $z = y^{2^{s-r+1}}$ — корень из единицы степени 2^r в $R_s^{(y)}$, и пусть $\Gamma(x) = \sum \gamma_i x^i$ — многочлен над $R_s^{(y)}$ степени $2^r - 1$. Рассмотрим

$$\Gamma(z^l) = \sum_{i=0}^{2^r-1} \gamma_i z^{il} = \sum_{i=0}^{2^{r-1}-1} \gamma_{2i} (z^2)^{il} + z^l \sum_{i=0}^{2^{r-1}-1} \gamma_{2i+1} (z^2)^{il} = \Gamma_0(z_*^{l_1}) + z^l \Gamma_1(z_*^{l_1}),$$

где $z_* = z^2$ — корень степени 2^{r-1} из единицы, $l_1 = l \pmod{2^{r-1}}$, а

$$\Gamma_j(x) = \sum_{i=0}^{2^{r-1}-1} \gamma_{2i+j} x^i, \quad j = 0, 1.$$

Пусть необходимые значения $\Gamma_j(z_*^i)$, $j = 0, 1$, $i = 0, 1, \dots, 2^{r-1} - 1$, найдены при помощи двух ДПФ порядка 2^{r-1} . Умножения на степени z не требуют вычислительных затрат, поэтому для вычисления каждого из 2^r значений $\Gamma(z^l)$ остается выполнить сложение в $R_s^{(y)}$ со сложностью 2^s и глубиной 1. Справедливы рекуррентные неравенства

$$\Phi(s, r) \leq 2^{s+r} + 2\Phi(s, r-1), \quad D_\Phi(s, r) \leq 1 + D_\Phi(s, r-1),$$

которые, с учетом $\Phi(s, 0) = D_\Phi(s, 0) = 0$, приводят к неравенствам

$$\Phi(s, r) \leq r2^{s+r}, \quad D_\Phi(s, r) \leq r.$$

Лемма 7. Пусть $m \leq 2^{s-r+1}$, тогда

$$\begin{aligned} M'(m, r+s) &\leq 2^{s+1}M'(m, s) + (m+1)(s+1)2^{2s+1} + m2^{r+s}, \\ D'_M(m, r+s) &\leq D'_M(m, s) + 2s + 3 + \lceil \log_2 m \rceil. \end{aligned}$$

Доказательство. Пусть $f_i \in R_{r+s}^{(x)}$ и $f = f_1 \dots f_m$. Как и в лемме 4, используем представление

$$f_i = \sum_{j=0}^{2^{r+s}-1} f_{i,j} x^j = \sum_{j=0}^{2^r-1} \varphi_{i,j}(\tilde{y}) x^j,$$

где $\tilde{y} = x^{2^r}$ и $\deg \varphi_{i,j} < 2^s$, и устанавливаем соответствие между $R_{r+s}^{(x)}$ и $R_s^{(y)}[x]$. Таким образом, обозначая через $f'_i(x)$ многочлены из $R_s^{(y)}[x]$, соответствующие f_i , и полагая $f'(x) = f'_1(x) \dots f'_m(x) \in R_s^{(y)}[x]$, получаем соответствие между $f \in R_{r+s}^{(x)}$ и $f'(x) \bmod (x^{2^r} - y)$.

Многочлен $f'(x)$ степени не выше $m(2^r - 1)$ однозначно восстанавливается по значениям в $2^{s+1} \geq m2^r$ точках. Рассмотрим следующий алгоритм m -кратного умножения в $R_{r+s}^{(x)}$.

- (А) Вычислим значения $f'_i(x)$ в точках $1, y, y^2, \dots, y^{2^{s+1}-1}$, где y — примитивный корень степени 2^{s+1} в $R_s^{(y)}$, с помощью ДПФ.
- (Б) Произведения $f'(y^j) = f'_1(y^j) \dots f'_m(y^j)$ вычисляются посредством 2^{s+1} m -кратных умножений в $R_s^{(y)}$.
- (В) Многочлен $f'(x)$ восстанавливается по значениям в точках $1, y, y^2, \dots, y^{2^{s+1}-1}$ при помощи обратного ДПФ.
- (Г) Многочлен $f'(x)$ приводится по модулю $x^{2^r} - y$.

Приведение по модулю на последнем шаге сводится к сложению (с вычитаниями) m многочленов над $R_s^{(y)}$ степени не выше $2^r - 1$ (так как умножение на степени y в $R_s^{(y)}$ является циклическим сдвигом со сменой знака у некоторых коэффициентов).

Лемма 8. Пусть $j \in \mathbb{N}$ и $m = 2^\mu$, $\mu \in \mathbb{N}$. Тогда

$$\begin{aligned} M'(m, \mu + v) &\leq m^j 2^{j+(1-2^{-j})v} M'(m, \mu + \lfloor v/2^j \rfloor) + O((\mu + v)2^{v+j} m^{j+2}), \\ D'_M(m, \mu + v) &\leq D'_M(m, \mu + \lfloor v/2^j \rfloor) + 3(\mu + 1)j + 2v. \end{aligned}$$

Доказательство. Выберем $s_1 = \mu + \lfloor v/2 \rfloor$ и $r_1 = \lceil v/2 \rceil$, и применим лемму 7. Получаем, что

$$\begin{aligned} M'(m, \mu + v) &\leq 2^{s_1+1} M'(m, s_1) + (m+1)(s_1+1)2^{2s_1+1} + m2^{r_1+s_1}, \\ D'_M(m, \mu + v) &\leq D'_M(m, s_1) + 2s_1 + 3 + \mu. \end{aligned}$$

Далее, пусть $s_1 = s_2 + r_2$, где $s_2 = \mu + \lfloor (s_1 - \mu)/2 \rfloor$, и $s_i = \mu + \lfloor (s_{i-1} - \mu)/2 \rfloor$. Очевидно, что $s_i = \mu + \lfloor v/2^i \rfloor$. Применяя j раз лемму 7, получаем, что

$$M'(m, \mu + v) \leq 2^{s_1 + \dots + s_j + j} M'(m, s_j) + (m + 1) \left(\sum_{i=1}^j (s_i + 1) 2^{s_1 + \dots + s_{i-1} + 2s_i + i} \right) + m(2^{\mu+v} + 2^{2s_1+1} + \dots + 2^{s_1 + \dots + s_{j-2} + 2s_{j-1} + j-1}).$$

Учитывая неравенства

$$s_1 + \dots + s_i \leq i\mu + v(1 - 2^{-i}), \quad s_1 + \dots + s_{i-1} + 2s_i \leq (i + 1)\mu + v,$$

получаем, что

$$\begin{aligned} M'(m, \mu + v) &\leq (2m)^j 2^{v(1-2^{-j})} M'(m, s_j) \\ &\quad + m(m + 1)2^v (s_1(2m) + s_2(2m)^2 + \dots + s_j(2m)^j) \\ &\quad + (2m + 1)m2^v (1 + 2m + \dots + (2m)^j) \\ &< (2m)^j 2^{v(1-2^{-j})} M'(m, s_j) \\ &\quad + m(m + 1)2^v \left(\frac{\mu(2m)^{j+1}}{2m - 1} + \frac{vm^{j+1}}{m - 1} \right) \\ &\quad + 2^v(2m + 1)(2m)^{j+1} \frac{m}{2m - 1}, \end{aligned}$$

откуда следует оценка сложности. Для глубины справедлива оценка

$$\begin{aligned} D'_M(m, \mu + v) &\leq D'_M(m, s_j) + 2(s_1 + \dots + s_j) + 3j + j\mu \\ &\leq D'_M(m, s_j) + 3(\mu + 1)j + 2v. \end{aligned}$$

3.3. Схема логарифмической глубины

Здесь будет указан способ построения схемы m -кратного умножения многочленов степени n над полем $GF(p)$, имеющей при $p = (mn)^{O(1)}$ сложность $M(m, n) = O(pm^3n^2)$ и глубину $D_M(m, n) = O(\log(mn))$. Алгоритм основан на следующих известных фактах.

Лемма 9. *Линейное отображение из $GF(p^n)$ в $GF(p^m)$ реализуется схемой сложности $O(mn/\log_p m)$ и глубины $O(\log n)$.*

Лемма 10. *Произвольная функция n переменных над $GF(p)$ реализуется схемой сложности $O(p^n/n)$ и глубины $O(n)$.*

Лемма 11. *Сумматор m n -разрядных p -ичных чисел реализуется схемой сложности $O(mn)$ и глубины $O(\log(mn))$.*

Лемма 12. *Экспоненцирование в $GF(p^n)$, то есть возведение фиксированного элемента $\alpha \in GF(p^n)$ в переменную степень, записываемую m разрядами над $GF(p)$, выполняется схемой сложности $O(m(M(n) + pn))$ и глубины $O(\log p + D_M(n) \log m)$.*

Первые две леммы являются обобщениями на схемы над $GF(p)$ методов О. Б. Лупанова асимптотически оптимального синтеза схем для линейных отображений и для

произвольных функций (см. [3, 22]). Следующая лемма является аналогичным обобщением метода Ю. П. Оффмана [23] сведения m -кратного суммирования к обычному сложению двух чисел, для сложения которых можно воспользоваться, например, p -ичным вариантом метода В. М. Храпченко [24]. Последняя лемма вытекает из стандартного способа экспоненцирования, основанного на предвычислении всех элементов α^{ip^j} , $i = 0, 1, \dots, p-1$, $j = 0, 1, \dots, n-1$.

Теорема 1. Пусть $p = (mn)^{O(1)}$. Тогда можно построить схему m -кратного умножения многочленов степени n над $GF(p)$ сложности и глубины

$$M(m, n) = O(pm^3n^2), \quad D_M(m, n) = O(\log(mn)).$$

Доказательство. Пусть $f(x) = f_1(x) \dots f_m(x)$. Положим $L = mn + 1$ и $k = \lceil \log_p L \rceil$. В поле $GF(p^k)$ зафиксируем набор элементов $\alpha_1, \dots, \alpha_L$. Рассмотрим следующий алгоритм, в основе которого лежат идея интерполяции, восходящая к А. Л. Тоому [25], и идея дискретного логарифмирования из работы Эберли [19].

- (1) Вычислим всевозможные $f_i(\alpha_j) \in GF(p^k)$, где $i = 1, \dots, m$, $j = 1, \dots, L$.
- (2) Для каждого j вычислим произведение $f_1(\alpha_j) \dots f_m(\alpha_j) = f(\alpha_j)$. Для этого в поле $GF(p^k)$ выберем примитивный элемент α . Если $f_i(\alpha_j) \neq 0$ для всех i , то
 - (2.1) вычислим дискретные логарифмы, $\log_\alpha f_i(\alpha_j)$,
 - (2.2) вычислим $l_j = \sum_{i=1}^m \log_\alpha f_i(\alpha_j)$,
 - (2.3) вычислим $f(\alpha_j) = \alpha^{l_j}$ (корректность этой формулы следует из справедливости сравнения $l_j \equiv \log_\alpha f(\alpha_j) \pmod{p^k - 1}$).
- (3) По значениям $f(\alpha_j)$, $j = 1, \dots, L$, восстанавливается многочлен $f(t)$ степени не выше $L - 1$.

Поскольку элементы α_i фиксированы, первый и последний шаги алгоритма состоят в выполнении линейных преобразований размерности $mLk \times mn$ и $L \times Lk$. По лемме 9, шаг 1 реализуется со сложностью $O(m^2Lnk / \log_p(mLk)) = O(m^3n^2)$ и глубиной $O(\log(mn))$, а шаг 3 — со сложностью $O(L^2k / \log_p L) = O(m^2n^2)$ и глубиной $O(\log(mn))$.

Рассмотрим шаг 2. Корректирующие подсхемы (вычисляющие, есть ли нули среди сомножителей и обнуляющие результат в таком случае) реализуются со сложностью $O(Lmk) = O(m^2n \log_p(mn))$ и увеличивают глубину реализации шага не более, чем на 1 относительно схемы, предполагающей, что все сомножители отличны от нуля.

На этом шаге вычисляется Lm дискретных логарифмов, L штук m -кратных сумм k -разрядных чисел и L степеней элемента α .

Схему для дискретного логарифма (с k входами и k выходами) можно построить методом леммы 10 со сложностью $O(p^k) = O(pmn)$ и глубиной $O(k) = O(\log_p(mn))$. Следовательно, сложность шага 2.1 есть $O(Lm^2n) = O(m^3n^2)$.

Лемма 11 позволяет построить схему для m -кратного суммирования k -разрядных чисел со сложностью $O(mk)$ и глубиной $O(\log(mk)) = O(\log(mn))$, следовательно, сложность шага 2.2 оценивается как $O(Lmk) = O(m^2n \log_p(mn))$.

Показатели l_j состоят не более чем из $k + \lceil \log_p m \rceil = O(k)$ разрядов. Поэтому согласно лемме 12 для возведения элемента α в степень l_j строится схема сложности $O(kM(k) + pk^2) = O(p \log_p^3(mn))$ и глубины $O(\log p + D_M(k) \log k) = O(\log(mn))$. Следовательно, сложность шага 2.3 оценивается как $O(Lp \log_p^3(mn)) = O(pmn \log_p^3(mn))$.

Суммируя оценки для всех подсхем, получаем утверждение теоремы.

Заметим, что если требуется выполнить многократное умножение с приведением по модулю некоторого фиксированного многочлена, то для этой операции также справедливы оценки теоремы 1, так как приведение по модулю (которое является линейной операцией) в композиции с линейным преобразованием, выполняемым на шаге 3, не приводит к увеличению размерности совокупного преобразования.

Более точные оценки построенной схемы в случае характеристики 2 можно получить, используя результаты из [18].

Теорема 2. Пусть $p = (mn)^{O(1)}$ и $j \in \mathbb{N}$. Тогда m -кратное умножение многочленов степени не выше $n - 1$ над $GF(p)$ выполняется схемой сложности и глубины

$$M(m, n) = O(pa^j m^{5+j} n^{1+2^{-j}}), \quad D_M(m, n) = O(\log(m^j n)),$$

где $a = 3$ при $p = 2$ и $a = 2$ в остальных случаях.

Доказательство. При помощи лемм 5 и 8 сложность многократного умножения над $GF(p)$ оценивается как (для упрощения вида формул далее будем пренебрегать округлением некоторых параметров)

$$\begin{aligned} M(m, n) &\leq M'(m, \log_a(mn)) \\ &\leq (am)^j n^{1-2^{-j}} M'(m, \log_a(mn^{2^{-j}})) + O(\log(mn) a^j n m^{j+2}), \end{aligned}$$

где $j \in \mathbb{N}$. Подставляя оценку теоремы 1, получаем, что

$$M(m, n) = O(pa^j m^{5+j} n^{1+2^{-j}}).$$

При этом глубина оценивается как

$$\begin{aligned} D_M(m, n) &\leq D'_M(m, \log_a(mn)) \\ &\leq D'_M(m, \log_a(mn^{2^{-j}})) + O(\log(m^j n)) = O(\log(m^j n)). \end{aligned}$$

3.4. О применении метода Д. Кантора

Концепция аддитивных подгрупп конечного поля и основанного на них аддитивного аналога дискретного преобразования Фурье, позволяющего построить асимптотически быстрый метод умножения многочленов над конечными полями, была предложена Д. Кантором в [26]. Впоследствии, в [27], метод Кантора был обобщен на более широкий класс полей, и одновременно упрощено изложение. Приведем необходимые сведения о применении аддитивного преобразования Фурье, опираясь на [27].

Пусть в поле $GF(p^k)$ выбран базис $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$. Положим $W_0 = \{0\}$, и пусть $W_i = \langle \alpha_1, \dots, \alpha_i \rangle$ — линейное подпространство поля $GF(p^k)$, то есть W_i является аддитивной подгруппой. Очевидно, что для $i < k$ выполняется равенство

$$W_{i+1} = \bigcup_{c \in GF(p)} \{c\alpha_{i+1} + W_i\}.$$

Определим многочлены $S_i(x)$, полагая

$$S_i(x) = \prod_{\beta \in W_i} (x - \beta).$$

Многочлены $S_i(x)$ обладают следующими легко проверяемыми свойствами (см. [27]):

- (1) $S_0(x) \mid S_1(x) \mid \dots \mid S_k(x) = x^{p^k} - x$,
- (2) $S_{i+1}(x) = S_i(x)(S_i^{p-1}(x) - S_i^{p-1}(\alpha_{i+1}))$,
- (3) многочлен $S_i(x)$ может содержать ненулевые коэффициенты только при степенях x^{p^j} , $0 \leq j \leq i$,
- (4) $S_i(\beta + \gamma) = S_i(\beta) + S_i(\gamma)$ для любых $\beta, \gamma \in GF(p^k)$.

Указанные свойства позволяют сформулировать аддитивный аналог алгоритма быстрого дискретного преобразования Фурье. Обозначим через n_i число ненулевых коэффициентов многочлена $S_i(x)$. Из свойства 3 следует, что $n_i \leq i + 1$. Нам также потребуется следующая лемма.

Лемма 13. Пусть $\alpha \in GF(p^k)$, $g(x) \in GF(p^k)[x]$ и $\deg g \leq p^{i+1} - 1$. Для любого $c \in GF(p)$ введем обозначение $g_c(x) = g(x) \bmod S_i(x - c\alpha_{i+1} - \alpha)$. Тогда

- (а) для всех $\beta \in \alpha + W_i$ справедливы равенства $g(\beta + c\alpha_{i+1}) = g_c(\beta + c\alpha_{i+1})$,
- (б) $g(x) = -S_i^{1-p}(\alpha_{i+1}) \sum_{c \in GF(p)} g_c(x) S_{i+1}(x - \alpha) / S_i(x - c\alpha_{i+1} - \alpha)$, а для поля характеристики 2 $g(x) = S_i^{-1}(\alpha_{i+1})(g_0(x) S_i(x - \alpha_{i+1} - \alpha) + g_1(x) S_i(x - \alpha))$,
- (в) если известен многочлен $g(x)$, то многочлены $g_c(x)$ вычисляются со сложностью $O(n_i p^{i+2} M(k))$ и глубиной $O(p(D_M(k) + \log n_i))$,
- (г) если известны многочлены $g_c(x)$, то многочлен $g(x)$ вычисляется со сложностью $O(n_i p^{i+1} M(k))$ и глубиной $O(p(D_M(k) + \log n_i))$.

Доказательство. Утверждение (а) очевидно. Равенство (б) многочленов степени не выше $p^{i+1} - 1$ следует из совпадения их значений в p^{i+1} точках $\beta \in \alpha + W_{i+1}$.

Многочлен $S_i(x)$ является n_i -членом степени p^i со следующим после старшего ненулевым коэффициентом при x^{p^j} , где $j \leq i - 1$. Многочлен вида $S_i(x - \beta)$ отличается от $S_i(x)$ постоянным членом $S_i(\beta)$. Приведение по модулю такого многочлена (или умножение на него) можно свести к вычитаниям (сложениям).

Алгоритм приведения многочлена $g(x)$ по модулю $S_i(x - \beta)$ состоит в последовательных приведениях по модулям $S_i(x - \beta)x^{j(p^i - p^{i-1})}$, $j = p - 1, \dots, 1$. Каждое из приведений требует $O(p^i n_i)$ умножений на коэффициенты многочлена $S_i(x - \beta)$ и $O(p^i n_i)$ сложений над $GF(p^k)$ (для приведения подобных). Эти сложения выполняются с глубиной $O(\log n_i)$, так как при каждой степени x образуется $O(n_i)$ подобных членов. Окончательно, одно приведение по модулю $S_i(x - \beta)$ выполняется со сложностью $O(n_i p^{i+1} M(k))$ и глубиной $O(p(D_M(k) + \log n_i))$, что доказывает (в).

Умножение $g_c(x)$ на многочлен $-S_i^{1-p}(\alpha_{i+1})S_{i+1}(x - \alpha)$, имеющий $n_{i+1} + 1$ ненулевых коэффициентов, требует $O(p^i n_{i+1})$ умножений и $O(p^i n_{i+1})$ сложений в $GF(p^k)$. Сложения выполняются с глубиной $O(\log n_{i+1})$, так как при каждой степени x имеется $O(n_{i+1})$ подобных членов. Последующее деление на многочлен $S_i(x - c\alpha_{i+1} - \alpha)$ выполняется алгоритмом предыдущего абзаца с тем отличием, что находится не остаток, а частное от деления; также, за счет того, что исходный многочлен может иметь степень $p^{i+1} + p^i - 1$, требуется, вообще говоря, не $p - 1$, а p промежуточных операций приведения по модулю. После вычисления всех многочленов-слагаемых в формуле (б), как указано выше, остается выполнить сложение p многочленов степени не выше $p^{i+1} - 1$, откуда, учитывая $n_{i+1} \leq 2n_i$, получаем (г).

Лемма 14. Вычисление всех $g(\beta)$, $\beta \in \alpha + W_l$, $g \in GF(p^k)[x]$, $\deg g \leq p^l - 1$, $\alpha \in GF(p^k)$, выполняется схемой сложности $O(l^2 p^{l+1} M(k))$ и глубины $O(pl(D_M(k) + \log l))$.

С такой же сложностью и глубиной восстанавливается единственный многочлен $g(x)$ степени не выше $p^l - 1$, принимающий заданные значения на множестве $\alpha + W_l$.

Доказательство. Воспользуемся индукцией. Для $l = 0$ утверждение леммы очевидно. Пусть оно справедливо для всех $l \leq L - 1$. Рассмотрим переход к $l = L$.

Согласно утверждению (а) леммы 13, вычисление всех значений многочлена $g(x)$ степени, не превосходящей $p^L - 1$, на множестве $\alpha + W_L$ равносильно вычислению значений многочленов $g_c(x)$ степени, не превосходящей $p^{L-1} - 1$, на соответствующих множествах $\alpha + c\alpha_L + W_{L-1}$, где $c \in GF(p)$. Из утверждения (в) следует, что многочлены $g_c(x)$ вычисляются со сложностью $O(n_{L-1} p^{L+1} M(k))$ и глубиной $O(p(D_M(k) + \log n_i))$. По предположению индукции, вычисление значений многочленов g_c на соответствующих подмножествах выполняется схемой сложности $O(p^{L+1} M(k)) \sum_{i=0}^{L-2} n_i$ и глубины $O(p(L-1)D_M(k)) + O(p) \sum_{i=0}^{L-2} \log n_i$. Суммируя указанные оценки и замечая, что из $n_i \leq i + 1$ следуют оценки

$$\sum_{i=0}^{l-1} n_i \leq \binom{l}{2}, \quad \sum_{i=0}^{l-1} \log n_i \leq \log l! = O(l \log l),$$

получаем первое утверждение леммы. Второе утверждение доказывается абсолютно аналогично.

Замечание 1. Вычисление значений многочлена степени $n < p^l - 1$ на множестве W_l методом леммы 14 выполняется схемой сложности $O(p^{l+1} M(k) \log_p^2 n)$ и глубины $O(p \log_p n(D_M(k) + \log \log_p n))$, так как нет необходимости вычислять остатки от деления на $S_i(x - \beta)$, если $p^i \leq n$.

Теорема 3. Пусть $p = O(mn)$. Тогда умножение m многочленов степени не выше $n - 1$ над $GF(p)$ выполняется схемой сложности и глубины

$$M(m, n) = O(m^2 p^2 n M(\log_p(mn)) \log_p^2 n),$$

$$D_M(m, n) = O(p \log_p(mn)(D_M(\log_p(mn)) + \log \log_p(mn))).$$

Доказательство. Пусть перемножаются многочлены $f_1(x), \dots, f_m(x) \in GF(p)[x]$ степени не выше $n - 1$. Выберем $k = \lceil \log_p(m(n-1) + 1) \rceil$, так что любой многочлен степени $m(n-1)$ может быть восстановлен по своим значениям в поле $GF(h^k)$. Пусть $f_i(x) \in GF(p^k)[x]$ и $f(x) = f_1(x) \dots f_m(x)$. Рассмотрим следующую схему вычислений.

- (А) Вычисляются значения всех многочленов $f_i(x)$ в точках поля $GF(p^k)$.
- (Б) Вычисляются значения $f(x)$ над полем $GF(xp^k)$ непосредственным перемножением значений многочленов сомножителей.
- (В) Многочлен $f(x)$ восстанавливается по известным значениям.

Согласно замечанию 1, шаг А реализуется схемой сложности $O(mp^{k+1} M(k) \log_p^2 n)$ и глубины $O(p \log_p n(D_M(k) + \log \log_p n))$. Шаг Б заключается в выполнении p^k операций m -кратного умножения в $GF(p^k)$ и имеет сложность $O(p^k m M(k))$ и глубину

$O(n(D_M(k) \log m))$. Шаг В, согласно лемме 14, может быть выполнен схемой сложности $O(k^2 p^{k+1} M(k))$ и глубины $O(pk(D_M(k) + \log k))$. В оценке сложности доминирует сложность реализации шага А, а в оценке глубины — глубина реализации шага В, откуда, учитывая, что $p^k < pmn$, получаем окончательный результат.

Оценки сложности и глубины в доказанной теореме могут быть уточнены при специальном выборе базиса (см. [26]). Например, при $p = 2$ они могут быть приведены к виду $O(m^2 n \log^{\log_2 6}(mn))$ и $O(\log(mn) \log \log(mn))$ соответственно.

4. Схемы для инвертирования

Теорема 4. Пусть $r \in \mathbb{N}$ и $p = n^{O(1)}$. Тогда для сложности и глубины инвертирования в стандартном базисе поля $GF(p^n)$ справедливы оценки

$$I(n) = O(rn^{w+1/r} + O(rpn^{3/2+6/r})), \quad D_I(n) = O(r \log n),$$

где $w < 1,667$.

Доказательство. В силу замечания из раздела 2, инвертирование с точностью до $O(n)$ выполняемых с глубиной $O(\log n)$ операций соответствует операции возведения в степень $(p^n - p)/(p - 1)$.

Согласно лемме 1, для этой операции справедливы оценки глубины и сложности

$$\begin{aligned} I(n) &= O(rE(n, m)) + O(rn \log n \log \log n), \\ D_I(n) &= O(rD_E(n, m)) + O(r \log n), \end{aligned}$$

где $m = O(n^{1/r})$. Далее, согласно разделу 2.1,

$$\begin{aligned} E(n, m) &\leq nS(n) + M(m, n) + O(mM(n)), \\ D_E(n, m) &\leq D_S(n) + D_M(m, n) + O(\log n). \end{aligned}$$

Подставляя оценки из леммы 2 и теоремы 2, в которых $j = 1$, получаем, что

$$E(n, m) = O(mn^w) + O(pm^6 n^{3/2}), \quad D_E(n, M) = O(\log n),$$

откуда следует утверждение теоремы.

Из доказанной теоремы, в частности, следует, что, выбирая параметр r^{-1} в пределах погрешности округления экспоненты матричного умножения из [12] равным 1,667, при ограничениях $p = O(n^{1/6})$ можно построить схему инвертирования сложности $O(n^{1,667})$ и глубины $O(\log n)$.

4.1. Инвертирование в базисах с низкой транзитивной сложностью

Основная асимптотическая сложность построенной в предыдущем разделе схемы инвертирования в стандартном базисе содержится в подсхеме, выполняющей операции Фробениуса. Однако эти операции выполняются “бесплатно” в схемной реализации, если вычисления производятся в нормальном базисе. Таким образом, для стандартного базиса, допускающего сравнительно несложный переход к нормальному базису и обратно (под переходом подразумевается преобразование координат элемента поля), оценка теоремы 4 может быть улучшена.

Идея об использовании перехода между двумя типами базисов для ускорения выполнения некоторых операций была явно высказана в работах [14, 28]. Если нормальный базис выгодно использовать для реализации операций Фробениуса, то умножение лучше выполнять в стандартном базисе. Алгоритм умножения Мессе–Омура (см. [29] или, например, 2.1.1.3 в [8]), разработанный для нормальных базисов, имеет оценку сложности $O(n^2)$ даже для оптимальных нормальных базисов и $O(n^3)$ в общем случае. В то же время, верхняя оценка сложности перехода между базисами в произвольном поле есть $O(n^{1.806})$ (см. [13]). Умножение в стандартном базисе может выполняться методом Шёнхаге со сложностью $O(n \log n \log \log n)$. Реально в полях, имеющих прикладное значение, когда n имеет порядок нескольких десятков или сотен, используется метод А. А. Карацубы [23] сложности $O(n^{\log_2 3})$.

Следуя [14], транзитивной сложностью стандартного (нормального) базиса поля $GF(q^n)$ назовем сумму сложностей схем прямого и обратного перехода к нормальному (стандартному) базису. Уточним, что здесь не требуется, чтобы оба базиса порождались одним и тем же элементом. Генератор стандартного базиса, вообще говоря, не всегда является одновременно и генератором нормального базиса. Транзитивную сложность будем обозначать через $T(n)$. Через $D_T(n)$ обозначим сумму глубин соответствующих схем.

Таким образом, справедливы очевидные оценки

$$S(n) \leq T(n), \quad D_S(n) \leq D_T(n).$$

Теорема 5. Пусть $r \in \mathbb{N}$ и $p = n^{O(1)}$. Тогда для инвертирования в стандартном или нормальном базисе поля $GF(p^n)$ можно построить схему сложности и глубины

$$\begin{aligned} I(n) &= O(pr^b n^{1+(\log_2 r + 6,2)/r}) + O(rn^{1/r} T(n)), \\ D_I(n) &= O(r \log n) + O(r D_T(n)), \end{aligned}$$

где $b = \log_2 6$ для $p = 2$ и $b = 2$ для $p > 2$.

Кроме того, при $p < n$ можно построить схему сложности и глубины

$$\begin{aligned} I(n) &= O(p^3 n^{1+2/(p \log_p \log_p n)} \log_p^4 n \log_p \log_p n) + O(pn^{1/(p \log_p \log_p n)} T(n) \log_p \log_p n), \\ D_I(n) &= O(p \log_p \log_p n (\log n + D_T(n))). \end{aligned}$$

Доказательство. Используем следующую стратегию: операции Фробениуса реализуем в нормальном базисе, а остальные — в стандартном, выполняя переходы между базисами при необходимости.

В этом случае

$$\begin{aligned} E(n, m) &\leq mT(n) + V(m, n) + O(mM(n)), \\ D_E(n, m) &\leq D_T(n) + D_M(m, n) + O(\log n). \end{aligned}$$

Для $m = O(n^{1/r})$ из теоремы 2 получаем, что

$$M(m, n) = O(pa^j n^{1+(5+j)/r+2^{-j}}), \quad D_M(m, n) = O((1+j/r) \log n),$$

где $a \in \{2, 3\}$ и $j \in \mathbb{N}$. Для того, чтобы минимизировать показатель $j/r + 2^{-j}$, положим $j = \lceil \log_2 r + \log_2 \ln 2 \rceil$, при этом выполняется неравенство $j/r + 2^{-j} < (\log_2 r + 1,2)/r$. При $p = 2$ оценка сложности принимает вид $O(r^{\log_2 3} n^{1+(\log_2 r + 6,2)/r})$, а при нечетных p сложность оценивается как $O(prn^{1+(\log_2 r + 6,2)/r})$. Глубина равна $O(\log n)$ в обоих случаях. Отсюда следует первое утверждение теоремы.

Второе утверждение теоремы следует из выбора параметра схемы инвертирования $r = \lceil p \log_p \log_p n \rceil$ (тогда $m = O(n^{1/(p \log_p \log_p n)})$) и результата теоремы 3

$$M(m, n) = O(m^2 p^2 n M(\log_p n) \log_p^2 n),$$

$$D_M(m, n) = O(p \log_p n (D_M(\log_p n) + \log \log_p n)),$$

в которую для упрощения вида формул подставлены оценки сложности и глубины умножения в поле $GF(p^k)$ в виде $M(k) + O(k^2)$ и $D_M(k) = O(\log k)$.

Из доказанной теоремы вытекает, что в базисах с почти линейной транзитивной сложностью инвертирование также выполняется с почти линейной сложностью. При этом, если соответствующие переходы между базисами выполняются с глубиной $O(\log n)$, то построенная схема инвертирования также имеет глубину $O(\log n)$.

Отметим, что схема, построенная на базе умножения по методу Кантора, при $p = O(1)$ имеет глубину $O(\log n \log \log n)$, что также меньше стандартной оценки $O(\log^2 n)$.

5. Примеры базисов низкой сложности

5.1. Оптимальные нормальные базисы

Оптимальные нормальные базисы впервые были описаны в [30]. Понятие оптимального нормального базиса связано с понятием его сложности.

Под сложностью нормального базиса поля $GF(q^n)$ с генератором α понимается суммарное число ненулевых коэффициентов в базисном разложении элементов α^{1+2^i} , $i = 0, 1, \dots, n-1$. Это определение мотивируется тем, что сложность умножения в нормальном базисе стандартным алгоритмом Мессис–Омура фактически пропорциональна сложности данного базиса. Более подробное изложение можно найти в [8, 31].

Оптимальным называется базис минимально возможной сложности $2n-1$. Различают три типа оптимальных нормальных базисов (ОНБ), а теорема Гао–Ленстры (см. гл. 5 в [31]) утверждает, что других ОНБ не существует.

ОНБ I типа существуют в полях $GF(q^n)$, когда $n+1$ — простое число, а q — примитивный корень по модулю $n+1$. В качестве генераторов ОНБ может быть выбран какой-либо из примитивных корней степени $n+1$ из единицы в этом поле.

ОНБ II и III типа возникают, когда $q = 2^m$ и $(m, n) = 1$, число $2n+1$ простое, и либо 2 является примитивным корнем по модулю $2n+1$ (II тип), либо n нечетно, а примитивным корнем по модулю $2n+1$ является -2 (III тип). В качестве генератора выбирается элемент $\alpha = \zeta + \zeta^{-1}$, где ζ — примитивный корень степени $2n+1$ из единицы в поле $GF(q^{2n})$.

Умножение в ОНБ реализуется методом Мессис–Омура со сложностью $O(n^2)$. Однако, как следует из результатов работы [14], для выполнения умножения в ОНБ еще большее значение имеет то, что базисы обладают малой транзитивной сложностью. Более точно, для базисов I типа $T(n) = O(n)$, а для базисов II и III типов $T(n) = O(n \log n)$.

ОНБ I типа совпадает с базисом $\{\alpha, \alpha^2, \dots, \alpha^n\}$ с точностью до перестановки его элементов, и для перехода к стандартному базису (или обратно) остается выразить α^n (или 1) из соотношения $\alpha^n + \dots + 1 = 0$. В этом случае $T(n) = O(n)$ и $D_T(n) = O(\log n)$.

ОНБ II или III типа является перестановкой элементов $\{a_1, \dots, a_n\}$, где $a_i = \zeta_i + \zeta_i^{-1}$. Справедливо соотношение $a_k a_m = a_{k+m} + a_{k-m}$, из которого следует, что при любом i базисные подмножества $\{a_1, \dots, a_i\}$ и $\{\alpha, \dots, \alpha^i\}$ выражаются друг через друга (обозначим

сложность соответствующего преобразования координат через L_i). Пусть $2^k \leq n \leq 2^{k+1}$, тогда

$$x = \sum_{i=1}^n x_i a_i = a_{2^k} \sum_{i=1}^{n-2^k} x_{2^{k+1}+i} a_i + \sum_{i=1}^{2^k} (x_{2^{k+1}-i} + x_i) a_i,$$

где $x_j = 0$ при $j > n$. Учитывая соотношение $a_{2^k} = \alpha^{2^k}$, приходим к неравенству $L_n \leq L_{2^k} + L_{2^k} + L_{n-2^k} + n - 2^k$, откуда $L = O(n \log n)$, следовательно, $T(n) = O(n \log n)$ (а $D_T(n) = O(\log n)$) с учетом соотношения $m(\alpha) = 0$, позволяющего выражать α^n или 1 через остальные базисные элементы, где m — минимальный многочлен для α . Более подробное изложение можно найти в гл. 5 в [8] и в [14].

Таким образом, для сложности умножения в этих базисах справедлива оценка $O(n \log n \log \log n)$, а практически приемлемые схемы можно строить методом Карацубы.

Следовательно, для схемы инвертирования в ОНБ, построенной методом Брауэра, справедливы оценки сложности $O(n \log^2 n \log \log n)$ и глубины $O(\log^2 n)$. Кроме того, из теоремы 5 вытекает следующее утверждение.

Предложение 1. Пусть $p = n^{O(1)}$. Тогда для любого $\varepsilon > 0$ можно построить схему инвертирования в ОНБ поля $GF(p^n)$ со сложностью $O(\varepsilon^{-b} p n^{1+c\varepsilon|\log \varepsilon|})$ и глубиной $O(\varepsilon^{-1} \log n)$.

5.2. Гауссовы нормальные базисы

Оптимальные нормальные базисы являются частным случаем гауссовых нормальных базисов (ГНБ), которые впервые были рассмотрены в [14]. Заметим, что в этой работе рассматривались только поля характеристики 2, обобщение для произвольных полей появилось несколько позже.

ГНБ k -го типа существует в поле $GF(q^n)$, если $kn + 1$ — простое число, и порождается элементом $\alpha = \zeta + \zeta^\gamma + \dots + \zeta^{\gamma^{k-1}}$, где ζ — примитивный корень степени $kn + 1$ в поле $GF(q^{kn})$, а γ — примитивный корень степени k в поле вычетов $\mathbf{Z}_{kn+1} \setminus \{0\}$.

Известно, что сложность ГНБ k -го типа не превосходит $k(n + 1) - 1$ (см., например, 5.3 в [8]), а в некоторых частных случаях можно получить и лучшие оценки (см. гл. 3 в [31]).

Как показано в [33], для ускорения реализации операций в ГНБ можно использовать переход к стандартному (или почти стандартному) базису в поле $GF(q^{kn})$, расширении поля $GF(q^n)$. Действительно, элементы ГНБ являются суммами различных элементов базиса $\{\zeta, \zeta^2, \dots, \zeta^{kn}\}$ поля $GF(q^{kn})$ (см. [8]). Для перехода к стандартному базису $\{1, \zeta, \dots, \zeta^{kn-1}\}$ остается выразить ζ^{kn} из условия $1 + \zeta + \dots + \zeta^{kn} = 0$, что можно выполнить со сложностью $O(kn)$ и глубиной $\log(kn + O(1))$ (подробнее см. [8]).

Таким образом, $O(kn \log(kn) \log \log(kn))$ есть оценка сложности умножения в ГНБ. Для инвертирования справедливо следующее следствие теоремы 2 (с учетом того, что понятие транзитивной сложности распространяется на переход к базису в расширении исходного поля).

Предложение 2. Пусть $p = n^{O(1)}$ и $k = n^{O(1)}$. Тогда для любого $\varepsilon > 0$ можно построить схему инвертирования в ГНБ k -го типа поля $GF(p^n)$ сложности $O(\varepsilon^{-b} p n^{1+c\varepsilon|\log \varepsilon|})$ и глубины $O(\varepsilon^{-1} \log n)$.

В [34] предложено обобщение конструкции гауссовых нормальных базисов, которое имеет практическое значение (см. [35]). Такие базисы также допускают сравнительно

простой переход к стандартному базису в некотором расширении поля, но удовлетворительных теоретических оценок для схем перехода в общем случае, кажется, пока не получено.

Список литературы

1. Litov B., Davida G., $O(\log n)$ parallel time finite field inversion. *Lecture Notes Computer Sci.* (1988) **319**, 74–80.
2. Von zur Gathen J., Inversion in finite fields using logarithmic depth. *J. Symb. Comput.* (1990) **9**, 175–183.
3. Лупанов О. Б., *Асимптотические оценки сложности управляющих систем*. МГУ, Москва, 1984.
4. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А., *Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых*. КомКнига, Москва, 2006.
5. Bailey D., Paar C., Efficient arithmetic in finite extensions with application in elliptic curve cryptography. *J. Cryptology* (2001) **14**, 156–173.
6. Barreto P., Kim H., Lynn B., Scott M., Efficient algorithms for pairing-based cryptosystems. *Lecture Notes Computer Sci.* (2002) **2442**, 354–368.
7. Itoh T., Tsujii S., A fast algorithm for computing multivariate inverses in $GF(2^n)$ using normal basis. *Inform. Comput.* (1988) **78**, 171–177.
8. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А., *Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы*. КомКнига, Москва, 2006.
9. Кнут Д., *Искусство программирования*, **2**. Вильямс, Москва, 2004.
10. Гашков С. Б., Сергеев И. С., О применении метода аддитивных цепочек к инвертированию в конечных полях. *Дискретная математика* (2006) **18**, №4, 56–72.
11. Brent R., Kung H., Fast algorithms for manipulating formal power series. *J. ASM* (1978) **25**, 581–595.
12. Huang X., Pan V., Fast rectangular matrix multiplication and applications. *J. Complexity* (1998) **14**, 257–299.
13. Сергеев И. С., О построении схем для перехода между полиномиальными и нормальными базисами конечных полей. *Дискретная математика* (2007) **19**, №3, 89–102.
14. Болотов А. А., Гашков С. Б., О быстром умножении в нормальных базисах конечных полей. *Дискретная математика* (2001) **13**, №3, 3–31.
15. Von zur Gathen J., Gerland J., *Modern computer algebra*. Cambridge Univ. Press, Cambridge, 1999.
16. Schönhage A., Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf.* (1977) **7**, 395–398.
17. Beame P., Cook S., Hoover H., Log depth circuits for division and related problems. *SIAM J. Comput.* (1986) **15**, 994–1003.
18. Сергеев И. С., Об инвертировании в конечных полях характеристики 2 с логарифмической глубиной. *Вестник МГУ. Серия I. Математика. Механика* (2007) **62**, №5, 29–33.
19. Eberly W., Very fast parallel polynomial arithmetic. *SIAM J. Comput.* (1989) **18**, 955–976.
20. Cantor D., Kaltofen E., On fast multiplication of polynomials over arbitrary algebras. *Acta Inf.* (1991) **28**, 693–701.
21. Ноден П., Китте Л., *Алгебраическая алгоритмика*. Мир, Москва, 1999.

22. Лупанов О. Б., О вентильных и контактно-вентильных схемах. *Доклады АН СССР* (1956) **111**, 1171–1174.
23. Карацуба А. А., Офман Ю. П., Умножение многозначных чисел на автоматах. *Доклады АН СССР* (1962) **145**, 293–294.
24. Храпченко В. М., Об асимптотической оценке времени сложения параллельного сумматора. *Проблемы кибернетики* (1967) **19**, 107–120.
25. Тоом А. Л., О сложности схемы из функциональных элементов, реализующей умножение целых чисел. *Доклады АН СССР* (1963) **150**, 496–498.
26. Cantor D., On arithmetical algorithms over finite fields. *J. Comb. Theory* (1989) **A50**, 285–300.
27. Von zur Gathen J., Gerhard J., Arithmetic and factorization of polynomials over $\mathbf{F}_2$. In: *Proc. ISSAC'96*. ACM Press, New York, pp. 1–9.
28. Kaltofen E., Shoup V., Subquadratic-time factoring of polynomials over finite fields. *Math. Comput.* (1998) **67**, 1179–1197.
29. Massey J., Omura J., *Apparatus for finite fields computation*, US Patent Application, №457627, 1986.
30. Mullin R., Onyszchuk I., Vanstone S., Wilson R., Optimal normal bases in $GF(p^n)$. *Discrete Appl. Math.* (149–161) **22**,.
31. Jungnickel D., *Finite fields: structure and arithmetics*. Wissenschaftsverlag, Mannheim, 1995.
32. Ash D., Blake I., Vanstone S., Low complexity normal bases. *Discrete Appl. Math.* (1989) **25**, 191–210.
33. Gao S., von zur Gathen J., Panario D., Gauss periods and fast exponentiation in finite fields. *Lecture Notes Computer Sci.* (1995) **911**, 311–322.
34. Feisel S., von zur Gathen J., Shokrollahi M. A., Normal bases via general Gauss periods. *Math. Comput.* (1999) **68**, 271–290.
35. von zur Gathen J., Nöcker M., Fast arithmetic with general Gauss periods. *Theor. Comput. Sci.* (2004) **315**, 419–452.

Статья поступила 29.01.2007.