Math-Net.Ru

Общероссийский математический портал

С. Б. Гашков, И. С. Сергеев, О сложности и глубине булевых схем для умножения и инвертирования в конечных полях характеристики 2, *Дискрет. матем.*, 2013, том 25, выпуск 1, 3–32

DOI: <https://doi.org/10.4213/dm1218>

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: 3.89.197.203

26 апреля 2023 г., 12:01:26

О сложности и глубине булевых схем для умножения и инвертирования в конечных полях характеристики 2

© 2013 г. С. Б. Гашков, И. С. Сергеев

Для сложности умножения в стандартном базисе поля $GF(2^n)$, где $n = 2 \cdot 3^k$, получены оценка сложности умножения $5n \log_3 n \log_2 \log_3 n + O(n \log n)$ и оценка сложности инвертирования, которая больше указанной асимптотически в 2,5 раза. Как следствие, для сложности умножения двоичных многочленов степени N справедлива верхняя оценка $(10 + o(1))N \log_3 N \log_2 \log N$.

Указанные оценки обобщаются на случай других конечных полей. Для случая, когда $n = (p-1)p^k$, где p — такое простое число, что 2 есть первообразный корень по модулю p и $2^{p-1} - 1$ не кратно p^2 , для стандартного базиса в поле $GF(2^n)$ построены мультипликатор сложности $(C + o(1))(n \log_3 n \log_2 \log n)$ и инвертор сложности $O(\log p)n \log n \log \log n$, где $C \leq 10$.

Работа выполнена при поддержке РФФИ, проекты 11-01-00508 и 11-01-00792-а, и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения», проект «Задачи оптимального синтеза управляющих систем».

1. Введение

Известно ([1]; см. также [2]), что при использовании стандартных базисов в полях $GF(2^n)$ сложность булевой схемы для умножения, построенной из двухвходовых элементов, асимптотически равна $O(n \log n \log \log n)$. Более аккуратные известные оценки сложности метода (см. [1]) или его модификаций для $n = 2 \cdot 3^k$ имеют вид $(A + o(1))n \log_3 n \log_2 \log_3 n$, где $A = 12$ [2] и $A = 8,25$ [3]; последняя оценка справедлива для $k = 2^l$. Глубина схем во всех случаях логарифмическая, то есть равная $O(\log n)$.

Для инвертирования (то есть для вычисления мультипликативного обратного) в тех же базисах известен быстрый вариант алгоритма Евклида [4, 5] (см. также [2]) сложности $O(n \log^2 n \log \log n)$, на основе которого может быть построена и булева схема такой же сложности, но глубины, равной $O(n)$. В [6] рассмотрена конструкция башни полей, для умножения и инвертирования в которой в некоторых случаях получены оценки сложности вида $O(n \log^C n)$, где C — некоторая константа; эти оценки хуже, чем упомянутые выше, но представляют интерес, так как получены для другого типа базисов; результат [1] был авторам работы [6], по-видимому, неизвестен. Однако основные формулы, приведенные на с. 227 в [6], вызывают некоторые сомнения, поэтому эти оценки не представляются бесспорными. Корректно в [6] для полей вида $GF(2^n)$, где $n = m^k$, для сложности

умножения и инвертирования получены оценки вида $O(n^{1+1/\log m})$. Подобная конструкция башни полей независимо рассматривалась в [7], но представленные там результаты несколько слабее. В [8] для тех же полей независимо получены более сильные оценки. Результаты [8] были усилены в [9]. В обозначениях настоящей работы их можно сформулировать следующим образом.

Пусть

$$n = (p - 1)p^k,$$

где p — такое простое число, что 2 есть первообразный корень по модулю p и $2^{p-1} - 1$ не кратно p^2 .

В случае $p = 3$ построена схема умножения в стандартном базисе поля $GF(2^n)$ сложности $5n \log_3 n \log_2 \log_3 n + O(n \log n)$ и глубины $6 \log_3 n + o(\log n)$. В том же случае построена схема инвертирования асимптотически в 2,5 раза большей сложности и глубины $O(\log^2 n)$. В предварительных публикациях [9, 10], оценки для сложности умножения при $p = 3$ указывались с мультипликативными постоянными $5\frac{5}{8}$ и $5\frac{1}{4}$ соответственно.

В общем случае, для стандартного базиса в поле $GF(2^n)$ может быть построена схема умножения сложности

$$(10 + o(1))n \log_3 n \log_2 \log_3 n \quad (1)$$

и глубины $(6 + o(1)) \log_3 n$, и схема инвертирования сложности $O(\log p)n \log n \log \log n$ и глубины $O(\log^2 n)$.

Подобные оценки можно вывести и в более общем случае, когда

$$n = (\text{ord}_p 2)p^k$$

при условии, что $2^{\text{ord}_p 2} - 1$ не кратно p^2 , где $\text{ord}_p q$ — порядок числа q по модулю p . Заметим, что условие, что $2^{p-1} - 1$ не кратно p^2 , как можно проверить, не выполняется среди первых 10^{12} чисел только для $p = 1093, 3511$. Однако при этих значениях p число 2 не является первообразным корнем. При $p = 1093$ не выполнено и более слабое условие, что $2^{\text{ord}_p 2} - 1$ не кратно p^2 . Как следствие, умножение двоичных многочленов суммарной степени $N - 1$ можно реализовать схемой сложности $(5 + o(1))N \log_3 N \log_2 \log_3 N$ и глубины $(6 + o(1)) \log_3 N$.

Излагаемый далее метод умножения является модификацией метода, предложенного в [1]. Метод инвертирования основан на технике сведения к инвертированию в подполе из [11].

Полученные результаты представляют интерес еще с одной стороны: указаны примеры многочленов $f_n(x)$, которые имеют вид $x^{(p-1)p^n} + \dots + x^{p^n} + 1$, где $p = O(1)$, таких, что инвертирование в кольце $GF(2)[x]/(f_n(x))$ выполняется по порядку с такой же сложностью, что и обычное умножение многочленов степени $\deg f_n$. Хорошо известным из арифметики степенных рядов примером такой последовательности является $f_n(x) = x^n$.

Изложение построено следующим образом. В разделе 2 сообщаются необходимые сведения о ДПФ. В разделе 3 описан основной метод умножения и следствия из него. В разделе 4 строится схема инвертирования. В разделе 5 показано, что константа 10 в (1) может быть улучшена для некоторых полей. В разделе 6 построен еще один пример последовательности полей с быстрым умножением. В разделе 7 указано следствие для сложности умножения многочленов над произвольным кольцом.

2. Дискретное преобразование Фурье

Напомним необходимые сведения о дискретном преобразовании Фурье.

Пусть $\mathbf{K}$ есть ассоциативное и коммутативное кольцо с единицей. Элемент $\zeta \in \mathbf{K}$ называется примитивным (первообразным) корнем степени $N \in \mathbb{N}$, если $\zeta^N = 1$, и никакой из элементов $\zeta^{N/p} - 1$, где p — простой делитель числа N , не является делителем нуля в $\mathbf{K}$. Напомним, что элемент a называется делителем нуля, если существует ненулевой элемент b , такой, что $ab = 0$.

Дискретным преобразованием Фурье (ДПФ) порядка N называется $(\mathbf{K}^N \rightarrow \mathbf{K}^N)$ -преобразование

$$\text{ДПФ}_{N,\zeta}[\mathbf{K}](\gamma_0, \dots, \gamma_{N-1}) = (\gamma_0^*, \dots, \gamma_{N-1}^*), \quad \gamma_j^* = \sum_{i=0}^{N-1} \gamma_i \zeta^{ij}, \quad (2)$$

где ζ — примитивный корень степени N .

Фундаментальное свойство ДПФ формулируется следующим образом:

Лемма 1. Пусть элементы γ_j^* определяются из (2). Тогда

$$\text{ДПФ}_{N,\zeta^{-1}}[\mathbf{K}](\gamma_0^*, \dots, \gamma_{N-1}^*) = (N\gamma_0, \dots, N\gamma_{N-1}),$$

где под N в правой части формулы понимается сумма N единиц кольца.

Как следствие, получаем, что если элемент $N = 1 + \dots + 1 \in \mathbf{K}$ обратим, то определено обратное к ДПФ преобразование

$$\text{ДПФ}_{N,\zeta}^{-1}[\mathbf{K}] = N^{-1} \text{ДПФ}_{N,\zeta^{-1}}[\mathbf{K}].$$

Известна следующая полиномиальная интерпретация ДПФ.

Рассмотрим многочлен

$$\Gamma(x) = \gamma_0 + \dots + \gamma_{N-1}x^{N-1}.$$

Тогда, по определению,

$$\text{ДПФ}_{N,\zeta}[\mathbf{K}](\gamma_0, \dots, \gamma_{N-1}) = (\Gamma(\zeta^0), \dots, \Gamma(\zeta^{N-1})),$$

то есть ДПФ вычисляет значения многочлена $\Gamma(x)$ в точках ζ^i . Смысл обратного преобразования $\text{ДПФ}_{N,\zeta}^{-1}[\mathbf{K}]$ заключается в восстановлении коэффициентов единственного многочлена степени, меньшей N , имеющего заданный набор значений в точках $\zeta^0, \dots, \zeta^{N-1}$.

Формально, связь между ДПФ и интерполяцией описывается следующей известной леммой, доказательство которой также опускаем.

Лемма 2. Преобразование $\text{ДПФ}_{N,\zeta}[\mathbf{K}]$ задает изоморфизм $\mathbf{K}[x]/(x^N - 1) \rightarrow \mathbf{K}^N$, причем операции в кольце $\mathbf{K}^n$ выполняются покомпонентно.

Рассмотренный изоморфизм приводит к следующему известному способу умножения многочленов над $\mathbf{K}$, обоснование которого опускаем.

Теорема 1. Пусть в кольце $\mathbf{K}$ определено преобразование $\text{ДПФ}_{N,\zeta}[\mathbf{K}]$ и обратное к нему. Тогда умножение двух многочленов суммарной степени не выше $N - 1$ над $\mathbf{K}$ можно выполнить при помощи двух преобразований $\text{ДПФ}_{N,\zeta}[\mathbf{K}]$, одного $\text{ДПФ}_{N,\zeta}^{-1}[\mathbf{K}]$ и N умножений в $\mathbf{K}$.

Независимое вычисление компонент вектора ДПФ по формулам (2) может быть выполнено за $O(N^2)$ операций сложения, вычитания и умножения на константы в кольце $\mathbf{K}$. Для вычисления ДПФ составного порядка N известен следующий более эффективный способ (метод Кули–Тьюки, см. [12, 13]).

Лемма 3. ДПФ порядка ST реализуется при помощи S ДПФ порядка T , T ДПФ порядка S и $(S-1)(T-1)$ операций умножения на степени ζ — примитивного корня степени ST , а именно, умножений на ζ^{jt} , $j = 1, \dots, S-1$, $t = 1, \dots, T-1$.

Доказательство. Заметим, что если ζ — примитивный корень степени ST , то ζ^S и ζ^T — примитивные корни степени T и S соответственно.

Для $s = 0, \dots, S-1$ и $t = 0, \dots, T-1$ запишем:

$$\begin{aligned} \gamma_{sT+t}^* &= \sum_{I=0}^{ST-1} \gamma_I \zeta^{I(sT+t)} = \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{(iS+j)(sT+t)} \\ &= \sum_{i=0}^{T-1} \sum_{j=0}^{S-1} \gamma_{iS+j} \zeta^{itS+jsT+jt} = \sum_{j=0}^{S-1} (\zeta^T)^{js} \cdot \zeta^{jt} \cdot \gamma_{(j),t}, \end{aligned}$$

где

$$\gamma_{(j),t} = \sum_{i=0}^{T-1} \gamma_{iS+j} (\zeta^S)^{it}.$$

Полученная формула позволяет произвести вычисления в следующем порядке.

(а) Для $j = 0, \dots, S-1$ вычисляются вектора

$$(\gamma_{(j),0}, \gamma_{(j),1}, \dots, \gamma_{(j),T-1}) = \text{ДПФ}_{T,\zeta^S}[\mathbf{K}](\gamma_j, \gamma_{S+j}, \dots, \gamma_{(T-1)S+j}).$$

(б) Вычисляются произведения

$$\omega_{(t),j} = \zeta^{jt} \cdot \gamma_{(j),t}, \quad j = 0, \dots, S-1, \quad t = 0, \dots, T-1.$$

(в) Заметим, что

$$\gamma_{sT+t}^* = \sum_{j=0}^{S-1} \omega_{(t),j} (\zeta^T)^{js}.$$

Это позволяет окончательно найти компоненты вектора ДПФ по формулам

$$(\gamma_t^*, \gamma_{T+t}^*, \dots, \gamma_{(S-1)T+t}^*) = \text{ДПФ}_{S,\zeta^T}[\mathbf{K}](\omega_{(t),0}, \omega_{(t),1}, \dots, \omega_{(t),S-1}),$$

где $t = 0, \dots, T-1$.

Утверждение леммы немедленно следует из вида действий, выполняемых на шагах (а)–(в), если заметить, что среди ST умножений на шаге (б) есть $S+T-1$ умножений на $\zeta^0 = 1$. Лемма доказана.

Известно также (см. [14, 13]), что если числа S и T взаимно просты, то для вычисления ДПФ порядка ST достаточно выполнить S ДПФ порядка T и T ДПФ порядка S , иными словами, дополнительных умножений не требуется.

Из леммы Кули–Тьюки следует известное еще, видимо, Рунге и Кенигу утверждение.

Лемма 4. Если кольцо $\mathbf{K}$ содержит примитивные корни порядка 2^k из единицы и элемент 2 обратим, то ДПФ порядка 2^k может быть выполнено за $k2^k$ операций сложения–вычитания и $(k-2)2^{k-1} + 1$ операций скалярного умножения (умножения на константу).

Эта оценка является асимптотически наилучшей из известных верхних оценок сложности ДПФ порядка 2^k .

Из теоремы 1 и леммы 4 приходим к следующему утверждению.

Следствие 1. Если кольцо $\mathbf{K}$ удовлетворяет условию леммы 4 при любых k , то для умножения двух многочленов суммарной степени N над ним требуется не более $3 \cdot 2^n n$ сложений и не более $\frac{3}{2}2^n n + O(2^n)$ умножений в этом кольце, где $n = \lceil \log_2 N \rceil$.

2.1. ДПФ в расширениях колец

Если кольцо $\mathbf{K}$ не содержит корней из единицы подходящей степени, то для умножения многочленов над $\mathbf{K}$ непосредственно использовать способ теоремы 1 невозможно. В алгоритме Шёнхаге–Штрассена [7, 8] и ему подобных в таком случае предлагается использовать расширение

$$\mathbf{K}_{2,n}(x) = \mathbf{K}[x]/(x^{2^n} + 1)$$

кольца $\mathbf{K}$, при этом двойка должна быть обратима в $\mathbf{K}$.

В кольце $\mathbf{K}_{2,n}(x)$ определено ДПФ порядка 2^{n+1} с примитивным корнем x ; здесь и далее вместо элементов фактор-кольца $\mathbf{K}_{2,n}(x)$, которыми являются классы эквивалентных по модулю $x^{2^n} + 1$ многочленов, будут фигурировать многочлены–представители классов.

Рассмотрим также более общую конструкцию, введенную в [15], а именно, для любого p определим кольцо $\mathbf{K}_{p,n}(x)$ как фактор-кольцо $\mathbf{K}[x]/(x^{(p-1)p^n} + x^{(p-2)p^n} + \dots + x^{p^n} + 1)$. В случае, если p — простое число и элемент $p = 1 + \dots + 1 \in \mathbf{K}$ является обратимым в $\mathbf{K}$, то в кольце $\mathbf{K}_{p,n}(x)$ элемент x является примитивным корнем из единицы степени p^{n+1} , так как

$$x^{p^{n+1}} - 1 = (x^{p^n} - 1)(x^{(p-1)p^n} + x^{(p-2)p^n} + \dots + x^{p^n} + 1) = 0,$$

и $x^{p^n} - 1$ — обратимый элемент в кольце $\mathbf{K}_{p,n}(x)$:

$$(x^{p^n} - 1)^{-1} = \frac{-1}{p}(x^{(p-2)p^n} + 2x^{(p-3)p^n} + \dots + (p-2)x^{p^n} + (p-1)).$$

Как следствие, в кольце $\mathbf{K}_{p,n}(x)$ определены ДПФ порядков p^k при всех $k \leq n+1$.

Вместо многочлена $x^{p-1} + \dots + x + 1$ можно взять любой его делитель $h(x)$ над кольцом $\mathbf{K}$, и вместо кольца $\mathbf{K}_{p,n}(x)$ рассмотреть кольцо

$$\mathbf{K}_{p,n}^h(x) = \mathbf{K}[x]/(h(x^{p^n})).$$

Тогда аналогичным образом в этом кольце можно определить ДПФ порядков p^k , $k \leq n+1$. Примитивность элемента x вытекает из взаимной простоты многочленов $x^{p^n} - 1$ и $h(x^{p^n})$, следующей из взаимной простоты многочленов $x^{p^n} - 1$ и $x^{(p-1)p^n} + x^{(p-2)p^n} + \dots + x^{p^n} + 1$.

Если $\mathbf{K}$ — конечное поле, то в качестве $h(x)$ удобно взять неприводимый делитель многочлена $x^{p-1} + \dots + x + 1$. Известно, что при этом

$$\deg h = \text{ord}_p(\text{char } \mathbf{K});$$

напомним, что $\text{ord}_p q$ обозначает порядок числа q по модулю p . Заметим, что

$$\text{ord}_p(\text{char } \mathbf{K}) = p - 1$$

означает, что

$$\mathbf{K}_{p,n}^h(x) \cong \mathbf{K}_{p,n}(x).$$

Если $\text{ord}_{p^2}(\text{char } \mathbf{K}) \neq \text{ord}_p(\text{char } \mathbf{K})$, то кольцо $\mathbf{K}_{p,n}^h(x)$ является полем. Обоснование указанных фактов можно найти, например, в [16].

Для реализации умножения в кольце $\mathbf{K}_{p,n}^h(x)$ его удобно представить как расширение некоторого кольца $\mathbf{K}_{p,m}^h(y)$. Справедливо следующее утверждение.

Лемма 5. Пусть $0 \leq m < n$. Имеет место изоморфизм колец

$$\mathbf{K}_{p,n}^h(x) \cong \mathbf{K}_{p,m}^h(y)[x]/(x^{p^{n-m}} - y), \quad (3)$$

порождаемый подстановкой $x^{p^{n-m}} = y$.

Доказательство. Действительно, многочлен $g(x) \in \mathbf{K}_{p,n}^h(x)$ можно записать в виде

$$g(x) = \sum_{i=0}^{p^{n-m}-1} g_i(x^{p^{n-m}})x^i,$$

где $\deg g_i < p^m \deg h$. Подстановка $x^{p^{n-m}} = y$ переводит $g(x)$ в многочлен

$$\sum_{i=0}^{p^{n-m}-1} g_i(y)x^i \in \mathbf{K}_{p,m}^h(y)[x]/(x^{p^{n-m}} - y),$$

где $g_i(y) \in \mathbf{K}_{p,m}^h(y)$.

Очевидно, что подстановка порождает линейное взаимно однозначное отображение. Остается проверить, что это отображение сохраняет операцию умножения, причем, в силу линейности, проверку можно ограничить нормированными одночленами. В кольце $\mathbf{K}_{p,n}^h(x)$ выполнено соотношение

$$\begin{aligned} x^{j_1 p^{n-m} + i_1} \cdot x^{j_2 p^{n-m} + i_2} &= x^{j_3 p^{n-m} + i_3} \\ &= (x^{j_3 p^{n-m}} \bmod h(x^{p^n}))x^{i_3} = g(x^{p^{n-m}})x^{i_3}, \end{aligned}$$

где

$$\begin{aligned} i_3 &= (i_1 + i_2) \bmod p^{n-m}, \\ j_3 &= j_1 + j_2 + (i_1 + i_2 - i_3)/p^{n-m}, \end{aligned}$$

и

$$\deg g < p^m \deg h.$$

С другой стороны, в кольце $\mathbf{K}_{p,m}^h(y)[x]/(x^{p^{n-m}} - y)$ также верно соотношение

$$y^{j_1} x^{i_1} \cdot y^{j_2} x^{i_2} = y^{j_3} x^{i_3} = g(y)x^{i_3}.$$

Видно, что результаты обоих умножений переходят друг в друга при подстановке $y = x^{p^{n-m}}$. Лемма доказана.

Далее будет существенно использоваться тот факт, что указанное в лемме отображение реализуется простой перестановкой коэффициентов, и поэтому вычисляется “бесплатно”. Из леммы 5 вытекает следующее утверждение.

Следствие 2. Умножение произвольного элемента кольца $\mathbf{K}_{p,n}^h(x)$ на элемент $x^{kp^{n-m}}$ выполняется за p^{n-m} параллельных умножений на y^k в кольце $\mathbf{K}_{p,m}^h(y)$.

Если в качестве примитивного корня p^{m+1} -й степени из единицы в кольце $\mathbf{K}_{p,n}^h(x)$ взять элемент $y = x^{p^{n-m}}$, то, аналогично следствию 2, можно доказать следующее утверждение.

Следствие 3. ДПФ порядка p^{m+1} в кольце $\mathbf{K}_{p,n}^h(x)$ выполняется при помощи p^{n-m} параллельных ДПФ порядка p^{m+1} в кольце $\mathbf{K}_{p,m}^h(y)$.

2.2. Двоичный метод умножения

Следующая теорема доказывается методом Шёнхаге–Штрассена (см. [17]).

Теорема 2. Умножение в кольце $\mathbf{K}_{2,n}(x)$ может быть выполнено при помощи $3 \cdot 2^n n (\log_2 n + O(1))$ операций сложения–вычитания, $3 \cdot 2^{n+\lceil \log_2 n \rceil - 1}$ операций умножения и 2^n операций скалярного умножения в $\mathbf{K}$.

Так как она малоизвестна, приведем ее доказательство.

Доказательство. Воспользуемся формулой (3) с выбором параметра $m = \lceil n/2 \rceil$. Умножение многочленов над $\mathbf{K}_{2,m}(y)$ по модулю $x^{2^{n-m}} - y$ выполним как обычное умножение многочленов степени не выше $2^{n-m} - 1$ с последующим приведением по модулю.

Умножение выполняется при помощи трех ДПФ порядка $2^{n-m+1} = 2^{\lfloor n/2 \rfloor + 1}$ и $2^{\lfloor n/2 \rfloor + 1}$ умножений в кольце $\mathbf{K}_{2,m}(y)$, при этом обратное ДПФ реализуется с точностью до постоянного множителя. Приведение по модулю $x^{2^{n-m}} - y$ реализуется за 2^n сложений–вычитаний в $\mathbf{K}$. Окончательно результат умножается на подходящую степень 2^{-1} .

Для чисел $\mu_A(n)$ сложений–вычитаний и $\mu_M(n)$ нескаларных умножений в предложенной схеме при $n \geq 2$ имеем рекуррентные соотношения:

$$\begin{aligned}\mu_A(n) &\leq 2^{\lfloor n/2 \rfloor + 1} \mu_A(\lceil n/2 \rceil) + 3(\lfloor n/2 \rfloor + 1)2^{n+1} + 2^n, \\ \mu_M(n) &\leq 2^{\lfloor n/2 \rfloor + 1} \mu_M(\lceil n/2 \rceil),\end{aligned}$$

которые разрешаются так, как заявлено в утверждении теоремы, если при $n = 1$ воспользоваться оценками

$$\mu_A(1) = 5, \quad \mu_M(1) = 3.$$

Иначе можно положить

$$\mu_A(1) = 2, \quad \mu_M(1) = 4$$

— в этом случае схема будет содержать $2^{n+\lceil \log_2 n \rceil + 1}$ умножений, но общее число операций будет несколько меньше. Теорема доказана.

Доказанная оценка сложности является асимптотически наилучшей из известных. Как известно, умножение многочленов над $\mathbf{K}$ можно выполнить при помощи подходящей схемы умножения в $\mathbf{K}_{2,n}(x)$.

Следствие 4. Умножение двух многочленов суммарной степени не выше $N - 1$ над кольцом $\mathbf{K}$ с обратимой двойкой выполнимо со сложностью $3N \log_2 N (\log_2 \log_2 N + O(1))$.

Доказательство. В случае $N = 2^n$ это прямое следствие теоремы 2. При произвольном N можно, например, воспользоваться следующим результатом работы [18]. Пусть $\mu(k)$ — сложность схемы умножения многочленов степени $2^k - 1$ по модулю $x^{2^k} + 1$. Запишем

$$N = 2^{n_1} + 2^{n_2} + \dots + 2^{n_s}, \quad n_1 > n_2 > \dots > n_s.$$

Тогда для умножения многочленов суммарной степени не выше $N - 1$ можно построить схему сложности не более $\mu(n_1) + \mu(n_2) + \dots + \mu(n_s) + 5,5N$. Следствие доказано.

Известно еще несколько способов доказательства следствия 4 — выбранный способ позволяет получить более аккуратную оценку сложности.

Заметим, что для реализации умножения многочленов можно использовать не только изоморфизмы из леммы 5.

3. Быстрое умножение при помощи ДПФ порядка 3

В кольце, в котором двойка необратима, нельзя определить ДПФ четного порядка, и поэтому Шёнхаге в [1] предложил использовать ДПФ порядка 3^k .

Компоненты ДПФ порядка 3 над $\mathbf{K}$ вычисляются по формулам

$$\begin{aligned} \gamma_0^* &= \gamma_0 + \gamma_1 + \gamma_2, \\ \gamma_1^* &= \gamma_0 - \gamma_2 + \zeta(\gamma_1 - \gamma_2), \\ \gamma_2^* &= \gamma_0 - \gamma_1 - \zeta(\gamma_1 - \gamma_2), \end{aligned}$$

где ζ — примитивный кубический корень в кольце $\mathbf{K}$. Эти вычисления можно выполнить, используя семь аддитивных операций и одно скалярное умножение, или шесть сложений — вычитаний и два умножения. Если $\text{char } \mathbf{K} = 2$, то достаточно пяти сложений и одного умножения.

Поэтому из леммы 3 получаем следующее утверждение.

Лемма 6. Если в кольце $\mathbf{K}$ есть примитивные корни степени 3^k и элемент 3 обратим, то ДПФ порядка 3^k можно вычислить, используя не более $(7/3)k3^k$ операций сложения — вычитания и $(k - 1)3^k + 1$ операций скалярного умножения. В кольце характеристики два число аддитивных операций оценивается как $(5/3)k3^k$.

Доказательство. Действительно, указанные оценки вытекают из рекуррентных соотношений на числа $F_A(3^k)$ аддитивных операций и $F_C(3^k)$ операций скалярного умножения в методе леммы 3:

$$\begin{aligned} F_A(3^k) &= 3F_A(3^{k-1}) + 3^{k-1}F_A(3), \\ F_C(3^k) &= 3F_C(3^{k-1}) + 3^{k-1}F_C(3) + 2 \cdot 3^{k-1} - 2, \end{aligned}$$

и начальных условий $F_C(3) = 1$, $F_A(3) = 7$ в общем случае или $F_A(3) = 5$ для кольца характеристики 2. Лемма доказана.

Из теоремы 1 и леммы 6 вытекает следующее утверждение.

Следствие 5. Если кольцо $\mathbf{K}$ удовлетворяет условию леммы 6 при любом k , то для умножения двух многочленов суммарной степени $N - 1$ над ним нужно не больше $7 \cdot 3^n n$ сложений–вычитаний и не больше $7 \cdot 3^n n + O(3^n)$ умножений в этом кольце, где

$$n = \lceil \log_3 N \rceil.$$

Если $\text{char } \mathbf{K} = 2$, то мультипликативную константу в первой оценке можно уменьшить до 5.

Область применения этого следствия довольно узка, но она не совпадает с областью применения следствия 1, в котором указана более сильная оценка.

Если в кольце $\mathbf{K}$ нет примитивных корней достаточно большой степени 3^k , но тройка обратима, то можно рассмотреть расширение

$$\mathbf{K}_{3,n}(x) = \mathbf{K}[x]/(x^{2 \cdot 3^n} + x^{3^n} + 1),$$

в котором x является примитивным корнем степени 3^{n+1} . В этом случае известные оценки сложности ДПФ ниже будут несколько улучшены.

Далее внутри этого раздела будем везде полагать $\text{char } \mathbf{K} = 2$, если особо не оговаривается иное.

Лемма 7. Пусть $f(x) \in \mathbf{K}_{p,n}(x)$. Тогда справедливы следующие утверждения.

- (i) Элемент $x^m f(x)$ в кольце $\mathbf{K}_{p,n}(x)$ вычисляется схемой глубины 1 и сложности $(p-2) \min\{|m|, p^n\}$.
- (ii) Все элементы $\{x^m f(x) \mid m \in \mathbf{Z}\}$ вычисляются схемой глубины 1 и сложности $\binom{p-1}{2} p^n$.

Доказательство. По модулю $x^{p^{n+1}} - 1$ умножение на степени x выполняется “бесплатно”, циклическим сдвигом коэффициентов. Можно записать, что

$$x^m f(x) \bmod (x^{p^{n+1}} - 1) = \sum_{i=0}^{p-2} a_i(x) x^{ip^n} + b(x) x^{(p-1)p^n},$$

где $\deg a_i, b = p^n - 1$. Тогда в кольце $\mathbf{K}_{p,n}(x)$ результат умножения вычисляется приведением подобных в сумме

$$\sum_{i=0}^{p-2} (a_i(x) + b(x)) x^{ip^n}. \quad (4)$$

Оценка в (i) получается, если учесть, что многочлен $b(x)$ содержит $\min\{|m|, p^n\}$ не тождественно нулевых коэффициентов, и столько же заведомо нулевых коэффициентов содержат многочлены $a_i(x)$. Для доказательства (ii) достаточно заметить, что, как следует из (4), все коэффициенты многочлена $x^m f(x) \in \mathbf{K}_{p,n}(x)$ принадлежат множеству $\{f_k \mid 0 \leq k < (p-1)p^n\} \cup \{f_{k+ip^n} + f_{k+jp^n} \mid 0 \leq k < 3^n, 0 \leq i, j \leq p-2\}$, где f_k есть коэффициент в выражении для $f(x)$ при x^k . Лемма доказана.

Лемма 8. Преобразование ДПФ $_{3,\zeta}[\mathbf{K}_{3,n}(x)](\gamma_0, x^{m_1} \gamma_1, x^{m_2} \gamma_2)$, где m_1 и $m_2 \in \mathbf{Z}$, $\zeta \in \{x^{3^n}, x^{2 \cdot 3^n}\}$, может быть выполнено со сложностью $10 \cdot 3^n$ и глубиной 3.

Доказательство. Положим

$$(\gamma_0^*, \gamma_1^*, \gamma_2^*) = \text{ДП}\Phi_{3,\zeta}[\mathbf{K}_{3,n}(x)](\gamma_0, x^{m_1}\gamma_1, x^{m_2}\gamma_2).$$

Ограничимся рассмотрением случая $\zeta = x^{3^n}$; другой случай рассматривается аналогично.

Пусть $0 \leq k < 3^n$. Положим $m_0 = 0$. Обозначим через a_i и b_i коэффициенты многочлена γ_i при степенях $x^{(k-m_i) \bmod 3^n}$ и $x^{3^n + ((k-m_i) \bmod 3^n)}$ соответственно. Через $a_{i,j}$ и $b_{i,j}$ обозначим коэффициенты многочлена $\zeta^j x^{m_i} \gamma_i$ при степенях, соответственно, x^k и x^{3^n+k} . Несложно видеть, что при любом i вектор коэффициентов $\left(\begin{bmatrix} a_{i,0} \\ b_{i,0} \end{bmatrix}, \begin{bmatrix} a_{i,1} \\ b_{i,1} \end{bmatrix}, \begin{bmatrix} a_{i,2} \\ b_{i,2} \end{bmatrix} \right)$ получается из вектора $\left(\begin{bmatrix} a_i \\ b_i \end{bmatrix}, \begin{bmatrix} b_i \\ a_i + b_i \end{bmatrix}, \begin{bmatrix} a_i + b_i \\ a_i \end{bmatrix} \right)$ некоторым циклическим сдвигом. В частности, $a_{i,j} = b_{i,j-1}$ (здесь и далее в доказательстве операции с индексами выполняются по модулю 3).

Обозначим через a_i^* и b_i^* коэффициенты многочлена γ_i^* при степенях x^k и x^{3^n+k} соответственно. Используя равенство $a_{i,j} = b_{i,j-1}$, получаем систему формул

$$\begin{aligned} a_0^* &= a_0 + a_{1,0} + a_{2,0}, & b_0^* &= b_0 + a_{1,1} + a_{2,1}, \\ a_1^* &= a_0 + a_{1,1} + a_{2,2}, & b_1^* &= b_0 + a_{1,2} + a_{2,0}, \\ a_2^* &= a_0 + a_{1,2} + a_{2,1}, & b_2^* &= b_0 + a_{1,0} + a_{2,2}, \end{aligned} \quad (5)$$

которая имеет вид

$$\begin{aligned} a_0^* &= a_0 + A_0, & a_1^* &= a_0 + A_1, & a_2^* &= a_0 + A_2, \\ b_0^* &= b_0 + B_0, & b_1^* &= b_0 + B_1, & b_2^* &= b_0 + B_2, \end{aligned}$$

где

$$A_i = a_{1,i} + a_{2,\sigma(i)}, \quad B_i = a_{1,i+1} + a_{2,\tau(i)},$$

и при этом

$$A_0 + A_1 + A_2 = 0, \quad B_0 + B_1 + B_2 = 0.$$

Заметим также, что при любом i

$$A_{i-1} + B_i = a_{1,i}. \quad (6)$$

Для доказательства леммы достаточно показать, как строится схема, вычисляющая все a_i^* и b_i^* со сложностью 10 и глубиной 3 (входами схемы являются a_i и b_i).

- (а) Вычислим те компоненты среди A_i и B_i , которые имеют вид $c + d$, где $c, d \in \{a_1, a_2, b_1, b_2\}$.

Из формул (5) и формул для $a_{i,j}$, $b_{i,j}$ видно, что множество компонент, вычисляемых в этом пункте, относится к одному из трех видов: $\{A_i, B_i\}$, $\{A_{i-1}, A_i, B_{i+1}\}$, или $\{A_{i-1}, B_i, B_{i+1}\}$ при некотором i .

- (б) Если вычислена только одна компонента A_i , то, используя подходящую формулу из (6), вычислим еще одну компоненту $A_j = B_l + c$, где $c \in \{a_1, a_2, b_1, b_2\}$, на глубине 2. Аналогично при необходимости вычислим недостающую компоненту B_j .

Приведем обоснование возможности вычисления по формулам (6). Если в (а) вычислены компоненты A_i и B_i , то $a_{1,i}, a_{1,i+1} \in \{a_1, a_2, b_1, b_2\}$, и по формулам (6) можно вычислить A_{i-1} и B_{i+1} . Если вычислены компоненты A_{i-1} , A_i и B_{i+1} , то $a_{1,i} \in \{a_1, a_2, b_1, b_2\}$, и по формуле (6) можно найти B_i . Если вычислены компоненты A_{i-1} , B_i и B_{i+1} , то $a_{1,i+1} \in \{a_1, a_2, b_1, b_2\}$, и по формуле (6) можно найти A_i .

Таким образом, реализовано по две компоненты A_i и B_i , причем не менее чем по одной — с глубиной 1.

- (в) Без ограничения общности предположим, что реализованы A_0 и A_1 , причем A_0 — с глубиной 1. Вычислим все a_i^* по формулам:

$$a_0^* = a_0 + A_0, \quad a_1^* = a_0 + A_1, \quad a_2^* = a_0^* + A_1,$$

используя еще 3 сложения. Ясно, что глубина вычисления a_i^* не больше 3. Аналогично вычислим b_i^* . Лемма доказана.

Замечание 1. Из доказательства следует, что оценка глубины остается справедливой, если вход γ_0 имеет глубину 1.

Замечание 2. Если не предполагать, что $\text{char } \mathbf{K} = 2$, то для сложности преобразования леммы можно указать оценку $13 \cdot 3^n$, см. [10].

Следующая лемма используется только для уточнения второго по порядку роста члена в оценке сложности умножения в $\mathbf{K}_{3,n}(x)$, поэтому ее доказательство мы приводим в сокращенном виде.

Лемма 9. Преобразование $(x^{l_0}\gamma_0^*, x^{l_1}\gamma_1^*, x^{l_2}\gamma_2^*)$, где $(\gamma_0^*, \gamma_1^*, \gamma_2^*)$ — вектор значений преобразования из леммы 8, и $3^n \geq l_0 \geq l_1 \geq l_2 \geq 0$, может быть выполнено со сложностью $10 \cdot 3^n$ и глубиной 4.

Доказательство. Пусть

$$f(x) = \sum_{k=0}^{2 \cdot 3^n - 1} f_k x^k,$$

тогда в кольце $\mathbf{K}_{3,n}(x)$ при $0 \leq l \leq 3^n$ многочлен $x^l f(x)$ имеет коэффициенты при x^k и x^{3^n+k} , равные f_{m+3^n} , $f_m + f_{m+3^n}$ (где $m = k - l + 3^n$) соответственно, если $k < l$, и f_m , f_{m+3^n} (где $m = k - l$), если $3^n > k \geq l$. Тогда в обозначениях предыдущей леммы при $k \geq l_0$ требуется вычислить те же выражения a_i^* и b_i^* , $i = 0, 1, 2$; при $l_0 > k \geq l_1$ — выражения b_0^* , $a_0^* + b_0^*$ и a_i^* , b_i^* , $i = 1, 2$; при $l_1 > k \geq l_2$ — выражения b_i^* , $a_i^* + b_i^*$, $i = 0, 1$, и a_2^* , b_2^* ; при $l_2 > k$ — выражения b_i^* , $a_i^* + b_i^*$, $i = 0, 1, 2$.

В первом случае имеем ту же систему, что и в лемме 8.

Во втором случае вычисляемая система имеет вид

$$\begin{aligned} a_0^* + b_0^* &= c_0 + a_{1,2} + a_{2,2}, & b_0^* &= b_0 + a_{1,1} + a_{2,1}, \\ a_1^* &= a_0 + a_{1,1} + a_{2,2}, & b_1^* &= b_0 + a_{1,2} + a_{2,0}, \\ a_2^* &= a_0 + a_{1,2} + a_{2,1}, & b_2^* &= b_0 + a_{1,0} + a_{2,2}, \end{aligned}$$

где $c_0 = a_0 + b_0$.

Имеется девять возможных вариантов для вида системы, записанной в переменных a_i и b_i , среди них — три пары совпадающих с точностью до перестановки $a_1 \leftrightarrow a_2$, $b_1 \leftrightarrow b_2$,

$a_1^* \leftrightarrow a_2^*$. Можно проверить, что в любом случае система вычисляется схемой сложности 10 и глубины 4, причем выражения a_1^* и b_1^* — с глубиной 3.

В третьем случае система отличается от системы во втором случае суммой $a_1^* + b_1^*$ вместо a_1^* . В последнем случае имеем систему, аналогичную первой:

$$\begin{aligned} a_0^* + b_0^* &= c_0 + a_{1,2} + a_{2,2}, & b_0^* &= b_0 + a_{1,1} + a_{2,1}, \\ a_1^* + b_1^* &= c_0 + a_{1,0} + a_{2,1}, & b_1^* &= b_0 + a_{1,2} + a_{2,0}, \\ a_2^* + b_2^* &= c_0 + a_{1,1} + a_{2,0}, & b_2^* &= b_0 + a_{1,0} + a_{2,2}, \end{aligned}$$

Можно проверить, что указанные системы также реализуются схемами сложности 10 и глубины не более 4.

Объединяя схемы преобразований по всем k , получаем необходимую оценку. Лемма доказана.

Лемма 10. ДПФ порядка 3^k над кольцом $\mathbf{K}_{3,n}(x)$, где $k \leq n+1$, может быть выполнено со сложностью $10k3^{n+k-1}$ и глубиной $3k$.

Доказательство. Действительно, вычисление ДПФ порядка 3^k , если воспользоваться леммой 3 с $S = 3$ и $T = 3^{k-1}$, сводится к выполнению 3^{k-1} внешних ДПФ порядка 3, трех внутренних ДПФ порядка 3^{k-1} , причем входы любого из внешних ДПФ имеют вид $\gamma_{(0),t}$, $x^l \gamma_{(1),t}$, $x^{2l} \gamma_{(2),t}$ в обозначениях леммы 3. Поэтому вместо внешних ДПФ можно использовать преобразования леммы 8. Теперь оценка леммы легко доказывается по индукции. Лемма доказана.

Замечание 3. Схема такой же сложности и глубины может быть построена для преобразования ДПФ $_{3^k, x^s}[\mathbf{K}_{3,n}(x)](\gamma_0, \dots, \gamma_{3^k-1-1}, x^{m_{3^k-1}} \gamma_{3^k-1}, \dots, x^{m_{3^k-1}} \gamma_{3^k-1})$, при этом входы γ_i , $0 \leq i < 3^{k-1}$, могут иметь глубину 1. Для этого нужно заменить самые внутренние ДПФ порядка 3 в конструкции леммы 10 преобразованиями леммы 8.

Заметим, что справедливо следующее утверждение.

Лемма 11. Умножение в кольце $\mathbf{K}_{3,1}(x)$ может быть выполнено со сложностью 57 и глубиной 5.

Доказательство. Представим перемножаемые многочлены $A(x), B(x) \in \mathbf{K}_{3,1}(x)$ в виде

$$A(x) = A_1 x^3 + A_0, \quad B(x) = B_1 x^3 + B_0,$$

где $\deg A_i, B_i \leq 2$. Их произведение вычислим методом Карацубы:

$$AB = A_1 B_1 x^6 + ((A_0 - A_1)(B_0 - B_1) + A_1 B_1 + A_0 B_0) x^3 + A_0 B_0.$$

Обозначим

$$C = (A_0 - A_1)(B_0 - B_1) = C_1 x^3 + C_0,$$

$$D = A_0 B_0 = D_1 x^3 + D_0,$$

$$E = A_1 B_1 = E_1 x^3 + E_0,$$

где $\deg C_0, D_0, E_0 \leq 2$ и $\deg C_1, D_1, E_1 \leq 1$. Тогда в кольце $\mathbf{K}_{3,1}(x)$, то есть по модулю $x^6 + x^3 + 1$, справедливо соотношение

$$\begin{aligned} AB &= E x^6 + (C + D + E) x^3 + D = (C + D) x^3 + (D - E) \\ &= ((D_0 - C_1) + C_0 - E_1) x^3 + ((D_0 - C_1) - E_0 - D_1) \\ &= G_1 x^3 + G_0. \end{aligned}$$

Произведения C , D , E многочленов степени не выше 2 выполним прямолинейным способом за 9 умножений и 4 сложения каждое. Остальные действия выполняются за 18 аддитивных операций: из них шесть используется для вычисления разностей $A_0 - A_1$, $B_0 - B_1$, и 12 — для вычисления сумм G_0 , G_1 . Несложно оценить глубину полученной схемы, если заметить, что все коэффициенты многочленов C , D , E вычисляются на глубине не выше 3, кроме коэффициента многочлена C при x^2 , который вычисляется с глубиной 4.

Определим функцию $\varphi(n)$ следующим образом:

$$\begin{aligned}\varphi(1) &= 0, \\ \varphi(n) &= 2(\varphi(\lceil n/2 \rceil) + \lfloor n/2 \rfloor).\end{aligned}$$

Прямой подстановкой несложно проверить, что

$$\varphi(n) \leq (n-1)(\lceil \log_2 n \rceil + 1),$$

причем в случае $n = 2^k + 1$ неравенство обращается в равенство. Следующая лемма легко доказывается по индукции.

Лемма 12. Пусть

$$\mu(n) \leq 2p^{\lfloor n/2 \rfloor} \mu(\lceil n/2 \rceil) + 2A \lfloor n/2 \rfloor p^n + Bp^n,$$

где A и B не зависят от n . Тогда

$$\mu(n) \leq A\varphi(n)p^n + (\mu(1) + B)2^{\lceil \log_2 n \rceil} p^n - Bp^n.$$

Теорема 3. Умножение в кольце $\mathbf{K}_{3,n}(x)$ может быть выполнено схемой сложности не выше $(10\varphi(n) + 64\frac{1}{3} \cdot 2^{\lceil \log_2 n \rceil} - 7\frac{1}{3})3^n$ и глубины $6n + 4\lceil \log_2 n \rceil - 1$.

Доказательство. При $n \geq 2$ представим кольцо $\mathbf{K}_{3,n}(x)$ как расширение кольца $\mathbf{K}_{3,m}(y)$ согласно лемме 5:

$$\mathbf{K}_{3,n}(x) \cong \mathbf{K}_{3,m}(y)[x]/(x^{3^{n-m}} - y)$$

и положим

$$m = \lceil n/2 \rceil.$$

Умножение многочленов над $\mathbf{K}_{3,m}(y)$ по модулю $x^{3^{n-m}} - y$ будем выполнять как обычное умножение многочленов степени не выше $3^{n-m} - 1$ с последующим приведением по модулю.

Для умножения используется шесть ДПФ порядка $N = 3^{n-m} = 3^{\lfloor n/2 \rfloor}$: три ДПФ используются обычным образом для вычисления произведения по модулю $x^N - 1$, а три других — для вычисления произведения по модулю $x^N - \alpha^N$, где $\alpha = y^{3^{2m-n}}$; существование этих ДПФ гарантируется выполнением неравенства $n - m \leq m$, а выбор α будет объяснен ниже. Второе умножение сводится к подстановке $x = \alpha z$, вычислению произведения по модулю $z^N - 1$, и обратной подстановке $z = x/\alpha$. Действительно,

$$(f(x) \bmod (x^N - \alpha^N))|_{x=\alpha z} = f(\alpha z) \bmod (z^N - 1). \quad (7)$$

Восстановление многочлена $f(x) \in \mathbf{K}_{3,m}(y)[x]$ степени не выше $2N - 2$ по остаткам f_1 и f_α от деления, соответственно, на $x^N - 1$ и $x^N - \alpha^N$ можно выполнить по формуле

$$f(x) = \frac{1}{\alpha^N - 1} ((x^N - 1)f_\alpha(x) - (x^N - \alpha^N)f_1(x)),$$

причем при $N = 3^{n-m}$ в силу соотношения $\alpha^{2N} = \alpha^N + 1$ множитель $(\alpha^N - 1)^{-1}$ равен $\alpha^N = y^{3^m}$. Тогда искомое произведение вычисляется по формуле

$$f(x) \bmod (x^N - y) = y^{3^m} ((y + 1)f_\alpha(x) + (y + y^{3^m})f_1(x)). \quad (8)$$

Подстановка $x = \alpha z$ сводится к умножению коэффициентов перемножаемых многочленов на степени y . Мы явно вычисляем только коэффициенты при степенях x^k , $k = 0, \dots, N/3 - 1$; остальные умножения могут быть внесены внутрь последующего ДПФ согласно замечанию к лемме 10.

Согласно лемме 7, указанные преобразования коэффициентов могут быть выполнены с глубиной 1 и сложностью

$$2 \sum_{k=0}^{3^{n-m-1}-1} k 3^{2m-n} = 3^{(2m-n)+(n-m-1)} (3^{n-m-1} - 1) = 3^{n-2} - 3^{m-1}.$$

Если $y \in \mathbf{K}_{3,m}(y)$, то, согласно лемме 7, выражение $(y^{m_1} + y^{m_2})y$ можно вычислить со сложностью 3^{m+1} и глубиной 2. Из этого следует, что слагаемое $y^{3^m}(y + y^{3^m})f_1(x)$ в формуле (8) вычисляется схемой сложности 3^{n+1} и глубины 2.

Пусть

$$f(\alpha z) \bmod (z^N - 1) = \sum_{k=0}^{N-1} a_k z^k.$$

Тогда можно вычислить многочлен

$$y^{3^m} f_\alpha(x) = \sum_{k=0}^{N-1} a_k y^{3^m - k 3^{2m-n}} x^k,$$

заменяв в схеме обратного ДПФ, вычисляющего коэффициенты многочлена $f(\alpha z) \bmod (z^N - 1)$, внешние ДПФ порядка 3 подходящими преобразованиями леммы 9. Эти преобразования имеют параметры

$$(l_0, l_1, l_2) = (3^m - l 3^{2m-n}, 2 \cdot 3^{m-1} - l 3^{2m-n}, 3^{m-1} - l 3^{2m-n}), \quad l = 0, \dots, 3^{n-m-1} - 1.$$

Согласно лемме 9, сложность модифицированного обратного оценивается так же, как в лемме 10, а глубина — на 1 больше.

Для завершения вычислений по формуле (8) остается выполнить умножение многочлена $y^{3^m} f_\alpha(x)$ на y и вычислить сумму $y^{3^m} f_\alpha(x) + y \cdot y^{3^m} f_\alpha(x) + y^{3^m} (y + y^{3^m}) f_1(x)$. Умножение, согласно лемме 7, выполняется со сложностью 3^{n-m} и глубиной 1, а сложения — со сложностью $4 \cdot 3^n$ и глубиной 2 относительно глубины слагаемых.

Окончательно для сложности $\mu(n)$ построенной схемы при $n \geq 2$ получаем рекуррентное соотношение

$$\mu(n) \leq 2 \cdot 3^{\lfloor n/2 \rfloor} \mu(\lceil n/2 \rceil) + 20 \lfloor n/2 \rfloor 3^n + 7 \frac{1}{9} \cdot 3^n + 3^{\lfloor n/2 \rfloor} - 3^{\lceil n/2 \rceil - 1},$$

где второе слагаемое отвечает сложности ДПФ, оцениваемой леммой 10. Разность $3^{\lfloor n/2 \rfloor} - 3^{\lfloor n/2 \rfloor - 1}$ можно оценить сверху как $2 \cdot 3^{n-2}$. Получаем, что

$$\mu(n) \leq 2 \cdot 3^{\lfloor n/2 \rfloor} \mu(\lceil n/2 \rceil) + 2A \lfloor n/2 \rfloor 3^n + B3^n,$$

где $A = 10$ и $B = 7 \frac{1}{3}$. Отсюда, при помощи леммы 12, следует утверждение теоремы в части сложности при подстановке $\mu(1) \leq 57$ (лемма 11).

Для глубины получаем соотношение

$$d(n) \leq d(\lceil n/2 \rceil) + 6 \lfloor n/2 \rfloor + 4,$$

из которого при $d(1) \leq 5$ (лемма 11), как можно проверить по индукции, следует утверждение теоремы в части глубины. Теорема доказана.

Замечание 4. Распространяя метод теоремы 3 на произвольное кольцо $\mathbf{K}$ с обратимой тройкой, можно оценить сложность умножения в $\mathbf{K}_{3,n}(x)$ как $(13\varphi(n) + O(n))3^n$ в силу замечания 2 к лемме 8.

Стандартным образом асимптотическая оценка сложности теоремы 3 может быть перенесена на случай произвольного N , если увеличить запас модулей, для которых построен быстрый алгоритм умножения. Для этого несколько модифицируем метод теоремы 3.

Вместо колец $\mathbf{K}_{3,n}(x)$ будем рассматривать кольца

$$\mathbf{K}_{3,n,s}(x) = \mathbf{K}[x]/(x^{2s3^n} + x^{s3^n} + 1).$$

Пусть далее $M(s)$ обозначает сложность умножения двоичных многочленов степени s с глубиной $O(\log s)$.

Теорема 4. Умножение в кольце $\mathbf{K}_{3,n,s}(x)$ может быть выполнено схемой сложности $10s\varphi(n)3^n + O(M(s)3^n n)$ и глубины $6n + O(\log(sn))$.

Доказательство. Переноса процедуру построения схемы умножения из теоремы 3 на кольцо $\mathbf{K}_{3,n,s}(x)$, для сложности $\mu_s(n)$ и глубины $d_s(n)$ умножения в $\mathbf{K}_{3,n,s}(x)$ приходим к соотношениям

$$\begin{aligned} \mu_s(n) &\leq 2 \cdot 3^{\lfloor n/2 \rfloor} \mu_s(\lceil n/2 \rceil) + 20s \lfloor n/2 \rfloor 3^n + O(s3^n), \\ d_s(n) &\leq d_s(\lceil n/2 \rceil) + 6 \lfloor n/2 \rfloor + 4, \end{aligned}$$

с учетом того, что аддитивные операции и умножения на степени x^s в кольце $\mathbf{K}_{3,n,s}(x)$ выполняются в s раз сложнее, чем аддитивные операции и умножения на соответствующие степени x в кольце $\mathbf{K}_{3,n}(x)$. Для доказательства теоремы остается подставить начальное условие $\mu_s(1) = M(6s)$.

Полагая $\mathbf{K} = GF(2)$, получаем следующее утверждение.

Следствие 6. Умножение двоичных многочленов суммарной степени не выше $N - 1$ можно выполнить схемой сложности не более $(5 + o(1))N \log_3 N \log_2 \log_2 N$ и глубины $(6 + o(1)) \log_3 N$.

Доказательство. Для доказательства выполним умножение как умножение в кольце $\mathbf{K}_{3,n,s}(x)$, выбирая параметры из условий

$$2(s-1)3^n < N \leq 2s3^n, \quad s = O(\sqrt{\log n}),$$

и воспользуемся оценками теоремы 4, подставив

$$M(s) = s^{1+o(1)}.$$

Замечание 5. Метод теоремы 2 и следствия 4 дает для сложности умножения многочленов суммарной степени не выше $N - 1$ асимптотическую оценку $3N \log_2 N \log_2 \log_2 N$, а следствие 6 — близкую оценку $3,16N \log_2 N \log_2 \log_2 N$.

Альтернативным образом можно воспользоваться теоремой 3 при $\mathbf{K} = GF(2^s)$. При этом в случае $(s, 6) = 1$ многочлен $x^{2 \cdot 3^n} + x^{3^n} + 1$ неприводим над $GF(2^s)$, см. [16]. Следовательно,

$$\mathbf{K}_{3,n}(x) \cong GF(2^{2s3^n}).$$

Тогда для умножения в кольце $\mathbf{K}_{3,n}(x)$ можно построить схему, удовлетворяющую таким же оценкам сложности, как в теореме 4. Эта конструкция дает пример полей $GF(2^N)$ с асимптотически быстрым умножением на более плотном множестве степеней $\{N\}$.

Следствие 7. Пусть $N \in \{2s3^n \mid (s, 6) = 1, s \leq \sqrt{\log n}\}$. Тогда умножение в стандартном базисе поля $GF(2^N)$ можно выполнить схемой сложности, не превосходящей $(5 + o(1))N \log_3 N \log_2 \log_2 N$ и глубины $(6 + o(1)) \log_3 N$.

Умножение в двоичных кольцах (полях) $\mathbf{K}_{p,n}^h(x)$ можно выполнить как умножение двоичных многочленов степени $(\deg h)p^n - 1$ с последующим приведением по модулю $h(x^{p^n})$. Как известно, приведение многочлена степени $km - 1$ по модулю многочлена степени m выполняется схемой сложности $O(kM(m))$ и глубины $O(\log(km))$ (см., например, [2]). Приведение по модулю $h(x^{p^n})$ выполняется схемой из p^n параллельных экземпляров схемы приведения по модулю $h(x)$, и имеет, следовательно, сложность $O(M(\deg h)p^n)$ и глубину $O(\log \deg h)$. Поэтому из следствия 6 приходим к следующему утверждению.

Следствие 8. Пусть $\text{char } \mathbf{K} = 2$. Умножение в кольце $\mathbf{K}_{p,n}^h(x)$ можно выполнить схемой сложности $(10 + o(1))N \log_3 N \log_2 \log_2 N$ и глубины $(6 + o(1)) \log_3 N$, где $N = (\deg h)p^n$ и $n \rightarrow \infty$.

4. Инвертирование

4.1. Общий случай

Рассмотрим кольцо $\mathbf{K}_{p,n}^h(x)$, $\text{char } \mathbf{K} = 2$. Обозначим

$$q_n = 2^{(\deg h)p^n}.$$

Пусть $X \in \mathbf{K}_{p,n}^h(x) \cong GF(q_n)$. Тогда обратный к X элемент можно вычислять по формулам (см. [11])

$$Z = X^{q_{n-1} + q_{n-1}^2 + \dots + q_{n-1}^{p-1}}, \quad Y = XZ, \quad X^{-1} = Y^{-1}Z. \quad (9)$$

Необходимо заметить, что $Y \in GF(q_{n-1})$, поскольку

$$Y^{q_{n-1}} = X^{q_{n-1}q_{n-1}^{p-1}/(q_{n-1}-1)} = X^{q_{n-1}}X^{q_{n-1}^{p-1}/(q_{n-1}-1)} = Y.$$

Для числа $q_{n-1} + q_{n-1}^2 + \dots + q_{n-1}^{p-1}$ несложно построить обобщенную аддитивную цепочку длины $O(\log p)$, которая отличается от обычной тем, что вместо удвоений используются умножения на степени q_{n-1} (см., например, [19, 20]). Тогда Z при помощи этой цепочки вычисляется за $O(\log p)$ умножений и возведений в степень q_{n-1} в поле $GF(q_n)$.

Рассмотрим “длинное” представление поля $GF(q_n)$ (кольца $\mathbf{K}_{p,n}^h(x)$): в нем элементы представляются многочленами степени $p^{n+1} - 1$, а операции с ними выполняются по модулю $x^{p^{n+1}} - 1$. В таком представлении возведение в степень q_{n-1}^k выполняется с линейной сложностью. Действительно, запишем

$$X = f_0(x^p) + f_1(x^p)x + \dots + f_{p-1}(x^p)x^{p-1},$$

где $\deg f_i < p^n$. Тогда, поскольку $f_i(x^p) \in GF(q_{n-1})$, справедливо равенство

$$X^{q_{n-1}^k} = f_0(x^p) + f_1(x^p)y + \dots + f_{p-1}(x^p)y^{p-1},$$

где $y = x^{q_{n-1}^k}$. Многочлен $f_i(x^p)y^i$ по модулю $x^{p^{n+1}} - 1$ вычисляется простым циклическим сдвигом, и остается лишь выполнить сложение этих многочленов.

Таким образом, инвертирование в поле $GF(q_n)$ сводится к инвертированию в поле $GF(q_{n-1})$, а также $O(\log p)$ умножениям в поле $GF(q_n)$ и $O(p^{n+1} \log p)$ поразрядным операциям.

Переход от длинного представления к стандартному выполняется приведением по модулю многочлена $h(x^{p^n})$ — это, как указано выше, реализуется схемой сложности $O(p^{n+1} M(\deg h) / \deg h)$ и глубины $O(n \log p)$.

Из вышесказанного вытекает следующее утверждение.

Теорема 5. Пусть кольцо $\mathbf{K}_{p,n}^h$ при $\mathbf{K} = GF(2)$ является полем; напомним, что для этого необходимо и достаточно, чтобы $p^2 \nmid (2^{\deg h} - 1)$; пусть также $q_n = 2^{(\deg h)p^n}$ и $N = p^{n+1}$. Тогда в стандартном базисе поля $GF(q_n)$ можно реализовать инвертирование схемой сложности $O(\log p)M(N) = O(\log p)N \log N \log \log N$ и глубины $O(\log^2 N)$.

Доказательство. Для сложности $I(GF(q_n))$ и глубины $d_I(GF(q_n))$ схемы инвертирования в поле $GF(q_n)$ справедливы рекуррентные соотношения

$$\begin{aligned} I(GF(q_n)) &\leq O(\log p)M(N) + I(GF(q_{n-1})), \\ d_I(GF(q_n)) &\leq O(\log p) \log N + d_I(GF(q_{n-1})). \end{aligned}$$

Используя для сложности умножения оценки следствия 6 и оценки

$$\begin{aligned} I(GF(q_0)) &= O(\log p)p^2, \\ d_I(GF(q_0)) &= O(\log^2 p) \end{aligned}$$

в основании индукции (соответствующую схему можно построить методом аддитивных цепочек, см., например, [19]), получаем утверждение теоремы.

4.2. Случай $p = 3$

Получим теперь более точную оценку для сложности инвертирования в случае $\text{char } \mathbf{K} = 2$ и $p = 3$. В этом разделе считаем, что

$$q_n = 2^{2 \cdot 3^n}.$$

Воспользуемся формулами (9). Элемент $X \in \mathbf{K}_{3,n}(x) \cong GF(q_n)$ удобно представить в виде

$$X = X_0 + X_1x + X_2x^2, \quad X_i \in GF(q_{n-1});$$

при этом

$$X_i = f_i(x^3), \quad \deg f_i < 2 \cdot 3^{n-1}.$$

Аналогично запишем

$$Z = Z_0 + Z_1x + Z_2x^2.$$

Несложно проверить, что

$$q_{n-1} = 2^{2 \cdot 3^{n-1}} \equiv (3^n + 1) \pmod{3^{n+1}}.$$

Тогда

$$x^{q_{n-1}} = x^{3^n}x$$

в кольце $\mathbf{K}_{3,n}(x)$. Получаем, что

$$\begin{aligned} X^{q_{n-1}} &= X_0 + X_1x^{3^n}x + X_2x^{2 \cdot 3^n}x^2, \\ X^{q_{n-1}^2} &= X_0 + (X_1x^{3^n})x^{3^n}x + (X_2x^{2 \cdot 3^n})x^{2 \cdot 3^n}x^2 \\ &= X_0 + X_1x^{2 \cdot 3^n}x + X_2x^{3^n}x^2, \end{aligned}$$

откуда следует, с учетом того, что $x^{2 \cdot 3^n} + x^{3^n} = 1$,

$$\begin{aligned} Z &= (X_0^2 + X_1X_2x^3) + (X_0X_1 + X_2^2x^3)x + (X_0X_2 + X_1^2)x^2, \\ Y &= X_0Z_0 + (X_1Z_2 + X_2Z_1)x^3, \\ X^{-1} &= Z_0Y^{-1} + Z_1Y^{-1}x + Z_2Y^{-1}x^2. \end{aligned}$$

Из приведенных формул видно, что для вычисления Z , Y и затем X^{-1} достаточно выполнить в общей сложности три возведения в квадрат, четыре сложения, три умножения на x в кольце $\mathbf{K}_{3,n-1}(x)$, причем любое из действий выполняется со сложностью $O(3^n)$ и глубиной 1, а также вычислить семь произведений X_0X_1 , X_0X_2 , X_1X_2 , X_0Z_0 , $Y^{-1}Z_0$, $Y^{-1}Z_1$, $Y^{-1}Z_2$ и сумму произведений $X_1Z_2 + X_2Z_1$ в том же кольце.

Обозначим через $\Pi(q_n)$ и $d_\Pi(q_n)$ сложность и глубину схемы, вычисляющей 7 произведений и одну сумму двух произведений, именно, X_0X_1 , X_0X_2 , X_1X_2 , X_0Z_0 , $X_1Z_2 + X_2Z_1$, Z_0W , Z_1W , Z_2W в поле $GF(q_n)$ с условием, что входы Z_i можно использовать только после того, как вычислены первые три произведения, а вход W — после того, как вычислены X_0Z_0 и $X_1Z_2 + X_2Z_1$. Тогда для сложности $I(GF(q_n))$ и глубины $d_I(GF(q_n))$ инвертирования в стандартном базисе поля $GF(q_n)$ справедливо следующее утверждение.

Лемма 13. *Имеют место неравенства*

$$\begin{aligned} I(GF(q_n)) &\leq I(GF(q_{n-1})) + \Pi(q_{n-1}) + O(3^n), \\ d_I(GF(q_n)) &\leq d_I(GF(q_{n-1})) + d_\Pi(q_n) + O(1). \end{aligned}$$

Величина $\Pi(q_n)$ оценивается при помощи следующей леммы.

Лемма 14. *Справедливы оценки*

$$\begin{aligned} \Pi(q_n) &\leq 50\varphi(n)3^n + O(3^n n), \\ d_\Pi(q_n) &= O(n). \end{aligned}$$

Доказательство. Лемма доказывается аналогично теореме 3, только нужно учесть, что сомножители X_0, X_1, X_2, W используются по три раза, сомножители Z_0, Z_1, Z_2 — по два раза, а при вычислении суммы $X_1Z_2 + X_2Z_1$, в силу линейности ДПФ, сложение можно выполнить в пространстве Фурье-образов, и только затем выполняется обратное ДПФ. Поэтому вместо шести, как в теореме 3, выполняется 30 ДПФ порядка $3^{\lfloor n/2 \rfloor}$. Окончательно оценка сложности вытекает из соотношения

$$\begin{aligned} \Pi(q_n) &\leq 2 \cdot 3^{\lfloor n/2 \rfloor} \Pi(q_{\lfloor n/2 \rfloor}) + 30F_{\lfloor n/2 \rfloor}(3^{\lfloor n/2 \rfloor}) + O(3^n) \\ &\leq 2 \cdot 3^{\lfloor n/2 \rfloor} \Pi(q_{\lfloor n/2 \rfloor}) + 100\lfloor n/2 \rfloor 3^n + O(3^n). \end{aligned}$$

Для глубины справедливо соотношение

$$d_{\Pi}(q_n) \leq d_{\Pi}(q_{\lfloor n/2 \rfloor}) + O(n),$$

откуда, очевидно,

$$d_{\Pi}(q_n) = O(n).$$

Лемма доказана.

Из последних двух лемм вытекает следующее утверждение.

Теорема 6. Пусть $\text{char } \mathbf{K} = 2$. Тогда инвертирование в кольце $\mathbf{K}_{3,n}(x)$ можно реализовать схемой сложности $25\varphi(n)3^n + O(3^n n)$ и глубины $O(n^2)$.

Замечание 6. Если не предполагать, что $\text{char } \mathbf{K} = 2$, то для сложности можно указать оценку $32,5\varphi(n)3^n + O(3^n n)$ (см. замечание к теореме 3).

5. Быстрое умножение при помощи ДПФ простого порядка $p > 3$

В разделе 3 показано, что ДПФ порядка 3 в кольцах характеристики 2 почти так же эффективно для построения быстрых алгоритмов умножения, как и ДПФ порядка 2 в других кольцах. Возникает вопрос, могут ли быть полезны в этом отношении ДПФ других простых порядков p . В этом разделе мы покажем, что, во всяком случае, в некоторых кольцах $\mathbf{K}_{p,n}^h(x)$ умножение можно выполнять быстрее, чем троичным методом следствия 8, если опираться на эффективную реализацию ДПФ порядка $p > 3$. В качестве примеров рассмотрим кольца $\mathbf{K}_{5,n}(x)$ и $\mathbf{K}_{7,n}^h(x)$, где

$$h(x) = x^3 + x + 1.$$

5.1. ДПФ простого порядка

Построению эффективных схем для реализации ДПФ, в первую очередь, простых порядков над полями характеристики 2 посвящена специальная литература, см., например, [21, 22, 23, 24]; в [22] приводятся сведения о последних результатах. В указанных исследованиях сложность преобразований исчисляется в операциях сложения и умножения в основном поле. Для оптимизации по сложности схем, как правило, применяется компьютерный счет при каждом конкретном значении порядка ДПФ. При этом, в переисчисленных работах в первую очередь минимизируется число умножений, и только потом

— число сложений в алгоритмах с минимальным числом умножений. Такая расстановка приоритетов не всегда оправдана, ввиду того, что в алгоритмах ДПФ используются умножения на константы, чаще всего, на степени примитивного корня или на сумму двух степеней, сложность которых, как правило, не выше, чем у сложения.

Нас интересует построение схем ДПФ простого порядка p в кольце $\mathbf{K}_{p,0}^h(x)$, сложность и глубина которых исчисляется в операциях над полем $\mathbf{K}$. Такое ДПФ может быть реализовано со сложностью $(p-1)(p^2-2)$ тривиальным способом (все компоненты преобразования вычисляются независимо) или со сложностью $O(p^2 \log p \log \log p)$, если воспользоваться методом Райдера [13], сводящим ДПФ порядка p к циклической свертке порядка $p-1$.

Далее полагаем $\text{char } \mathbf{K} = 2$.

Пусть $p = 5$. В [22] указано, что ДПФ порядка 5 над полем $GF(2^m)$ можно выполнить за 5 умножений и 16 сложений в этом поле; детали алгоритма не разъясняются, что не позволяет указать битовую сложность в интересующем нас случае $m = 4$. Следующий способ является модификацией схемы из 6 умножений и 14 сложений в $\mathbf{K}_{5,0}(x)$, которая в пересчете на операции в $\mathbf{K}$ имеет сложность 72 и глубину 7.

Лемма 15. Пусть $\text{char } \mathbf{K} = 2$. Тогда ДПФ порядка 5 над кольцом $\mathbf{K}_{5,0}(x)$ можно реализовать схемой сложности 71 и глубины 6.

Доказательство. Обозначим

$$(f_0^*, \dots, f_4^*) = \text{ДПФ}_{5,\omega}(f_0, \dots, f_4), \quad \omega = x \in \mathbf{K}_{5,0}(x).$$

Воспользуемся формулами Герцля (см. [13])

$$\begin{aligned} f_0^* &= f_0 + f_1 + f_2 + f_3 + f_4, \\ f_1^* &= A_0 + A_1\omega, \\ f_4^* &= A_0 + A_1\omega^{-1}, \\ f_2^* &= A_2 + A_3\omega^2, \\ f_3^* &= A_2 + A_3\omega^{-2}, \\ A_0 &= f_0 + f_2 + (f_3 + f_4)(\omega + \omega^{-1}), \\ A_2 &= A_0 + (f_3 + f_4), \\ A_1 &= f_1 + f_4 + (f_2 + f_3)(\omega + \omega^{-1}), \\ A_3 &= A_1 + (f_2 + f_3). \end{aligned}$$

Пусть

$$\begin{aligned} f_1 + f_4 &= x_0 + x_1\omega + x_2\omega^2 + x_3\omega^3, \\ f_2 + f_3 &= y_0 + y_1\omega + y_2\omega^2 + y_3\omega^3, \end{aligned}$$

тогда

$$\begin{aligned} A_1\omega &= x_3 + y_0 + y_2 + y_3 + (x_0 + x_3 + y_1 + y_2)\omega + (x_1 + x_3 + y_0)\omega^2 \\ &\quad + (x_2 + x_3 + y_1 + y_2 + y_3)\omega^3, \\ A_1\omega^{-1} &= x_0 + x_1 + y_0 + y_1 + y_2 + (x_0 + x_2 + y_3)\omega + (x_0 + x_3 + y_1 + y_2)\omega^2 \\ &\quad + (x_0 + y_0 + y_1 + y_3)\omega^3, \end{aligned}$$

$$\begin{aligned}
A_3\omega^2 &= x_2 + x_3 + y_1 + (x_2 + y_0 + y_1 + y_2)\omega + (x_0 + x_2 + y_0 + y_2 + y_3)\omega^2 \\
&\quad + (x_1 + x_2 + y_0 + y_3)\omega^3, \\
A_3\omega^{-2} &= x_1 + x_2 + y_0 + y_3 + (x_1 + x_3 + y_0 + y_1 + y_3)\omega + (x_1 + y_1 + y_2 + y_3)\omega^2 \\
&\quad + (x_0 + x_1 + y_2)\omega^3.
\end{aligned}$$

Указанные четыре выражения можно вычислить с помощью 20 операций сложения в кольце $\mathbf{K}$ следующей схемой глубины 4 относительно x_i и y_i :

$$\begin{aligned}
u_0 &= x_0 + y_2, & u_1 &= x_1 + y_0, & u_2 &= x_2 + y_3, & u_3 &= x_3 + y_1, & v &= x_3 + y_0 + y_2, \\
l_1 &= u_0 + u_3, & l_2 &= u_1 + u_2, & l_3 &= u_0 + x_1, & l_4 &= u_1 + x_3, & l_5 &= u_2 + x_0, \\
l_6 &= u_3 + x_2, & l_7 &= l_1 + l_4, & l_8 &= l_1 + l_5, & l_9 &= l_2 + l_3, & l_{10} &= l_2 + l_6, \\
l_{11} &= v + y_3, & l_{12} &= l_1 + l_{11}, & l_{13} &= v + l_6, & l_{14} &= v + l_{10}; \\
A_1\omega &= l_{11} + l_1\omega + l_4\omega^2 + l_8\omega^3, & A_1\omega^{-1} &= l_7 + l_5\omega + l_1\omega^2 + l_{12}\omega^3, \\
A_3\omega^2 &= l_6 + l_{13}\omega + l_9\omega^2 + l_2\omega^3, & A_3\omega^{-2} &= l_2 + l_{10}\omega + l_{14}\omega^2 + l_3\omega^3.
\end{aligned}$$

Заметим, что A_0, A_2, f_0^* вычисляются с помощью 6 операций сложения в кольце $\mathbf{K}_{5,0}(x)$ и одной операции умножения на константу $\omega + \omega^{-1}$ сложности 3 и глубины 2 с общей глубиной 5. Для вычисления $f_1^*, f_2^*, f_3^*, f_4^*$ остается выполнить 4 сложения в $\mathbf{K}_{5,0}(x)$ по приведенным выше формулам с дополнительной глубиной 1. Лемма доказана.

Рассмотрим случай $p = 7$. Методом из [23] ДПФ порядка 7 реализуется при помощи 24 сложений и 6 умножений на константы в $\mathbf{K}[x]/(x^3 + x^2 + 1)$. Если учесть, что сложение в $\mathbf{K}[x]/(x^3 + x^2 + 1)$ выполняется за 3 сложения в $\mathbf{K}$, а каждое из умножений — за 2, то общую сложность ДПФ можно оценить как 84 операции в $\mathbf{K}$. Глубина при этом большая, так как при вычислении линейных форм используются преимущественно линейные переходы (этот термин из теории аддитивных цепочек означает, что очередная операция использует результат предыдущей операции). Сложность следующего способа можно указать как 23 сложения и 8 умножений в $\mathbf{K}_{7,0}^h(x) = \mathbf{K}[x]/(x^3 + x + 1)$, но она может быть еще уменьшена при пересчете в операции над $\mathbf{K}$.

Лемма 16. Пусть

$$\text{char } \mathbf{K} = 2, \quad h(x) = x^3 + x + 1.$$

Тогда ДПФ порядка 7 над кольцом $\mathbf{K}_{7,0}^h(x)$ можно реализовать схемой сложности 73 и глубины 7.

Доказательство. Обозначим

$$(f_0^*, \dots, f_6^*) = \text{ДПФ}_{7,\omega}(f_0, \dots, f_6),$$

где $\omega = x \in \mathbf{K}_{7,0}^h(x)$. Несложно проверить, что

$$\begin{aligned}
f_0^* &= f_0 + \dots + f_6, \\
f_1^* &= C_0 + \omega(A_0 + B_0) + \omega^2 A_0, & f_2^* &= C_0 + \omega A_0 + \omega^2 B_0, \\
f_4^* &= C_0 + \omega B_0 + \omega^2(A_0 + B_0), & f_3^* &= C_1 + \omega B_1 + \omega^2(A_1 + B_1), \\
f_5^* &= C_1 + \omega A_1 + \omega^2 B_1, & f_6^* &= C_1 + \omega(A_1 + B_1) + \omega^2 A_1,
\end{aligned}$$

где

$$\begin{aligned} C_0 &= f_0 + f_3 + f_5 + f_6, & C_1 &= f_0 + f_1 + f_2 + f_4, \\ A_0 &= f_2 + f_4 + f_5 + f_6, & A_1 &= f_1 + f_2 + f_3 + f_5, \\ B_0 &= f_1 + f_2 + f_3 + f_6, & B_1 &= f_1 + f_4 + f_5 + f_6. \end{aligned}$$

Вычисления состоят из двух этапов. На первом этапе реализуются A_i , B_i , C_i и f_0^* схемой из 13 сложений в $\mathbb{K}_{7,0}^h(x)$, в которой f_0^* вычисляется на глубине 4, а остальные выходы — на глубине 3. Порядок вычислений следующий: $f_1 + f_2$, $f_3 + f_5$, $f_2 + f_4$, $f_5 + f_6$, A_0 , A_1 , $f_1 + f_2 + f_4$, $f_3 + f_5 + f_6$, C_0 , C_1 , $B_0 = A_1 + (f_5 + f_6)$, $B_1 = A_0 + (f_1 + f_2)$, $f_0^* = C_0 + (f_1 + f_2 + f_4)$.

Далее заметим, что f_1^* , f_2^* , f_4^* выражаются через A_0 , B_0 , C_0 теми же формулами, что f_6^* , f_5^* , f_3^* через A_1 , B_1 , C_1 . Поэтому достаточно описать схему вычисления f_1^* , f_2^* , f_4^* .

Для представления элементов кольца используем стандартный базис $\{1, \omega, \omega^2\}$. Пусть

$$\begin{aligned} A_0 &= a_0 + a_1\omega + a_2\omega^2, \\ B_0 &= b_0 + b_1\omega + b_2\omega^2, \\ C_0 &= c_0 + c_1\omega + c_2\omega^2, \\ f_i^* &= f_{i0} + f_{i1}\omega + f_{i2}\omega^2. \end{aligned}$$

Тогда коэффициенты представления f_1^* , f_2^* , f_4^* задаются линейными формами:

$$\begin{aligned} f_{10} &= c_0 + a_1 + b_1 + b_2, \\ f_{11} &= c_1 + a_1 + a_2 + b_0 + b_1, \\ f_{12} &= c_2 + a_0 + a_2 + b_0 + b_1 + b_2, \\ f_{20} &= c_0 + a_2 + b_1, \\ f_{21} &= c_1 + a_0 + a_2 + b_1 + b_2, \\ f_{22} &= c_2 + a_1 + b_0 + b_2, \\ f_{40} &= c_0 + a_1 + a_2 + b_2, \\ f_{41} &= c_1 + a_0 + a_1 + b_0 + b_2, \\ f_{42} &= c_2 + a_0 + a_1 + a_2 + b_1. \end{aligned}$$

Данная система линейных форм может быть вычислена со сложностью 17 и глубиной 4. Порядок вычислений следующий: в каждой строчке с глубиной 2 вычисляется по одной компоненте α_j вида $f_{ij} - c_j$:

$$\begin{aligned} \alpha_0 &= a_2 + b_1, \\ \alpha_1 &= (a_2 + b_1) + (a_0 + b_2), \\ \alpha_2 &= (a_1 + b_2) + b_0. \end{aligned}$$

На глубине 3 вычисляется еще по одной подобной компоненте β_j :

$$\begin{aligned} \beta_0 &= (a_1 + b_2) + b_1, \\ \beta_1 &= \alpha_2 + a_0, \\ \beta_2 &= \alpha_1 + b_0. \end{aligned}$$

Окончательно заметим, что

$$\{f_{1j}, f_{2j}, f_{4j}\} = \{c_j + \alpha_j, c_j + \beta_j, (c_j + \alpha_j) + \beta_j\}.$$

Лемма доказана.

Оценки лемм 15 и 16, по всей видимости, не лучшие из возможных, однако для наших целей достаточны.

5.2. ДПФ порядка p^k

ДПФ порядка p^k в кольце $\mathbf{K}_{p,n}^h(x)$ сводится к ДПФ того же порядка в кольце $\mathbf{K}_{p,k-1}^h(x)$. Справедлив следующий аналог следствия 3.

Лемма 17. Пусть $1 \leq k \leq n + 1$. ДПФ порядка p^k над кольцом $\mathbf{K}_{p,n}^h(x)$ реализуется при помощи p^{n+1-k} ДПФ порядка p^k над кольцом $\mathbf{K}_{p,k-1}^h(x)$, выполняемых параллельно.

Доказательство. Согласно лемме 5, подстановка $x^{p^{n+1-k}} = y$ задает изоморфизм колец $\mathbf{K}_{p,n}^h(x)$ и $\mathbf{K}_{p,k-1}^h(y)[x]/(x^{p^{n+1-k}} - y)$. Рассмотрим второе кольцо: в нем y является примитивным корнем порядка p^k . Тогда преобразование ДПФ $_{p^k,y}$ не зависит от x и выполняется независимо при каждой степени x . Лемма доказана.

Обозначим через Φ_k сложность ДПФ порядка p^k в кольце $\mathbf{K}_{p,k-1}^h(x)$. Тогда, согласно лемме 3, в которой полагаем $S = p$ и $T = p^k$, и лемме 17, получаем оценку

$$\Phi_{k+1} \leq p^2 \Phi_k + p^{2k} \Phi_1 + \sum_{j=1}^{p-1} \sum_{t=1}^{p^k-1} M(x^{jt}, k), \quad (10)$$

в которой через $M(x^{jt}, k)$ обозначена сложность умножения на x^{jt} в $\mathbf{K}_{p,k}^h(x)$.

Оценивая величину $M(x^{jt}, k)$ при помощи леммы 7, нетрудно получить оценку сложности ДПФ порядка p^k в кольце $\mathbf{K}_{p,k-1}^h(x)$, $\text{char } \mathbf{K} = 2$. В интересующем нас случае $p = 5$ рекуррентное соотношение (10) разрешается точно. Используя лемму 7, переписываем (10) как

$$\Phi_{k+1} \leq 25\Phi_k + 5^{2k}\Phi_1 + 3 \sum_{j=1}^4 \sum_{t=1}^{5^k-1} \min\{jt, 5^k\}. \quad (11)$$

Двойную сумму в правой части вычислим как $\Sigma_1 + \Sigma_2 + \Sigma_3 + \Sigma_4$, где

$$\Sigma_j = \sum_{t=1}^{5^k-1} \min\{jt, 5^k\},$$

именно,

$$\Sigma_1 = \sum_{t=1}^{5^k-1} t = 5^k(5^k - 1)/2,$$

$$\Sigma_2 = 2 \sum_{t=1}^{(5^k-1)/2} t + 5^k(5^k - 1)/2 = (5^k - 1)(3 \cdot 5^k + 1)/4,$$

$$\Sigma_4 = 4 \sum_{t=1}^{(5^k-1)/4} t + 5^k \cdot \frac{3}{4}(5^k - 1) = (5^k - 1)(7 \cdot 5^k + 3)/8,$$

$$\Sigma_3 = 3 \sum_{t=1}^{\lfloor (5^k-1)/3 \rfloor} t + 5^k \left(5^k - 1 - \left\lfloor \frac{5^k - 1}{3} \right\rfloor \right) = (5^k - 1)(5^{k+1} + 2)/6.$$

Окончательно получаем, что

$$\sum_{j=1}^4 \sum_{t=1}^{5^k-1} \min\{jt, 5^k\} = \frac{71}{24} \cdot 5^{2k} - 2 \cdot 5^k - \frac{23}{24}.$$

Подставляя значение суммы в (11) и решая рекуррентное соотношение стандартным образом, например, решение можно искать в виде

$$\Phi_k = (ak + b)5^{2k} + c5^k + d,$$

получаем, что

$$\Phi_k \leq \left(\Phi_1 + \frac{71}{8} \right) k 5^{2k-2} - \frac{403}{192} \cdot 5^{2k-1} + \frac{3}{2} \cdot 5^{k-1} + \frac{23}{192}.$$

Лемма 15 дает оценку $\Phi_1 \leq 71$. Тогда, с учетом леммы 17, из доказанного вытекает следующее утверждение.

Лемма 18. Пусть $\text{char } \mathbf{K} = 2$. ДПФ порядка 5^k над кольцом $\mathbf{K}_{5,n}(x)$, где $k \leq n+1$, может быть выполнено схемой сложности $79\frac{7}{8}k5^{n+k-1} - \frac{403}{192} \cdot 5^{n+k} + \frac{3}{2} \cdot 5^n + \frac{23}{192} \cdot 5^{n-k+1}$ и глубины $7k - 1$.

Оценка для глубины следует из структуры схемы, описанной в лемме 3, и оценок глубины подсхем из лемм 7 и 15.

Аналогичным образом, исходя из (10), можно получить оценку сложности ДПФ порядка 7^k в кольце $\mathbf{K}_{7,n}^h(x)$, только вместо леммы 15 нужно использовать лемму 16, а вместо леммы 7 — следующую лемму.

Лемма 19. Пусть $\text{char } \mathbf{K} = 2$. Умножение на x^m в кольце $\mathbf{K}_{7,n}^h(x)$, где

$$h(x) = x^3 + x + 1,$$

выполняется схемой сложности $\min\{|m|, 3 \cdot 7^n\}$ и глубины 2.

Доказательство. Лемма доказывается отдельно для каждого интервала значений $m \in [i7^n, (i+1)7^n]$. В качестве примера рассмотрим один случай: $2 \cdot 7^n < m \leq 3 \cdot 7^n$. Запишем равенство

$$x^m f(x) = a_2(x)x^m + a_3(x)x^{3 \cdot 7^n} + a_4(x)x^{4 \cdot 7^n} + a_5(x)x^{5 \cdot 7^n},$$

где

$$\deg a_2 = 3 \cdot 7^n - m - 1, \quad \deg a_3 = \deg a_4 = 7^n - 1, \quad \deg a_5 = m - 2 \cdot 7^n - 1.$$

Тогда в кольце $\mathbf{K}_{7,n}^h(x)$ выполнено равенство

$$x^m f(x) = (a_3 + a_5) + (a_3 + a_4 + a_5)x^{7^n} + (a_4 + a_5)x^{2 \cdot 7^n} + a_2 x^m.$$

Реализуя сумму в правой части, выполняем сложения $a_3 + a_5$ и $a_4 + a_5$ со сложностью $m - 2 \cdot 7^n$ каждое, $a_4 + a_2 x^{m-2 \cdot 7^n}$ со сложностью $3 \cdot 7^n - m$, и затем $a_3 + (a_4 + a_5)$ со сложностью 7^n .

Остальные случаи рассматриваются аналогично.

Теперь неравенство (10) можно переписать как

$$\Phi_{k+1} \leq 49\Phi_k + 7^{2k}\Phi_1 + \sum_{j=1}^6 \sum_{t=1}^{7^k-1} \min\{jt, 7^{k+1} - jt, 3 \cdot 7^k\}. \quad (12)$$

Вводя, как и выше, обозначение

$$\Sigma_j = \sum_{t=1}^{7^k-1} \min\{jt, 7^{k+1} - jt, 3 \cdot 7^k\},$$

можно установить, что

$$\begin{aligned} \Sigma_1 + \Sigma_2 + \Sigma_3 &= 6 \sum_{t=1}^{7^k-1} t = 3 \cdot 7^k (7^k - 1), \\ \Sigma_4 &= \frac{15}{8} \cdot 7^{2k} - \frac{3}{2} \cdot 7^k - \frac{9}{8} - \frac{3}{2} (k \bmod 2), \\ \Sigma_5 &= 2 \cdot 7^{2k} - 7^k - 1, \\ \Sigma_6 &= 6 \sum_{t=1}^{(7^k-1)/2} t + \frac{7^k-1}{6} (3 \cdot 7^k) + \sum_{t=(2 \cdot 7^k+1)/3}^{7^k-1} (7^{k+1} - 6t) \\ &= \frac{19}{12} \cdot 7^{2k} - \frac{1}{2} \cdot 7^k - \frac{17}{12}. \end{aligned}$$

Следовательно,

$$\sum_{j=1}^6 \sum_{t=1}^{7^k-1} \min\{jt, 7^{k+1} - jt, 3 \cdot 7^k\} \leq \frac{203}{24} \cdot 7^{2k} - 6 \cdot 7^k - \frac{85}{24}.$$

Используя эту оценку, мы приводим (12) к виду

$$\Phi_k \leq \left(\Phi_1 + \frac{203}{24} \right) k 7^{2k-2} - \frac{10981}{1152} \cdot 7^{2k-2} + 7^{k-1} + \frac{85}{1152}.$$

Теперь отсюда и из лемм 16 и 17 приходим к следующему утверждению.

Лемма 20. Пусть

$$h(x) = x^3 + x + 1$$

и $\text{char } \mathbf{K} = 2$. ДПФ порядка 7^k над кольцом $\mathbf{K}_{7,n}^h(x)$, где $k \leq n+1$, может быть выполнено схемой сложности $81 \frac{11}{24} k 7^{n+k-1} - \frac{10981}{1152} \cdot 7^{n+k-1} + 7^n + \frac{85}{1152} \cdot 7^{n-k+1}$ и глубины $9k - 2$.

5.3. Оценки сложности умножения

Умножение в кольце $\mathbf{K}_{p,n}^h(x)$ выполняется тем же способом, что и в теореме 3. При $n \geq 2$ кольцо $\mathbf{K}_{p,n}^h(x)$ представляется как расширение кольца $\mathbf{K}_{p,m}^h(y)$ (см. лемму 3):

$$\mathbf{K}_{p,n}^h(x) \cong \mathbf{K}_{p,m}^h(y)[x]/(x^{p^{n-m}} - y).$$

Пусть $m = \lceil n/2 \rceil$. Тогда умножение в $\mathbf{K}_{p,n}^h(x)$ сводится к обычному умножению многочленов степени не выше $p^{n-m} - 1$ над $\mathbf{K}_{p,m}^h(y)$ с последующим приведением по модулю $x^{p^{n-m}} - y$.

Для умножения используем шесть ДПФ порядка $N = p^{n-m} = p^{\lceil n/2 \rceil}$: три ДПФ для вычисления произведения по модулю $x^{p^{n-m}} - 1$, а три других — для вычисления произведения по модулю $x^{p^{n-m}} - \alpha^{p^{n-m}}$, где $\alpha = y^{2^{m-n}}$. Второе умножение сводится к подстановке $x = \alpha z$ и вычислению произведения по модулю $z^{p^{n-m}} - 1$, см. (7).

Вычисление любого из преобразований $x = \alpha z$ и $z = x/\alpha$ выполняется в кольце $\mathbf{K}_{p,n}^h(x)$ посредством N операций умножения на степени y в кольце $\mathbf{K}_{p,m}^h(y)$.

При $N = p^{n-m}$ справедливо соотношение

$$\alpha^N = y^{p^m} \neq 1,$$

значит, $\alpha^N - 1 \neq 0$. Тогда восстановление многочлена $f(x) \in \mathbf{K}_{p,m}^h(y)[x]$ степени не выше $2N - 2$ по остаткам f_1 и f_α от деления, соответственно, на $x^N - 1$ и $x^N - \alpha^N$ можно выполнить по формуле

$$f(x) = \frac{1}{\alpha^N - 1}((x^N - 1)f_\alpha - (x^N - \alpha^N)f_1). \quad (13)$$

В силу равенства

$$\alpha^{(p-1)N} + \dots + \alpha^N + 1 = y^{(p-1)p^m} + \dots + y^{p^m} + 1 = 0,$$

множитель $(\alpha^N - 1)^{-1}$ равен

$$-p^{-1}(\alpha^{(p-2)N} + 2\alpha^{(p-3)N} + \dots + (p-2)\alpha^N + p-1), \quad (14)$$

потому что

$$\begin{aligned} -p &= (\alpha^{(p-1)N} - 1) + \dots + (\alpha^N - 1) \\ &= (\alpha^N - 1)(\alpha^{(p-2)N} + 2\alpha^{(p-3)N} + \dots + (p-2)\alpha^N + p-1). \end{aligned}$$

Восстановление многочлена по формуле (13) может быть выполнено за $2N$ аддитивных операций, N умножений на $\alpha^N = y^{p^m}$ и $2N - 1$ умножений на $(\alpha^N - 1)^{-1}$ в кольце $\mathbf{K}_{p,m}^h(y)$. Приведение многочлена $f(x)$ степени не выше $2N - 2$ по модулю $x^N - y$ выполняется за $N - 1$ сложений и $N - 1$ умножений на y в кольце $\mathbf{K}_{p,m}^h(y)$.

Пусть $\text{char } \mathbf{K} = 2$. В качестве кольца $\mathbf{K}_{p,n}^h(x)$ далее рассматриваем кольцо $\mathbf{K}_{p,n}(x)$ или кольцо $\mathbf{K}_{7,n}^h(x)$, где

$$h(x) = x^3 + x + 1.$$

Сложность операции сложения и операции умножения на степень y в любом из колец $\mathbf{K}_{p,m}(y)$ и $\mathbf{K}_{7,m}^h(y)$ оценивается как $O(p^{m+1})$ (лемма 7 или лемма 19). Сложность умножения на константу (14) в этих кольцах можно грубо оценить при помощи леммы 7

или леммы 19 как $O(p^{m+2})$. Всего в описанном выше алгоритме сведения умножения в $\mathbf{K}_{p,n}^h(x)$ к умножениям в $\mathbf{K}_{p,m}^h(x)$ используется $O(N)$ операций каждого из перечисленных видов, поэтому их общую сложность можно оценить как $O(Np^{m+2}) = O(p^{n+2})$.

Пусть $F_n(k)$ — сложность, а $d_F(n, k)$ — глубина схемы ДПФ порядка p^k в $\mathbf{K}_{p,n}^h(x)$. Тогда для сложности $\mu(n)$ построенной схемы умножения в $\mathbf{K}_{p,n}^h(x)$ справедливо соотношение

$$\mu(n) \leq 2 \cdot p^{\lfloor n/2 \rfloor} \mu(\lceil n/2 \rceil) + 6F_{\lceil n/2 \rceil}(\lfloor n/2 \rfloor) + O(p^{n+2}), \quad (15)$$

а для глубины $d(n)$ построенной схемы при $p = O(1)$ можно выписать соотношение

$$d(n) \leq d(\lceil n/2 \rceil) + d_F(\lceil n/2 \rceil, \lfloor n/2 \rfloor) + O(1). \quad (16)$$

Если соотношение (15) переписывается в виде

$$\mu(n) \leq 2 \cdot p^{\lfloor n/2 \rfloor} \mu(\lceil n/2 \rceil) + 2Ap^n \lfloor n/2 \rfloor + O(p^n),$$

то, согласно лемме 12,

$$\mu(n) \leq A\varphi(n)p^n + (\mu(1) + O(1))2^{\lceil \log_2 n \rceil} p^n.$$

Если

$$d_F(n, k) \leq Ck + O(1),$$

то из (16) следует, что

$$d(n) \leq Cn + O(\log n).$$

В случае кольца $\mathbf{K}_{5,n}(x)$ можно положить $A = 47\frac{37}{40}$ и $C = 7$, используя лемму 18, а в случае кольца $\mathbf{K}_{7,n}^h(x)$ лемма 20 позволяет выбрать $A = 34\frac{51}{56}$ и $C = 9$. Тем самым, доказана следующая теорема.

Теорема 7. Пусть

$$\text{char } \mathbf{K} = 2, \quad h(x) = x^3 + x + 1.$$

- (i) Умножение в кольце $\mathbf{K}_{5,n}(x)$ реализуется схемой сложности $47\frac{37}{40} \cdot 5^n n(\log_2 n + O(1))$ и глубины $7n + O(\log n)$.
- (ii) Умножение в кольце $\mathbf{K}_{7,n}^h(x)$ реализуется схемой сложности $34\frac{51}{56} \cdot 7^n n(\log_2 n + O(1))$ и глубины $9n + O(\log n)$.

Заметим, что из теоремы выше следует, что сложность умножения многочленов над кольцом $\mathbf{K}$ характеристики 2 суммарной степени $N - 1$ при $N = 4 \cdot 5^n$ асимптотически не превосходит $5,17N \log_2 N \log_2 \log N$, а при $N = 3 \cdot 7^n$ асимптотически не превосходит $4,15N \log_2 N \log_2 \log N$.

6. Пример последовательности полей с быстрым умножением

Конструкция, представленная в теореме 3 и разделе 5.3, позволяет строить быстрые схемы умножения не только для полей порядка $2^{(\text{ord}_p 2)p^n}$. В целом, хорошие оценки можно получать для последовательности полей $\mathbf{K}[x]/(h(x^{3^n}))$, где $h(x)$ — малочлен и x — примитивный корень порядка $m3^{n-k}$ в кольце $\mathbf{K}[x]/(h(x^{3^n}))$, при этом $k = o(n)$.

В качестве примера такой последовательности можно указать кольца

$$\mathbf{K}_{15,m,n}^h(x) = \mathbf{K}[x]/(h(x^{3^n 5^m})),$$

где

$$h(x) = x^4 + x + 1, \quad m \ll n.$$

При $\mathbf{K} = GF(2)$ кольцо $\mathbf{K}_{15,m,n}^h(x)$ является полем $GF(2^{4 \cdot 3^n 5^m})$; в этом можно убедиться при помощи теоремы 2.47 из [16]. Элемент x является примитивным корнем степени $3^{n+1}5^{m+1}$ в кольце $\mathbf{K}_{15,m,n}^h(x)$.

Элементы кольца $\mathbf{K}_{15,m,n}^h(x)$, иными словами, многочлены по модулю $x^{4N} + x^N + 1$, где $N = 3^n 5^m$, удобно представить в виде $a_0(x) + x^{5N} a_1(x)$, $\deg a_i < 2N$. Это позволяет оптимизировать ДПФ порядка 3, которые дают основной вклад в сложность умножения.

Фактически, представление имеет вид $a_0 + \sqrt[3]{1} \cdot a_1$, что позволяет частично перенести реализации ДПФ из раздела 3. Например, справедлив аналог частного случая леммы 8: преобразование

$$\text{ДПФ}_{3,\xi}[\mathbf{K}_{15,m,n}^h(x)](\gamma_0, x^{m_1} \gamma_1, x^{m_2} \gamma_2), \quad m_1, m_2 \in \{\pm 5N\}, \quad (17)$$

реализуется со сложностью $20N$, то есть со сложностью пяти сложений в $\mathbf{K}_{15,m,n}^h(x)$ (доказательство леммы 8 в этом случае проходит без изменений).

Пусть $v(k)$ — минимум из сложностей умножения на x^k , $x^{\pm 5N+k}$ в $\mathbf{K}_{15,m,n}^h(x)$. Результат вычисления $v(k)$ изображен на рис. 1, k приведено к отрезку $[0, 5N]$.

При реализации ДПФ порядка 3^k методом леммы 3, возникающие в процессе вычислений ДПФ порядка 3 с аргументами γ_0 , $x^{m_1} \gamma_1$, $x^{m_2} \gamma_2$ удобно сводить к преобразованиям (17) домножением на подходящие степени x , минимизируя сложность таких умножений.

Рекуррентное соотношение для сложности $F(3^{k+1})$ ДПФ порядка 3^{k+1} над $GF(2^{4N})$ имеет вид

$$\begin{aligned} F(3^{k+1}) &\leq 3^k F(3) + 3F(3^k) + \sum_{j=1}^2 \sum_{t=1}^{3^k-1} v\left(\frac{5N}{3^k} jt\right) \\ &= 3^k F(3) + 3F(3^k) + 2 \sum_{t=1}^{3^k-1} v\left(\frac{5N}{3^k} t\right), \end{aligned}$$

где через $F(3)$ обозначается сложность преобразования (17).

Последнюю сумму можно приближенно (допуская ошибку в остаточном члене) оценить $3^k/(5N)$ -й частью площади фигуры под графиком; эта площадь равна $14\frac{1}{4}N^2$. Получаем, что

$$F(3^{k+1}) \lesssim 3F(3^k) + (20 + 5,7)3^k N,$$

Рис. 1.

откуда

$$F(3^k) \lesssim \frac{257}{30} k 3^k N.$$

Как следствие, применяя стандартную аргументацию, подобную проведенной в разделе 5.3, для сведения умножения в $\mathbf{K}_{15,m,n}^h(x)$ к умножению в $\mathbf{K}_{15,m,\lceil n/2 \rceil}^h(x)$, для сложности умножения двоичных многочленов по модулю $x^{4N} + x^N + 1$, где $N = 3^n 5^m$ и $m = o(\log n)$, можно вывести верхнюю оценку $(6,425 + o(1))4N \log_3 N \log_2 \log N$.

7. Умножение над произвольным кольцом

Стратегию умножения многочленов над кольцом $\mathbf{K}$, в котором необратимы двойка и тройка, указывает метод Кантора–Калтофена (см. [15]). Способом теорем 2 и 3, лишь заменяя обратные преобразования $\text{ДПФ}_{N,\xi}^{-1}$ ненормированными преобразованиями $\text{ДПФ}_{N,\xi-1}$, вычисляем “почти произведения”

$$\begin{aligned} 2^{N_1} fg &= 2^{N_1} fg \bmod (x^{2^{n_1}} + 1), \\ 3^{N_2} fg &= 3^{N_2} fg \bmod (x^{2 \cdot 3^{n_2}} + x^{3^{n_2}} + 1) \end{aligned}$$

при подходящих $n_i, N_i \in \mathbf{N}$, где f, g — перемножаемые многочлены. Окончательно произведение fg можно вычислить как $q2^{N_1} fg + s3^{N_2} fg$, где q, s — коэффициенты Безу, иными словами, $q2^{N_1} + s3^{N_2} = 1$.

Отталкиваясь от оценок теоремы 2 и замечания к теореме 3, для сложности умножения многочленов суммарной степени $N - 1$ методом Кантора–Калтофена можно получить оценку $(C + o(1))N \log_2 N \log_2 \log_2 N$, где $C = 3 + 6,5/\log_2 3 \approx 7,1$.

Список литературы

1. Schönhage A., Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf.* (1977) 7, 395–398.

2. Von zur Gathen J., Gerhard J., *Modern computer algebra*. Cambridge University Press, Cambridge, 1999.
3. Mateer T., *Fast Fourier algorithms with applications*, PhD Thesis. Clemson Univ., 2008.
4. Schönhage A., Schnelle Berechnung von Kettenbruchentwicklungen. *Acta Inf.* (1971) **1**, 139–144.
5. Strassen V., The computational complexity of continued fractions. *SIAM J. Comput.* (1983) **12**, 1–27.
6. Afanassiev V. B., Davydov A. A., Finite field tower: iterated presentation and complexity of arithmetic. *Finite Fields Appl.* (2002) **8**, 216–232.
7. Baktir S., Sunar B., Optimal tower fields. *IEEE Trans. Comput.* (2004) **53**, 1231–1243.
8. Бурцев А. А., Гашков И. Б., Гашков С. Б., О сложности булевых схем для арифметики в некоторых башнях конечных полей. *Вестник Московского университета, Сер. I: Математика, механика* (2006), № 5 10–16.
9. Гашков С. Б., Сергеев И. С., О сложности и глубине схем для умножения и инвертирования в некоторых полях $GF(2^n)$. *Вестник Московского университета, Сер. I: Математика, механика* (2009), № 4 3–7.
10. Гашков С. Б., Сергеев И. С., Алгоритмы быстрого преобразования Фурье. В сб.: *Дискретная математика и ее приложения*, V. ИПМ РАН, Москва, 2009, с. 3–23.
11. Itoh T., Tsujii S., A fast algorithm for computing multiplicative inverses in $GF(2^n)$ using normal basis. *Inf. Comput.* (1988) **78**, 171–177.
12. Cooley J. W., Tukey J. W., An algorithm for the machine calculation of complex Fourier series. *Math. Comput.* (1965) **19**, 297–301.
13. Блейхут Р., *Быстрые алгоритмы цифровой обработки сигналов*. Мир, Москва, 1989.
14. Good I. J., The interaction algorithm and practical Fourier analysis. *J. R. Statist. Soc. B* (1958) **20**, 361–372.
15. Cantor D., Kaltofen E., On fast multiplication of polynomials over arbitrary algebras. *Acta Inf.* (1991) **28**, 693–701.
16. Лидл Р., Нидеррайтер Х., *Конечные поля*, 1. Мир, Москва, 1988.
17. Шёнхаге А., Штрассен В., Быстрое умножение больших чисел. *Кибернетический сборник* (1973) **10**, 87–98.
18. Сергеев И. С., Регуляризация некоторых оценок сложности умножения многочленов. В сб.: *Материалы VII молодежной научной школы по дискретной математике и ее приложениям*, II. ИПМ РАН, Москва, 2009, с. 26–32.
19. Гашков С. Б., Сергеев И. С., О применении метода аддитивных цепочек к инвертированию в конечных полях. *Дискретная математика* (2006) **18**, №4, 56–72.
20. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. А., *Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы*. КомКнига, Москва, 2006.
21. Трифонов П. В., Федоренко С. В., Метод быстрого вычисления преобразования Фурье над конечным полем. *Проблемы передачи информации* (2003) **39**, №3, 3–10.
22. Wu X., Wagh M., Chen N., Wang I., Yan Z., Composite cyclotomic Fourier transforms with reduced complexities. *IEEE Trans. Signal Proc.* (2011) **59**, 2136–2145.
23. Costa E., Fedorenko S. V., Trifonov P. V., On computing the syndrome polynomial in Reed–Solomon decoder. *Eur. Trans. Telecomms* (2004) **15**, 337–342.
24. Захарова Т. Г., Вычисление преобразования Фурье в полях характеристики 2. *Проблемы передачи информации* (1992) **28**, №2, 62–77.