С. Б. Гашков, Замечания о быстром умножении многочленов, преобразовании Фурье и Хартли, *Дискрет. матем.*, 2000, том 12, выпуск 3, 124–153

DOI: 10.4213/dm340

Дискретная математика

том 12 выпуск 3 * 2000

УДК 519.7

Замечания о быстром умножении многочленов, преобразовании Фурье и Хартли

© 2000 г. С. Б. Гашков

Предложен быстрый алгоритм умножения действительных многочленов без использования комплексных чисел и быстрого преобразования Фурье. Эффективность этого алгоритма сравнивается с эффективностью алгоритма умножения, основанного на применении дискретного преобразования Хартли. Показано, что сложность преобразования Хартли совпадает с точностью до линейного слагаемого со сложностью преобразования Фурье, однако применение преобразования Хартли приводит к более эффективному алгоритму умножения.

Приведены аналоги упомянутых результатов для конечных полей. Показано, что в некоторых случаях мультипликативные константы в оценках сложности умножения многочленов и преобразований Фурье и Хартли над конечными полями меньше, чем аналогичные константы в случае поля действительных чисел.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 99–01–01175, и ФЦП «Интеграция», проект 473.

1. Введение

Стандартная схема быстрого умножения многочленов с действительными коэффициентами, основанная на циклической теореме о свертке (см., например, [1, 2]) такова: если нужно перемножить два многочлена степени $n-1$, то сначала применяют дискретное преобразование Фурье (ДПФ) порядка $2n$ к двум $2n$-мерным векторам, образованным коэффициентами многочленов и дополненным каждый n нулями, потом полученные два $2n$-мерных вектора покомпонентно перемножаются, и к полученному в результате $2n$-мерному вектору применяется обратное преобразование Фурье порядка $2n$ (подробное изложение имеется, например, в [3]). Для выполнения ДПФ порядка $2n$ требуется использование первообразного корня порядка $2n$ из единицы, поэтому необходим выход в поле комплексных чисел (или подходящего расширения поля коэффициентов перемножаемых многочленов в общем случае). Выполнение ДПФ в случае n, равного степени двойки, по существу эквивалентно вычислению методом деления пополам (называемого также разделяй и властвуй [3] или стратегия дублирования [2]) множества значений многочлена во всех n корнях порядка n из единицы, или, что равносильно, нахождению всех остатков от деления этого многочлена на линейные двучлены, получающиеся в результате разложения

на множители (в поле комплексных чисел) двучлена $x^n - 1$. Об этом можно прочитать, например, в [3], где этот метод применен также в более общей ситуации, а именно, в быстрой реализации вычисления системы остатков данного многочлена по данным взаимно простым модулям, и восстановления многочлена по эти остаткам (быстрый китайский алгоритм). Может быть, более ясно это изложено в последнем пункте [13], где показано, как при умножении многочленов можно вообще обойтись без ДПФ, заменив его применение использованием быстрого китайского алгоритма (при этом применение обратного преобразования Фурье маскируется под быструю интерполяцию многочлена в корнях порядка n из единицы и не используется ни формула для обратного ДПФ, ни теорема о циклической свертке).

Далее будет показано, как можно обойтись и без применения комплексных чисел.

Отметим, что в реальных вычислениях операции с комплексными числами заменяются на операции с действительными числами (комплексное умножение заменяется на 4 действительных умножения и 2 действительных сложения-вычитания или на 3 умножения и 5 сложений-вычитаний, а в случае умножения на константу число сложений-вычитаний может быть уменьшено до 3, см. [2]), и сложность комплексного преобразования Фурье F_n обычно оценивают числом действительных операций, необходимых для его вычисления. В общем случае наилучшие оценки имеют вид $F(n) = O(n \log n)$, алгоритмы, для которых она достигается, называются алгоритмами быстрого преобразования Фурье (БПФ).

Уменьшение константы в знаке O имеет прикладной интерес, поэтому найдено большое количество разнообразных алгоритмов БПФ (см., например, [2, 4, 8]). Обычно лучшие константы получаются при $n = 2^k$. Наилучшая известная константа в этом случае равна 4, она достигается на нескольких алгоритмах, например, так называемый split-radix алгоритм требует $n(k-3)+4$ умножений (во всех алгоритмах БПФ обычно используются только умножения на заранее вычисленные константы, как правило по модулю не превосходящие единицу) и $3n(k-1)+4$ сложений. Если БПФ применяется к действительному вектору, то число операций сокращается вдвое (см., например, [2, 4]). Так как именно эта ситуация возникает в двух БПФ порядка $2n$, выполняемых в указанном выше алгоритме умножения, его сложность $M(n)$ можно оценить как $4F(2n)+O(n)$, что в случае $n = 2^k$ дает оценку $16n \log n + O(n)$.

В общем случае асимптотически оценка остается такой же. Для ее получения выбираем $m = 2^k 3^l$ так, чтобы $n \leqslant m = n(1+\varepsilon_n)$, где $\varepsilon_n \to 0$, $k \to \infty$ (пользуясь равномерной распределенностью по модулю единица последовательности $\{n \log_2 3\}$), потом сводим задачу к умножению многочленов степени $m-1$, а для БПФ порядка m применяем комбинацию алгоритма Гуда–Томаса (см., например, [2]), произвольного БПФ порядка 3^l и указанного выше БПФ порядка 2^k. Отметим, что в отличие от оценки F_n оценку $M(n)$ обычно приводят в виде $O(n \log n)$, не уточняя мультипликативную константу, иногда отмечая, как в [8], что она порядка 20 и поэтому алгоритмы быстрого умножения непрактичны при небольших n.

Далее мы излагаем метод быстрого умножения многочленов с действительными коэффициентами, не использующий ни преобразования Фурье, ни вообще комплексных чисел, как в реализации алгоритма, так и в его обосновании. В этом алгоритме легко заметить использование модулярной арифметики, также как и в [13], но в его обосновании не используется китайская теорема об остатках. Отметим, что если все же применять китайскую теорему и не стремиться получить наилучшую константу, то следующее далее изложение можно было бы значительно сократить (хотя оно и так не слишком длинное, если учесть его почти полную замкнутость в себе).

Как указал в [10] А. А. Карацуба, идея возможности применения к быстрому умножению модулярной арифметики и китайской теоремы об остатках высказывалась А. Н. Колмогоровым в начале шестидесятых годов.

Излагаемый далее алгоритм использует идею алгоритма Герцеля (см., например, [2]) для вычисления значений тригонометрических многочленов (который также применяется к вычислению ДПФ, но дает лишь квадратичную оценку сложности), но приводит к лучшей, в сравнении с последним, оценке числа выполняемых операций благодаря применению метода деления пополам А. А. Карацубы [9], имеющей вид

$$M(n) = \frac{27}{2} n \log_2 n + 11.$$

Кроме этого, далее будет показано, как можно применить для еще более быстрого умножения действительных многочленов дискретное преобразование Хартли (ДПХ). При этом все его свойства будут выведены из свойств ДПФ. Точнее, будет показано, что сложность ДПХ отличается от сложности ДПФ лишь на линейное слагаемое (поэтому не вполне понятно, зачем вообще для ДПХ предлагаются во многочисленных статьях разнообразные алгоритмы быстрого вычисления, так как, вероятно, любой из них можно получить из соответствующего алгоритма БПФ), и для сложности умножения многочленов справедлива оценка

$$\begin{aligned} M(n) &= 3F(2n) + O(n) \\ &= 6F(n) + O(n) \\ &= 12n \log_2 n + O(n). \end{aligned}$$

Если же для умножения действительных многочленов применять комплексные операции (включая операцию сопряжения), то оценка сложности принимает вид

$$M(n) = \frac{9}{2} n \log_2 n + O(n).$$

С этой точки зрения ДПХ можно рассматривать как алгебраический трюк, по существу нужный лишь для ускорения умножения действительных многочленов.

В конце статьи рассмотрены некоторые вопросы о быстром умножении многочленов, БПФ и БПХ в конечных полях. Подобные вопросы представляют интерес для теории кодирования, в которой иногда вместо ДПФ используют термин преобразование Фурье–Мэттсона–Соломона (ФМС). В частности, с помощью алгоритма БПФ с расщепленным основанием показано, что сложность умножения многочленов степени, меньшей $q/2$, над полем $\mathrm{GF}(q)$, где $q = 2^p - 1$ — простое число Мерсенна, оценивается как

$$\frac{93}{8} q \log_2 q + O(q),$$

а мультипликативная сложность как

$$\frac{9}{4} q \log_2 q + O(q).$$

Для сравнения оценка мультипликативной сложности умножения действительных многочленов степени n асимптотически равна $3n \log_2 n$.

Получены также некоторые оценки сложности БПФ порядка степени тройки в конечных полях. Везде под сложностью понимается число операций в рассматриваемом поле.

Вопросы, связанные с битовой сложностью, не рассматриваются. Отметим, что Шенхаге в [12] получил для битовой сложности умножения многочленов над полем GF(2) оценку, по порядку такую же, как оценка битовой сложности умножения целых чисел [11].

2. Алгоритм

В описании алгоритма с целью краткости будем всегда полагать, что числа α с индексами или без них равны 0 или 1, а обозначаемые иногда таким же образом векторы составлены только из 0 или 1. Пусть трехчлен

$$p(x) = x^n + ax^{n/2} + 1, \qquad |a| \leqslant 2,$$

и 2^{k+1} делит n. Введем обозначение

$$p_\alpha(x) = x^{n/2} + a_\alpha x^{n/4} + 1,$$

где

$$a_\alpha = (-1)^\alpha \sqrt{2 - a}, \qquad \alpha = 0, 1,$$

и заметим, что

$$\begin{aligned} p(x) &= x^n + ax^{n/2} + 1 = (x^{n/2} + 1)^2 - (2 - a)x^{n/2} \\ &= (x^{n/2} + 1)^2 - (\sqrt{2 - a}\, x^{n/4})^2 \\ &= (x^{n/2} + \sqrt{2 - a}\, x^{n/4} + 1)(x^{n/2} - \sqrt{2 - a}\, x^{n/4} + 1) \\ &= (x^{n/2} + a_\alpha x^{n/4} + 1)(x^{n/2} - a_\alpha x^{n/4} + 1) \\ &= p_0(x) p_1(x). \end{aligned}$$

Для любого вектора из нулей и единиц $\alpha = (\alpha_1, \ldots, \alpha_m)$, $m \leqslant k$, положим

$$p_\alpha(x) = p_{\alpha_1, \ldots, \alpha_m}(x) = (\ldots(p_{\alpha_1})_{\alpha_2} \ldots)_{\alpha_m}(x).$$

Индукцией по m легко проверить, что

$$p_\alpha(x) = x^{n/2^m} + a_\alpha x^{n/2^{m+1}} + 1,$$

где

$$\begin{aligned} a_\alpha = a_{\alpha_1, \ldots, \alpha_m} &= (-1)^{\alpha_1} \sqrt{2 - a_{\alpha_2, \ldots, \alpha_m}} \\ &= (-1)^{\alpha_1} \sqrt{2 + (-1)^{\alpha_2} \sqrt{2 + \ldots (-1)^{\alpha_{m-1}} \sqrt{2 + (-1)^{\alpha_m} \sqrt{2 - a}}}}, \end{aligned}$$

$|a_\alpha| \leqslant 2$ и при $m < k$ и любом $\alpha = (\alpha_1, \ldots, \alpha_m)$ справедливо разложение

$$p_\alpha(x) = p_{\alpha,0}(x) p_{\alpha,1}(x),$$

а при $m = k$ разложение

$$\begin{aligned} p(x) &= \prod_{\alpha_1, \ldots, \alpha_k} p_\alpha(x) \\ &= \prod_{\alpha_1, \ldots, \alpha_k} (x^{n/2^k} + a_\alpha x^{n/2^{k+1}} + 1). \end{aligned}$$

Заметим, хотя нам это далее не понадобится, что при $a = 0$ здесь неявно получено известное разложение двучлена $p(x) = x^n + 1$ на неприводимые квадратные множители,

$$x^n + 1 = \prod_{i=0}^{n/2-1} (x^2 - 2\cos(\pi(2i+1)/n)x + 1),$$

из которого, пользуясь формулой

$$x^{2n} - 1 = (x^n - 1)(x^n + 1),$$

легко получить следующее разложение двучлена $x^{2n} - 1$ на неприводимые множители над полем действительных чисел:

$$x^{2n} - 1 = \prod_{i=1}^{n} (x^2 - 2\cos(\pi i/n)x + 1).$$

Тригонометрические коэффициенты этого разложения у нас выражаются только с помощью арифметических операций и извлечения квадратного корня.

Действительно, индукцией по k можно показать, что разложение

$$\begin{aligned} x^n + 1 = p(x) &= \prod_{\alpha_1,\dots,\alpha_k} p_\alpha(x) \\ &= \prod_{\alpha_1,\dots,\alpha_k} (x^{n/2^k} + a_\alpha x^{n/2^{k+1}} + 1) \end{aligned}$$

имеет вид

$$x^n + 1 = \prod_{i=0}^{2^k-1} (x^{n/2^k} - 2\cos(\pi(2i+1)/2^{k+1})x^{n/2^{k+1}} + 1)$$

Для этого достаточно заметить, что при $a = 2\cos(\pi(2i+1)/2^k)$

$$x^{n/2^{k-1}} - ax^{n/2^k} + 1 = (x^{n/2^k} + \sqrt{2+a}\, x^{n/2^{k+1}} + 1)(x^{n/2^k} - \sqrt{2+a}\, x^{n/2^{k+1}} + 1),$$

и

$$\sqrt{2+a} = \sqrt{2 + 2\cos 2\varphi} = 2\cos\varphi,$$

где $\varphi = \pi(2i+1)/2^{k+1}$, $i < 2^{k-1}$.

Положим

$$f_\alpha = f \pmod{p_\alpha(x)}, \qquad \alpha = (\alpha_1, \dots, \alpha_k).$$

Тогда эту последовательность можно вычислить следующим образом:

$$\begin{aligned} f_{\alpha_1} &= f \pmod{p_{\alpha_1}(x)}, \\ f_{\alpha_1,\alpha_2} &= f_{\alpha_1} \pmod{p_{\alpha_1,\alpha_2}(x)}, \\ &\dots \\ f_{\alpha_1,\dots,\alpha_{k-1}} &= f_{\alpha_1,\dots,\alpha_{k-2}} \pmod{p_{\alpha_1,\dots,\alpha_{k-1}}(x)}, \\ &\dots \\ f_\alpha &= f_{\alpha_1,\dots,\alpha_{k-1}} \pmod{p_\alpha(x)}. \end{aligned}$$

Заметим, что для многочлена $f = f_0 + f_1 y + f_2 y^2 + f_3 y^3$ справедливо равенство

$$\begin{aligned} f &= f_3 y^3 + (f_2 - af_3)y^2 + af_3 y^2 + a(f_2 - af_3)y + f_3 y + f_2 - af_3 \\ &\quad + (f_1 - f_3 - a(f_2 - af_3))y + f_0 - (f_2 - af_3) \\ &= (f_3 y + f_2 - af_3)(y^2 + ay + 1) \\ &\quad + (f_1 - f_3 - a(f_2 - af_3))y + f_0 - (f_2 - af_3), \end{aligned}$$

откуда находим, что

$$f \pmod{y^2 + ay + 1} = f_0 - (f_2 - af_3) + (f_1 - f_3 - a(f_2 - af_3))y,$$

и значит, вычеты $f \pmod{y^2+ay+1}$ и $f \pmod{y^2-ay+1}$ можно вычислить, выполняя 6 операций сложения-вычитания и 3 операции умножения на фиксированный скаляр в следующей последовательности:

$$\begin{gathered} g_1 = f_0 - f_2, \qquad g_2 = af_3, \\ g_3, g_4 \coloneqq g_1 \pm g_2 = f_0 - (f_2 \pm af_3), \\ g_5 = (a^2 - 1)f_3, \quad g_6 = f_1 + g_5, \quad g_7 = af_2, \\ g_8, g_9 = g_6 \pm g_7 = (f_1 - f_3 \pm a(f_2 \pm af_3)). \end{gathered}$$

Восстановить многочлен f по вычетам

$$\begin{aligned} f_{00} + f_{01} y &= f \pmod{y^2 + ay + 1} \\ f_{10} + f_{11} y &= f \pmod{y^2 - ay + 1} \end{aligned}$$

можно, выполняя 6 операций сложения-вычитания и 5 операций умножения на фиксированный скаляр в следующей последовательности:

$$\begin{gathered} h_1 = f_{00} - f_{10}, \quad h_2 = \frac{h_1}{2a} = f_3, \quad h_3 = f_{11} - f_{01}, \quad h_4 = \frac{h_3}{2a} = f_2, \\ h_5 = f_{00} + f_{10}, \quad h_6 = h_5/2 = f_0 - f_2, \quad h_7 = h_6 + h_4 = f_0, \\ h_8 = f_{01} + f_{11}, \qquad h_9 = h_8/2 = f_1 + (a^2 - 1)f_3, \\ h_{10} = (a^2 - 1)h_2, \qquad h_{11} = h_9 - h_{10} = f_1, \end{gathered}$$

причем две из операций умножения (речь идет об умножении на $1/2$) очень быстро выполняются в двоичной системе, так как реализуются просто сдвигом, поэтому иногда ими можно пренебречь.

Можно, однако, и в чистом виде сэкономить эти операции, если восстанавливать не сам многочлен, а его удвоение, то есть многочлен $2f$. Тогда для его вычисления достаточно будет сделать следующие операции:

$$\begin{gathered} h_1 = f_{00} - f_{10}, \quad h_2 = h_1/a = 2f_3, \quad h_3 = f_{11} - f_{01}, \quad h_4 = h_3/a = 2f_2, \\ h_5 = f_{00} + f_{10} = 2(f_0 - f_2), \quad h_6 = h_5 + h_4 = 2f_0, \\ h_7 = f_{01} + f_{11} = 2(f_1 + (a^2 - 1)f_3), \\ h_8 = 2(a^2 - 1)h_2, \qquad h_9 = h_7 - h_8 = 2f_1. \end{gathered}$$

Заметим еще (хотя нам это не понадобится), что вычисление только одного вычета $f \pmod{y^2+ay+1}$ требует 6 операций:

$$g_1 = af_3, \qquad g_2 = g_1 - f_2 g_3 = f_1 + g_2 = f_0 - (f_2 - af_3),$$
$$g_4 = f_1 - f_3, \qquad g_5 = ag_2,$$
$$f_1 - f_3 - a(f_2 - af_3) = g_6 = g_5 + g_4.$$

Заменяя в предыдущем тексте переменную y на $x^{n/4}$ и многочлены f_i на многочлены степени, не большей $n/4-1$, получаем, что для многочлена

$$p(x) = x^n + ax^{n/2} + 1, |a| \leqslant 2,$$

где n кратно 4, и многочлена f степени, не большей $n-1$, вычеты

$$f \pmod{p_\alpha}, \qquad \alpha = 0,1$$

можно вычислить за $3n/2$ операций сложения-вычитания и $3n/4$ операций умножения на фиксированный скаляр, то есть всего за $9n/4$ операций, а по вычетам $f \pmod{p_\alpha}$, $\alpha = 0,1$ восстановить исходный многочлен f можно за $11n/4$ аналогичных операций, в числе которых будет $5n/4$ операций умножения на фиксированный скаляр, причем нетривиальных умножений только $3n/4$.

Заметим также, что многочлен $2f$ можно восстановить за $9n/4$ операций, в числе которых будет $3n/4$ операций умножения на фиксированный скаляр. Отметим еще, что один только вычет $f \pmod{p_\alpha}$ можно вычислить за $3n/2$ операций.

Пусть $p(x) = x^n + ax^{n/2} + 1$, $|a| \leqslant 2$, число 2^k делит n, а f — многочлен степени, не большей $n-1$. Обозначим $C[f,p,k]$ неветвящуюся программу (в более краткой терминологии — схему) вычисления всех вычетов

$$f_\alpha = f \pmod{p_\alpha(x)}, \qquad \alpha = (\alpha_1, \dots, \alpha_k),$$

и через $C(n,k)$ число операций над числами, требующихся для этого вычисления. Так как

$$f_\alpha = f_{\alpha_1} \pmod{(p_{\alpha_1}(x))_{\alpha_2,\dots,\alpha_k}},$$

схема вычисления $C[f,p,k]$ может быть составлена из схемы, вычисляющей

$$f_{\alpha_1} = f \pmod{p_{\alpha_1}(x)}, \qquad \alpha_1 = 0,1,$$

и двух схем $C[f_{\alpha_1}, p_{\alpha_1}, k-1], \alpha_1 = 0,1$, откуда следует рекурсивная оценка

$$C(n,k) \leqslant 2C(n/2, k-1) + 9n/4.$$

Так как $C(n,1) \leqslant 9n/4$, отсюда индукцией по k можно вывести, что

$$C(n,k) \leqslant 9nk/4,$$

причем оценка числа мультипликативных операций будет $3nk/4$.

Обозначим $C^{-1}[(f_\alpha), p, k]$ обратную схему восстановления f по заданным вычетам $f_\alpha = f \pmod{p_\alpha(x)}, \alpha = (\alpha_1, \dots, \alpha_k)$, и через $C^{-1}(n,k)$ число операций над числами, требующихся для этого вычисления.

Схема обратного восстановления $C^{-1}[(f_\alpha), p, k]$ может быть составлена из двух схем

$$C^{-1}[((f_{\alpha_1})_{\alpha_2,\dots,\alpha_k}), p_{\alpha_1}, k-1], \qquad \alpha_1 = 0, 1,$$

и схемы, восстанавливающей многочлен f по его известным вычетам

$$f_{\alpha_1} = f \pmod{p_{\alpha_1}(x)}, \qquad \alpha_1 = 0, 1,$$

откуда следует рекурсивная оценка

$$C^{-1}(n, k) \leqslant 2C^{-1}(n/2, k-1) + 11n/4,$$

а так как $C^{-1}(n, 1) \leqslant 11n/4$, отсюда индукцией по k можно вывести, что

$$C^{-1}(n, k) \leqslant 11nk/4,$$

причем оценка числа мультипликативных операций будет $5nk/4$, а количества нетривиальных среди них — $3nk/4$.

Заметим, что схема, восстанавливающая по заданным вычетам не сам многочлен f, а его кратное $2^k f$, может быть составлена только из $9nk/4$ операций, из которых мультипликативных операций будет $3nk/4$.

Допустим, что число 2^k делит n, многочлен $p(x) = x^n - 1$, а f — многочлен степени, не большей $n-1$. Обозначим $C_0[f, n, k]$ схему вычисления по f всех вычетов

$$f_\alpha = f \pmod{p_\alpha(x)}, \qquad \alpha = (\alpha_1, \dots, \alpha_k).$$

Так как тогда $p_0 = x^{n/2} - 1$, $p_1 = x^{n/2} + 1$, схему $C_0[f, n, k]$ можно составить из схемы, вычисляющей

$$f_{\alpha_1} = f \pmod{p_{\alpha_1(x)}}, \qquad \alpha_1 = 0, 1,$$

и двух схем $C[f_{\alpha_1}, p_{\alpha_1}, k-1]$, $\alpha_1 = 0, 1$, откуда следует рекурсивная оценка

$$C_0(n, k) \leqslant C_0(n/2, k-1) + \frac{9n}{8}(k-1) + n,$$

а так как $C_0(n, 1) \leqslant n$, применяя индукцию, отсюда выводим оценку

$$C_0(n, k) \leqslant \frac{9nk}{4} - \frac{5n}{2} + \frac{5n}{2^{k+1}}.$$

Пусть теперь $p(x) = x^{2n} - 1$, число 2^k делит n, а f— многочлен степени, не большей $n-1$. Обозначим $C[f, n, k]$ схему вычисления по многочлену f всех его вычетов

$$f_\alpha = f \pmod{p_\alpha(x)}, \qquad \alpha = (\alpha_1, \dots, \alpha_k).$$

Так как тогда $p_0 = x^n - 1$, $p_1 = x^n + 1$, $f = f_0 = f_1$, схема вычисления $C[f, n, k]$ может быть составлена из схем $C[f, p_\alpha, k-1]$, $\alpha = 0, 1$. Обозначим $C_k(n)$ число операций в схеме $C[f, n, k]$. Число операций в схеме $C[f, p_0, k-1] = C[f, n, k-1]$ равно $C_0(n, k-1)$, а в схеме $C[f, p_1, k-1]$ равно $C(n, k-1)$, значит,

$$\begin{aligned} C_k(n) &\leqslant C_0(n, k-1) + C(n, k-1) \\ &\leqslant \frac{9n(k-1)}{4} + \frac{9n(k-1)}{4} - \frac{5n}{2} + \frac{5n}{2^k} \\ &= \frac{9n(k-1)}{2} - \frac{5n}{2} + \frac{5n}{2^k} = \frac{9nk}{2} - 7n + \frac{5n}{2^k}. \end{aligned}$$

3. Оценка сложности

Оценим число операций $M(n)$, требующихся для вычисления произведения $h(x)$ двух многочленов f и g степеней, меньших n. Допустим, что 2^k делит n. Вначале вычислим все вычеты по модулям $p_\alpha(x)$, $\alpha = (\alpha_1, \dots, \alpha_k)$, где $p(x) = x^{2n} - 1$, для этого требуется

$$2C_k(n) = 9nk - 14n + \frac{5n}{2^{k-1}}$$

операций. Потом попарно перемножим эти вычеты и получим

$$h_\alpha = f_\alpha g_\alpha, \qquad \alpha = (\alpha_1, \dots, \alpha_k).$$

Число требующихся для этого операций равно $2^k M(2^{-k+1}n)$. Затем вычислим вычеты

$$r_\alpha = h_\alpha \pmod{p_\alpha(x)}, \qquad \alpha = (\alpha_1, \dots, \alpha_k).$$

Для этого требуется $2^k 3(2^{-k+2}n)/2 = 6n$ операций.

Заметим теперь, что

$$h(x) \pmod{p_\alpha(x)} = f(x)g(x) \pmod{p_\alpha(x)} = h_\alpha \pmod{p_\alpha(x)} = r_\alpha.$$

Так как степень $h(x)$ меньше $2n$, то для его восстановления по указанным остаткам требуется $C^{-1}(2n, k) \leqslant 11nk/2$ операций.

В результате получаем оценку

$$\begin{aligned} M(n) &\leqslant C_k(n) + 2^k M(2^{-k+1}n) + 6n + C^{-1}(2n, k) \\ &\leqslant 9nk - 14n + \frac{5n}{2^{k-1}} + 2^k M(2^{-k+1}n) + 6n + \frac{11nk}{2} \\ &= \frac{29nk}{2} - 8n + 2^k M(2^{-k+1}n) + \frac{5n}{2^{k-1}}. \end{aligned}$$

В частности, если $n = 2^k$, то

$$\begin{aligned} M(n) &\leqslant \frac{29}{2}nk - 8n + M(2)n + 10 \\ &= \frac{29}{2}nk - 2n + 10 = \frac{29}{2}n\log_2 n - 2n + 10. \end{aligned}$$

Если же восстанавливать не сам многочлен h, а $2^k h$, как было указано выше, а потом находить h с помощью $2n - 1$ умножений на 2^{-k}, то получим оценку

$$\begin{aligned} M(n) &\leqslant 9nk - 14n + \frac{5n}{2^{k-1}} + 2^k M(2^{-k+1}n) + 6n + \frac{9nk}{2} + 2n - 1 \\ &= \frac{27nk}{2} - 8n + 2^k M(2^{-k+1}n) + \frac{5n}{2^{k-1}} + 2n - 1, \end{aligned}$$

в частности, если $n = 2^k$, то

$$M(n) \leqslant \frac{27}{2}nk + 11 = \frac{27}{2}n\log_2 n + 11.$$

В общем случае выберем k так, чтобы

$$\frac{1}{2}\sqrt{\log_2 n} \leqslant 2^{-k+1}n < \sqrt{\log_2 n},$$

и увеличим n менее чем на 2^k так, чтобы n стало делиться на 2^k. Тогда

$$2^{-k+1}n \leqslant 2 + \lfloor\sqrt{\log_2 n}\rfloor,$$

откуда в силу очевидной монотонности функции $M(n)$ и соотношения $M(n) = O(n^2)$ находим, что

$$\begin{aligned} M(n) &\leqslant \frac{27}{2}nk - 6n + 2^k M(2^{-k+1}n) + \frac{5n}{2^{k-1}} \\ &= \frac{27}{2}nk + O(n\sqrt{\log_2 n}) \\ &= \frac{27}{2}n\log_2 n + O(n\sqrt{\log_2 n}). \end{aligned}$$

Теперь, если воспользоваться уже доказанным соотношением $M(n) = O(n\log_2 n)$, можно получить оценку

$$M(n) \leqslant \frac{27}{2}n\log_2 n + O(n\log_2\log_2 n).$$

Отметим, что оценка только числа мультипликативных операций имеет вид

$$\frac{9}{2}n\log_2 n + O(n\log_2\log_2 n).$$

В приведенных оценках мы пренебрегли (как обычно делается и в оценках БПФ) сложностью предварительного вычисления фиксированных (не зависящих от коэффициентов перемножаемых многочленов) констант из множества

$$a_\alpha = a_{\alpha_1,\ldots,\alpha_k} = (-1)^{\alpha_1}\sqrt{2 - a_{\alpha_2,\ldots,\alpha_{k-1}}}, \quad \alpha_i = 0,1, \quad 1 \leqslant i \leqslant k.$$

Кроме них, использовались также системы констант $1/a_\alpha$ и $2a_\alpha^2 - 2$. Заметим, что $a_\alpha^2 - 1 = 1 - a_{\alpha_2,\ldots,\alpha_{k-1}}$, поэтому для предварительного вычисления всех нужных констант достаточно $2n$ операций вычитания из единицы или двойки (эти операции выполняются быстрее, чем вычитание произвольных чисел), n операций умножения на 2 и n операций извлечения квадратного корня. Последние операции, конечно, труднее выполнимы, чем даже умножение, и могут быть выполнены только приближенно. Но в БПФ приходится извлекать комплексные корни из единицы, а эта процедура сводится к вычислению значений тригонометрических функций и также выполняется только приближенно и не быстрее извлечения квадратного корня.

4. Связь с ДПФ

В прямом ходе приведенного выше алгоритма по произвольному многочлену

$$f(x) = f_0 + f_1 x + \ldots + f_{n-1}x^{n-1}$$

с четным n фактически вычисляется система вычетов

$$\begin{aligned} f(x) \pmod{p_k} &= a_k x + b_k, \\ p_k &= (x - \omega_n^k)(x - \omega_n^{-k}) = x^2 - 2\cos\left(\frac{2\pi k}{n}\right)x + 1, \\ \omega_n &= e^{2\pi i/n}, \qquad k = 0,\ldots,n/2-1, \end{aligned}$$

(так как разложение многочлена $x^n - 1$ на неприводимые множители над полем действительных чисел состоит из выписанных выше квадратных трехчленов p_k, $k = 0, 1, \ldots, n/2 - 1$). Заметим еще, что

$$p_k = (x - \omega_n^k)(x - \omega_n^{-k}) = (x - \omega_n^k)(x - \omega_n^{n-k}) = p_{n-k}, \qquad k = 0, 1, \ldots, n,$$

если распространить определение трехчленов p_k на все k от 0 до $n-1$. Далее станет ясно, что преобразование G_n, вычисляющее по вектору

$$f = (f_0, f_1, \ldots, f_{n-1})$$

вектор

$$G_n[f] = (a_0, b_0, \ldots, a_{n/2-1}, b_{n/2-1})$$

является действительным линейным преобразованием.

Так как

$$\begin{aligned}
F_n(k)[f] &= \sum_{l=0}^{n-1} f_l \omega_n^{kl} = f(\omega_n^k) = f(x) \pmod{x - \omega_n^k} \\
&= (f(x) \pmod{p_k}) \pmod{x - \omega_n^k} \\
&= a_k x + b_k \pmod{x - \omega_n^k} \\
&= a_k \omega_n^k + b_k, && k < n/2, \\
F_n(k)[f] &= a_{n-k} x + b_{n-k} \pmod{x - \omega_n^k} \\
&= a_{n-k} \omega_n^k + b_{n-k}, && n/2 \leqslant k \leqslant n-1,
\end{aligned}$$

решая систему линейных уравнений, находим, что

$$\begin{aligned}
a_k &= \frac{F_n(k) - F_n(n-k)}{\omega_n^k - \omega_n^{-k}} = \frac{F_n(k) - F_n(n-k)}{2i \sin(2\pi k/n)}, \\
b_k &= \frac{F_n(k)\omega_n^{-k} - F_n(n-k)\omega_n^k}{\omega_n^{-k} - \omega_n^k} = \frac{F_n(n-k)\omega_k^k - F_n(k)\omega_n^{-k}}{2i \sin(2\pi k/n)}.
\end{aligned}$$

В действительном случае полученные формулы можно переписать в виде

$$\begin{aligned}
\Re F_n(k) &= a_k \cos(2\pi k/n) + b_k, \\
\Im F_n(k) &= a_k \sin(2\pi k/n), && 0 \leqslant k < n/2, \\
\Re F_n(k) &= a_{n-k} \cos(2\pi k/n) + b_{n-k}, \\
\Im F_n(k) &= a_{n-k} \sin(2\pi k/n), && n/2 \leqslant k < n, \\
b_k &= \frac{-\Im(F_n(k)\omega_n^{-k})}{\sin(2\pi k/n)} = \Re F_n(k) - \operatorname{ctg}(2\pi k/n)\Im F_n(k), \\
a_k &= \frac{\Im F_n(k)}{\sin(2\pi k/n)}, && 0 \leqslant k < n/2,
\end{aligned}$$

где $\Re$ обозначает действительную, а $\Im$ мнимую часть числа, вектора, или преобразования.

Явные формулы для преобразования G_n имеют вид

$$\begin{aligned} a_k &= \sum_{l=0}^{n-1} f_l \frac{\omega_n^{kl} - \omega_n^{-kl}}{\omega_n^k - \omega_n^{-k}} \\ &= \sum_{l=0}^{n-1} f_l \frac{\sin(2\pi kl/n)}{\sin(2\pi k/n)}, \qquad k = 0, 1, \ldots, n/2 - 1, \\ b_k &= \sum_{l=0}^{n-1} f_l \frac{\omega_n^{kl}\omega_n^{-k} - \omega_n^{-kl}\omega_n^{k}}{\omega_n^k - \omega_n^{-k}} \\ &= \sum_{l=0}^{n-1} f_l \frac{\omega_n^{k(l-1)} - \omega_n^{-k(l-1)}}{\omega_n^k - \omega_n^{-k}} \\ &= \sum_{l=0}^{n-1} f_l \frac{\sin(2\pi k(l-1)/n)}{\sin(2\pi k/n)}, \qquad k = 0, 1, \ldots, n/2 - 1. \end{aligned}$$

Из них видно, что это преобразование похоже на синусное преобразование, но несколько от него отличается.

Если обозначить $G(n)$ сложность вычисления преобразования G_n, то из полученных формул следует, что в действительном случае

$$F(n) \leqslant G(n) + 3n/2, \qquad G(n) \leqslant F(n) + 3n/2,$$

а в комплексном случае для действительной сложности

$$F(n) \leqslant G(n) + 4n, \qquad G(n) \leqslant F(n) + 7n$$

при условии, что сложность предварительного вычисления необходимых коэффициентов, как обычно, игнорируется. Из полученных неравенств следует, что преобразования G_n и F_n имеют одинаковую сложность с точностью до линейных слагаемых. В частности, приведенный выше алгоритм можно использовать (после очевидной модификации) для вычисления F_n со сложностью $(1/2)n\log_2 n + O(n)$ в действительном и с действительной сложностью $2n\log_2 n + O(n)$ в комплексном случае. Однако наилучшие алгоритмы БПФ, как отмечалось, имеют меньшую сложность, и наоборот их можно использовать для более быстрого вычисления G_n.

5. О преобразовании Хартли

Известно (см., например, [6]), что использование преобразования Хартли вместо преобразования Фурье позволяет улучшить приведенную во введении оценку сложности умножения действительных многочленов. Так как этот факт достаточно мало известен, мы для полноты приведем его обоснование, причем необходимые для этого свойства преобразования Хартли мы выведем из более известных свойств преобразования Фурье.

Будем обозначать действительное ДПФ порядка n через F_n. Тогда соответствующее преобразование Хартли (ДПХ) по определению равно

$$H_n = aF_n + \bar{a}\bar{F}_n,$$

где $a = (1-\imath)/2$, а знаком $\bar{a}$ будем обозначать переход к комплексно сопряженному числу (или преобразованию). Из определения следует, что

$$H_n = \Re F_n + \Im F_n,$$

так как для любого комплексного числа z справедливо тождество $az + \overline{az} = \Re z + \Im z$, из которого следуют равенства

$$a^2 + \bar{a}^2 = \Re a + \Im a = 0, \qquad 2a\bar{a} = \Re\bar{a} + \Im\bar{a} = 1$$

и тождество $a\bar{z} + \bar{a}z = \Re z - \Im z$.

Из указанного тождества также следует, что элементы матрицы ДПХ, имеют вид

$$\Re\omega_n^{kl} + \Im\omega_n^{kl} = \sin(2\pi kl/n) + \cos(2\pi kl/n), \qquad 0 \leqslant k, l \leqslant n-1,$$

где $\omega_n^{kl} = e^{2\pi\imath kl/n}$ — элементы матрицы ДПФ, хотя это далее не понадобится. Заметим все же, что обычно вместо $\sin(2\pi kl/n) + \cos(2\pi kl/n)$ пишут $\operatorname{cas}(2\pi kl/n)$, и ДПХ представляют в виде

$$H_n(k) = \sum_{l=0}^{n-1} x_l \operatorname{cas}(2\pi kl/n), \qquad k = 0, \ldots, n-1,$$

откуда видно, что оно является действительным линейным преобразованием.

Другим удобным его свойством является то, что оно фактически совпадает со своим обратным преобразованием. Действительно, известно, что

$$F_n\bar{F}_n = nE_n, \qquad F_n^2 = nI_n,$$

где E_n, I_n — единичные матрицы, в которых единицы стоят соответственно на главной и побочной диагоналях (а в остальных местах стоят нули). Поэтому

$$\begin{aligned} H_n^2 &= (aF_n + \bar{a}\bar{F}_n)^2 \\ &= a^2F_n^2 + \bar{a}^2\bar{F}_n^2 + a\bar{a}(F_n\bar{F}_n + \bar{F}_nF_n) \\ &= (a^2 + \bar{a}^2)nI_n + a\bar{a}2nE_n \\ &= a\bar{a}2nE_n = nE_n, \end{aligned}$$

откуда

$$H_n^{-1} = \frac{1}{n}H_n.$$

Обозначим A^* преобразование, получающееся из преобразования A обратной перестановкой компонент, а именно,

$$A^*(k) = A(n-k), \qquad k = 0, \ldots, n-1.$$

Очевидно, что $A^{**} = A$. Очевидно также, что для действительного ДПФ (то есть применяемого к действительным векторам) справедливо равенство $F_n^* = \bar{F}_n$. Отсюда следует, что

$$\begin{aligned} H_n^* &= (aF_n + \bar{a}\bar{F}_n)^* \\ &= aF_n^* + \bar{a}\bar{F}_n^* \\ &= a\bar{F}_n + \bar{a}F_n \\ &= \Re F_n - \Im F_n. \end{aligned}$$

Обозначим сложность (то есть число операций, необходимых для выполнения) ДПХ n-го порядка через $H(n)$. Тогда с помощью равенств

$$H_n = \Re F_n + \Im F_n,$$
$$H_n^* = \Re F_n - \Im F_n \Re F_n = \frac{H_n + H_n^*}{2},$$
$$\Im F_n = \frac{H_n - H_n^*}{2}$$

легко получить, что

$$H(n) \leqslant F(n) + n,$$
$$F(n) \leqslant H(n) + 3n,$$

если под сложностью понимать действительную сложность, то есть число действительных операций.

Комплексное ДПХ удобнее определить равенством

$$H_n = aF_n + \bar{a}F_n^*,$$

которое можно использовать и в действительном случае, так как тогда $F_n^* = \bar{F}_n$. Ясно, что

$$\Re H_n(z) = H_n(\Re z),$$
$$\Im H_n(z) = H_n(\Im z),$$

чего нельзя сказать о ДПФ. Из указанного равенства следует, что

$$H_n^* = aF_n^* + \bar{a}F_n^{**} = aF_n^* + \bar{a}F_n,$$
$$\bar{a}H_n + aH_n^* = 2a\bar{a}F_n + (a^2 + \bar{a}^2)F_n^* = F_n,$$
$$\bar{a}H_n^* + aH_n = 2a\bar{a}F_n^* + (a^2 + \bar{a}^2)F_n = F_n^*.$$

Из полученных равенств $H_n = aF_n + \bar{a}F_n^*$ и $F_n = \bar{a}H_n + aH_n^*$ легко получить как для комплексных, так и для действительных преобразований и комплексной сложности неравенства

$$H(n) \leqslant F(n) + 3n,$$
$$F(n) \leqslant H_n + 3n,$$

а для комплексных преобразований и действительной сложности неравенства

$$H(n) \leqslant F(n) + 14n,$$
$$F(n) \leqslant H(n) + 14n$$

(в которых можно заменить $14n$ на $6n$, если считать, что действительные умножения на $1/2$ выполняются бесплатно).

Отметим еще, что действительная сложность комплексного ДПХ очевидно совпадает с действительной сложностью совместного вычисления двух действительных ДПХ для независимо выбранных аргументов. Для ДПФ справедливо несколько более слабое утверждение, а именно,

$$F^{\mathbf{C}}(n) \leqslant 2F^{\mathbf{R}}(n) + 2n, \qquad \operatorname{comp}(F_n^{\mathbf{R}}(x), F_n^{\mathbf{R}}(y)) \leqslant F^{\mathbf{C}}(n) + 8n,$$

где во втором неравенстве под $\operatorname{comp}(F_n^{\mathbf{R}}(x), F_n^{\mathbf{R}}(y))$ понимается действительная сложность совместного вычисления двух действительных ДПФ. Для доказательства достаточно воспользоваться тождествами

$$\begin{aligned}
F_n(z) &= F_n(\Re z) + \imath F_n(\Im z),\\
F_n^*(z) &= \bar{F}_n(\bar{z}) = \overline{F_n(\Re z) - \imath F_n(\Im z)},\\
\bar{F}_n^*(z) &= F_n(\Re z) - \imath F_n(\Im z),\\
F_n(\Re z) &= \frac{F_n(z) + \bar{F}_n^*(z)}{2},\\
F_n(\Im z) &= \frac{F_n(z) - \bar{F}_n^*(z)}{2\imath}.
\end{aligned}$$

Из известного неравенства Кули–Тьюки ([2]) вытекает, что для действительной сложности действительных ДПФ справедливо неравенство

$$F(2n) \leqslant 2F(n) + 8n,$$

где под $2F(n)$ можно понимать, в частности, сложность совместного вычисления двух действительных ДПФ порядка n. Поэтому

$$\begin{aligned}
F^{\mathbf{C}}(n) &\leqslant 2F^{\mathbf{R}}(n) + 2n,\\
F^{\mathbf{R}}(2n) &\leqslant F^{\mathbf{C}}(n) + 16n,
\end{aligned}$$

откуда следует, что наилучшие из известных алгоритмов комплексного БПФ, имеющие при $n = 2^k$ оценку действительной сложности

$$F(n) = 4n\log_2 n + O(n),$$

дают для действительного БПФ оценку действительной сложности

$$F(n) = 2n\log_2 n + O(n),$$

а значит, и для действительного ДПХ справедлива известная оценка

$$H(n) = 2n\log_2 n + O(n).$$

Отметим, что для комплексной сложности также справедливо неравенство

$$F^{\mathbf{C}}(n) \leqslant 2F^{\mathbf{R}}(n) + 2n,$$

а вместо второго соответствующего неравенства — даже неравенство

$$\operatorname{comp}(F_n^{\mathbf{R}}(x), F_n^{\mathbf{R}}(y)) \leqslant F^{\mathbf{C}}(n) + 6n,$$

если к числу арифметических операций добавить операцию сопряжения, а неравенство Кули–Тьюки для комплексной сложности действительного ДПФ принимает вид $F(2n) \leqslant 2F(n) + 2n$. Учитывая, что для комплексной сложности комплексного ДПФ справедлива известная оценка

$$F^{\mathbf{C}}(n) = (1 + 1/2)n\log_2 n,$$

отсюда получаем, что комплексная сложность действительного ДПФ не превосходит $(3/4)n\log_2 n + 4n$, а значит, согласно, доказанному выше, комплексная сложность действительного ДПХ не превосходит $(3/4)n\log_2 n + O(n)$.

Известно, что для ДПФ выполняется замечательное тождество (теорема о циклической свертке)

$$F_n(x \odot y) = F_n(x) \otimes F_n(y),$$

где $x \otimes y$ — операция покомпонентного умножения векторов x и y, а $u = x \odot y$ — циклическая свертка векторов x и y, которая определяется равенством

$$u_k = \sum_{i \oplus j = k} x_i y_j,$$

где $i \oplus j = i + j \pmod n$ — операция сложения по модулю n. Для ДПХ соответствующее тождество принимает несколько менее красивый вид

$$H_n(x \odot y) = \frac{1}{2}(H_n(x) \otimes H_n(y) + H_n^*(x) \otimes H_n(y) + H_n(x) \otimes H_n^*(y) - H_n^*(x) \otimes H_n^*(y)),$$

так как

$$\begin{aligned}
H_n(x \odot y) &= aF_n(x \odot y) + \bar{a}F_n^*(x \odot y) \\
&= aF_n(x) \otimes F_n(y) + \bar{a}(F_n(x) \otimes F_n(y))^* \\
&= aF_n(x) \otimes F_n(y) + \bar{a}F_n^*(x) \otimes F_n^*(y) \\
&= a((\bar{a}H_n(x) + aH_n^*(x)) \otimes (\bar{a}H_n(y) + aH_n^*(y))) \\
&\quad + \bar{a}((\bar{a}H_n^*(x) + aH_n(x)) \otimes (\bar{a}H_n^*(y) + aH_n(y))) \\
&= (a\bar{a}^2 + a^2\bar{a})H_n(x) \otimes H_n(y) + (a^2\bar{a} + a\bar{a}^2)H_n^*(x) \otimes H_n(y) \\
&\quad + (a^2\bar{a} + a\bar{a}^2)H_n(x) \otimes H_n^*(y) + (a^3 + \bar{a}^3)H_n^*(x) \otimes H_n^*(y) \\
&= \frac{1}{2}(H_n(x) \otimes H_n(y) + H_n^*(x) \otimes H_n(y) \\
&\quad + H_n(x) \otimes H_n^*(y) - H_n^*(x) \otimes H_n^*(y)),
\end{aligned}$$

благодаря равенствам

$$\begin{aligned}
a^2\bar{a} + a\bar{a}^2 &= (a + \bar{a})a\bar{a} = (a + \bar{a})/2 = 1/2, \\
a^3 + \bar{a}^3 &= (a + \bar{a})((a + \bar{a})^2 - 3a\bar{a}) = 1 - 3a\bar{a} = -1/2.
\end{aligned}$$

Отметим, что и ДПФ и ДПХ-варианты теоремы о свертке справедливы, очевидно, как в действительном, так и в комплексном случаях.

6. Сложность умножения многочленов, ДПФ и ДПХ

Если обозначить $M(n)$ сложность умножения многочленов степени $n-1$, а $Z(n)$ сложность вычисления циклической свертки, то известно (и легко вытекает из ска-

занного выше), что $M(n) \leqslant Z(2n)$ и в случае действительной свертки и для действительной сложности

$$\begin{aligned} Z(n) &\leqslant 2F^{\mathbf{R}}(n) + F^{\mathbf{C}}(n) + 8n + 1 \\ &\leqslant 4F^{\mathbf{R}}(n) + 10n + 1, \qquad (1) \\ Z(n) &\leqslant 3H(n) + 8n + 1. \qquad (2) \end{aligned}$$

Отметим, что (2) сильнее, чем (1), так как $H(n) \leqslant F(n) + n$, откуда следует, что $Z(n) \leqslant 3F(n) + 11n + 1$. Применяя (2), получаем, что для действительной сложности умножения действительных многочленов справедлива оценка

$$\begin{aligned} M(n) = M^{\mathbf{R}}_{\mathbf{R}}(n) &\leqslant 3F(2n) + 22n + 1 \\ &\leqslant 6F(n) + 46n + 1 \\ &\leqslant 12n \log_2 n + O(n). \qquad (3) \end{aligned}$$

Неравенство (3) верно лишь для n, равных степени двойки. Для произвольных n оно заменяется на асимптотическое неравенство (которое можно получить приемом, указанным во введении).

В случае комплексной свертки и действительной сложности неравенство (2) не меняется, а в первом слагаемое $10n + 1$ заменяется на $8n + 1$, то есть оба неравенства принимают одинаковый вид (с заменой F на H). Оценка для действительной сложности умножения комплексных многочленов при $n = 2^k$ принимает вид

$$M(n) = M^{\mathbf{R}}_{\mathbf{C}}(n) \leqslant 24n \log_2 n + O(n). \qquad (4)$$

В случае комплексной свертки и комплексной сложности неравенство (2) не меняется, а в (1) слагаемое $8n + 1$ заменяется на $2n + 1$, то есть в этом случае использование ДПХ преимуществ не дает. Учитывая, что комплексная сложность ДПФ при $n = 2^k$ равна, как известно, $(3/2)n \log_2 n$, получаем, что оценка для комплексной сложности умножения комплексных многочленов в этом случае принимает вид

$$\begin{aligned} M(n) = M^{\mathbf{C}}_{\mathbf{C}}(n) &\leqslant 3F^{\mathbf{C}}_{\mathbf{C}}(2n) + 2n + 1 \\ &\leqslant 9n \log_2 n + 2n + 1. \end{aligned}$$

И наконец, оценка для комплексной сложности умножения действительных многочленов принимает вид

$$M(n) = M^{\mathbf{C}}_{\mathbf{R}}(n) \leqslant 3F^{\mathbf{C}}_{\mathbf{R}}(2n) + 2n + 1 \leqslant 2n \log_2 n + 26n + 1.$$

Отметим для полноты, что можно оценить и $F(n)$ сверху через $M(n)$. Для этого сначала заметим, что в комплексном случае $F(n) \leqslant Z(n) + 2n$ при четном n и $F(n) \leqslant 2C(n) + 4n$ при любом n, где $C(n)$ — сложность обычной свертки, то есть операции умножения векторов x и y по формуле

$$c_k = \sum_{i=0}^{k} x_i y_{k-i}, \qquad k = 0, 1, \ldots, n-1.$$

Это вытекает из следующего алгоритма Блюстейна для вычисления ДПФ (см., например, [2], где есть небольшая неточность):

$$\begin{aligned} F_n(k) &= \sum_{i=0}^{n-1} x_i \omega_n^{ki} = \beta_n^{-k^2} \sum_{i=0}^{n-1} \beta_n^{(k-i)^2} (\beta_n^{-i^2} x_i) \\ &= \beta_n^{-k^2} \left(\sum_{i=0}^{k} \beta_n^{(k-i)^2} (\beta_n^{-i^2} x_i) + \sum_{i=k+1}^{n-1} \beta_n^{(i-k)^2} (\beta_n^{-i^2} x_i) \right) \\ &= \beta_n^{-k^2} \left(\sum_{i=0}^{k} Y_{k-i} X_i + \sum_{j=0}^{n-k-1} Y_{n-k-1-j} U_j - X_k \right) \\ &= \beta_n^{-k^2} \sum_{i \oplus j = k} X_i Y_j, \end{aligned}$$

где

$$\beta_n^{-2} = \omega_n, \quad \beta_n = e^{-\pi \imath / n}, \quad Y_i = \beta_n^{i^2}, \quad X_i = \beta_n^{-i^2} x_i, \quad U_i = X_{n-1-i},$$

так как при четном n

$$((k-i) \pmod n)^2 \pmod{2n} = (k-i)^2 \pmod{2n}.$$

Указанные выше оценки получаются, если не учитывать сложность предварительного вычисления коэффициентов $\beta_n^{-k^2}$ и $\beta_n^{k^2}$. Очевидно, что эта сложность равна $O(n)$, если разрешается пользоваться $O(1)$ раз операцией извлечения квадратного корня. Поэтому в общем случае (и в действительном тоже) $F(n) \leqslant 2C(n) + O(n)$, где $C(n)$ — сложность (может быть действительная) комплексной свертки. В действительном случае из этой оценки легко следует оценка $F(n) \leqslant 8C(n) + O(n)$, где $C(n)$ — сложность (действительная) действительной свертки.

Известно (и легко проверяется), что (и в действительном и в комплексном случаях)

$$\begin{aligned} Z(n) &\leqslant 2C(n) + 2n, \\ C(n) &\leqslant M(n) \leqslant C(2n-1), \end{aligned}$$

откуда следует, что

$$\begin{aligned} F(n) &\leqslant 2C(n) + O(n) \\ &\leqslant M(n)/2 + O(n), \end{aligned}$$

где $M(n)$ — сложность умножения комплексных многочленов. В действительном случае очевидно справедлива оценка

$$\begin{aligned} F(n) &\leqslant 8C(n) + O(n) \\ &\leqslant 4M_{\mathbf{R}}^{\mathbf{R}}(n) + O(n). \end{aligned}$$

В результате в любом из возможных смыслов $F(n) = O(M(n))$, $M(n) = O(F(n))$, откуда следует, что все функции $M(n)$, $C(n)$, $Z(n)$, $F(n)$, $G(n)$, $H(n)$ равны по порядку.

7. Об умножении многочленов, ДПФ и ДПХ в конечных полях

Пусть $\mathrm{GF}(q^2)$ — расширение конечного поля $\mathrm{GF}(q)$ с помощью неприводимого многочлена x^2+1 (аналог поля комплексных чисел). Известно, что такое расширение существует при $q \pmod 4 = 3$ и только при этом условии. Элементы поля $\mathrm{GF}(q^2)$ можно представить в виде $a+\imath b$, где $a, b \in \mathrm{GF}(q)$, $\imath \in \mathrm{GF}(q^2)$ — корень уравнения $x^2+1=0$ (в качестве $\imath$ можно взять $\alpha^{(q^2-1)/4}$, где α — любой примитивный элемент поля $\mathrm{GF}(q^2)$). Для существования первообразного корня n-й степени из единицы в поле $\mathrm{GF}(q^2)$ необходимо и достаточно, чтобы q^2-1 было кратно n (тогда в качестве этого корня можно взять $\alpha^{(q^2-1)/n}$, где α — упоминавшийся примитивный элемент). Допустим, что $q-1$ не кратно n, то есть в поле $\mathrm{GF}(q)$ первообразного корня n-й степени из единицы нет. Тогда для выполнения ДПФ порядка n придется вместо поля $\mathrm{GF}(q)$ использовать его квадратичное расширение $\mathrm{GF}(q^2)$ аналогично тому, как в случае вычисления обычного ДПФ приходится использовать комплексные числа. В указанном расширении можно по аналогии с комплексными числами ввести операцию сопряжения, и также как в случае комплексных чисел сопряженное к произведению двух чисел число будет равно произведению чисел, сопряженных к исходным (мультипликативность операции сопряжения).

Предположим дополнительно, что в поле $\mathrm{GF}(q^2)$ существует такой первообразный корень n-й степени из единицы α, что $\alpha\bar{\alpha}=1$ (здесь $\bar{\alpha}$, как и выше, обозначает сопряженное к α число), тогда $\alpha^{n-1}=\bar{\alpha}$, и все приведенные в разделе 6 результаты могут быть без существенных изменений перенесены в рассматриваемую ситуацию. Операции в поле $\mathrm{GF}(q^2)$ также могут быть сведены к операциям в поле $\mathrm{GF}(q)$, как и операции над комплексными числами сводятся к операциям над действительными числами. Количество операций в поле $\mathrm{GF}(q^2)$, необходимых для вычисления рассматриваемого ДПФ, будет играть роль комплексной сложности, а количество операций в поле $\mathrm{GF}(q)$ — роль действительной сложности. Аналогично разделу 5 может быть определено для случая конечных полей и ДПХ и введены аналоги его комплексной и действительной сложности.

Для выполнения умножения многочленов степени не выше $(n-1)/2$ над полем $\mathrm{GF}(q)$ аналогично действительному случаю могут быть применены ДПФ и ДПХ порядка n с теми же оценками сложности, что и в действительном (комплексном) случае. Отличие от последнего случая только в том, что в поле $\mathrm{GF}(q^2)$ нельзя выполнять ДПФ порядка, большего n, а в поле комплексных чисел можно выполнять ДПФ любого порядка.

Для получения оценок сложности умножения действительных многочленов выгодно использовать ДПФ порядка, равного степени двойки, так как для этого случая известны алгоритмы с наименьшими мультипликативными константами в оценках сложности. В случае поля $\mathrm{GF}(q)$ соответствующий ему порядок n может не иметь такого вида. Однако в одном важном (и наиболее популярном) случае n может иметь такой вид, а именно, когда $q=2^p-1$ — простое число Мерсенна, тогда в поле $\mathrm{GF}(q^2)$ возможно выполнение ДПФ порядка $n=2^{p+1}$ ([2, 7]). Как известно ([4, 7]), в случае $n=2^{p+1}$ любой первообразный корень n-го порядка удовлетворяет условию $\alpha\bar{\alpha}=-1$. Примером такого корня является

$$2^{2^{p-2}}+\imath 3^{2^{p-2}} \pmod q.$$

Квадрат этого элемента является при $n = 2^p$ примером первообразного корня n-го порядка, удовлетворяющего условию $\alpha\bar{\alpha} = 1$ (см. [7]).

Согласно (4) сложность умножения многочленов степени, меньшей $q/2$, над полем $\mathrm{GF}(q)$ не превосходит $12q\log_2 q + O(q)$, где под элементарными операциями понимаются арифметические операции по модулю q.

В отличие от действительного случая используемое здесь ДПХ выполняется абсолютно точно, и умножение многочленов тоже выполняется точно (в действительном случае даже умножение многочленов с целыми коэффициентами с помощью ДПФ формально говоря может быть выполнено только приближенно).

Отметим, что если выполнять умножение многочленов с коэффициентами 0 и 1 степени не выше $q-2$ над кольцом целых чисел, то его результат можно однозначно восстановить, выполнив умножение тех же многочленов над полем $\mathrm{GF}(q)$. По результату умножения этих многочленов над полем $\mathrm{GF}(q)$ можно также однозначно восстановить их произведение над полем $\mathrm{GF}(2)$. Сложность во всех случаях будет оцениваться как $12q\log_2 q + O(q)$. Для оценки битовой сложности нужно приведенную оценку умножить на $O(M(p))$ — оценку битовой сложности умножения p-разрядных двоичных чисел.

При оценке времени вычисления указанных произведений на компьютере битовая сложность не нужна, вместо нее естественно использовать оценку числа операций в поле $\mathrm{GF}(q)$, или в поле $\mathrm{GF}(q^2)$, если объем оперативной памяти машины (а точнее, размер кэш-памяти) позволяет хранить таблицы умножения и сложения в этих полях. Это можно сделать, например, при $q = 2^6 - 1$ для поля $\mathrm{GF}(q^2)$, поэтому сложность умножения многочленов степени $n < 32$ по модулю 63 в этой ситуации можно оценить как $(9/2)n\log_2 n + 26n + 1$ (аналог оценки комплексной сложности умножения действительных многочленов). Эта оценка вполне сравнима со стандартной оценкой сложности умножения многочленов при $n = 31$.

8. Алгоритм БПФ с расщепленным основанием в конечных полях

Приведенные выше оценки сложности умножения многочленов над полями $\mathrm{GF}(q^2)$, где $q = 2^p - 1$ — простое число Мерсенна, можно улучшить, если применить алгоритм с расщепленным основанием [4]. Мы приведем полиномиальную версию этого алгоритма, на наш взгляд более легкую для восприятия, чем версия, изложенная в [4].

Как известно, для вычисления ДПФ n-мерного вектора a достаточно взять многочлен $(n-1)$-й степени $a(x)$ с указанным вектором коэффициентов и найти все его остатки

$$f_k = a(x) \pmod{x - \omega_n^k}, \qquad k = 0, 1, \ldots n-1,$$

по модулям линейных двучленов, коэффициенты которых ω_n^k пробегают множество всех корней из единицы в рассматриваемом поле. Для этого при n, кратном 8, воспользуемся разложением

$$\begin{aligned} x^n - 1 &= (x^{n/2} - 1)(x^{n/2} + 1) = (x^{n/2} - 1)(x^{n/4} - \imath)(x^{n/4} + \imath) \\ &= (x^{n/2} - 1)(x^{n/8} - \varepsilon)(x^{n/8} - \imath\varepsilon)(x^{n/8} + \varepsilon)(x^{n/8} + \imath\varepsilon), \end{aligned}$$

где

$$\varepsilon = 2^{(p-1)/2} + \imath 2^{(p-1)/2}, \qquad \varepsilon^2 = 2^{p-1} 2\imath = \imath,$$
$$\varepsilon^4 = -1, \quad \varepsilon^6 = -\imath, \quad \varepsilon^8 = 1,$$
$$\varepsilon^3 = \imath\varepsilon, \quad \varepsilon^5 = -\varepsilon, \quad \varepsilon^7 = -\imath\varepsilon$$

(идея использовать корни восьмой степени из единицы в поле $\mathrm{GF}(q^2)$ при выполнении ДПФ принадлежит Нуссбаумеру, см. [7]). Тогда в силу разложений

$$x^{n/2} - 1 = \prod_{k=0}^{n/2-1} (x - \omega_n^{2k}),$$
$$x^{n/8} - \varepsilon = \prod_{k=0}^{n/8-1} (x - \omega_n^{8k+1}),$$
$$x^{n/8} + \varepsilon = \prod_{k=0}^{n/8-1} (x - \omega_n^{8k+5}),$$
$$x^{n/8} - \imath\varepsilon = \prod_{k=0}^{n/8-1} (x - \omega_n^{8k+3}),$$
$$x^{n/8} + \imath\varepsilon = \prod_{k=0}^{n/8-1} (x - \omega_n^{8k+7})$$

справедливы равенства

$$f_{2k} = (a(x) \pmod{x^{n/2} - 1}) \pmod{x - \omega_{n/2}^k}, \qquad \omega_{n/2} = \omega_n^2, \quad \omega_{n/2}^{n/4} = -1,$$
$$f_{8k+1} = (a(x) \pmod{x^{n/8} - \varepsilon}) \pmod{x - \omega_n \omega_{n/8}^k}, \qquad \omega_{n/8} = \omega_n^8, \quad \omega_{n/8}^{n/16} = -1,$$
$$f_{8k+3} = (a(x) \pmod{x^{n/8} - \imath\varepsilon}) \pmod{x - \omega_n^3 \omega_{n/8}^k},$$
$$f_{8k+5} = (a(x) \pmod{x^{n/8} + \varepsilon}) \pmod{x - \omega_n^5 \omega_{n/8}^k},$$
$$f_{8k+7} = (a(x) \pmod{x^{n/8} + \imath\varepsilon}) \pmod{x - \omega_n^7 \omega_{n/8}^k}.$$

Очевидно, вычисление остатков

$$a(x) \pmod{x^{n/2} - 1}, \qquad a(x) \pmod{x^{n/2} + 1}$$

требует n комплексных сложений (вычитаний), а вычисление остатков f_{2k}, $k = 0, 1, \ldots, n/2 - 1$, выполняется с помощью ДПФ порядка $n/2$.

Далее, вычисление остатков

$$a(x) \pmod{x^{n/4} - \imath}, \qquad a(x) \pmod{x^{n/4} + \imath}$$

по формулам

$$a(x) \pmod{x^{n/4} - \imath} = (a(x) \pmod{x^{n/2} + 1}) \pmod{x^{n/4} - \imath},$$
$$a(x) \pmod{x^{n/4} + \imath} = (a(x) \pmod{x^{n/2} + 1}) \pmod{x^{n/4} + \imath}$$

требует $n/2$ комплексных сложений (умножения на $\pm\imath$ бесплатные).

После этого вычисление остатков

$$a(x) \pmod{x^{n/8} \pm \varepsilon}, \qquad a(x) \pmod{{}^{n/8} \pm \imath\varepsilon}$$

по формулам

$$\begin{aligned}
a(x) \pmod{x^{n/8} - \varepsilon} &= (a(x) \pmod{x^{n/4} - \imath}) \pmod{x^{n/8} - \varepsilon},\\
a(x) \pmod{x^{n/8} - \imath\varepsilon} &= (a(x) \pmod{x^{n/4} + \imath}) \pmod{x^{n/8} - \imath\varepsilon},\\
a(x) \pmod{x^{n/8} + \imath\varepsilon} &= (a(x) \pmod{x^{n/4} + \imath}) \pmod{x^{n/8} + \imath\varepsilon},\\
a(x) \pmod{x^{n/8} + \varepsilon} &= (a(x) \pmod{x^{n/4} - \imath}) \pmod{x^{n/8} + \varepsilon}
\end{aligned}$$

требует еще $n/2$ комплексных сложений и $n/8$ умножений на ε и $\imath\varepsilon$, каждая пара которых ввиду формул

$$\varepsilon = 2^{(p-1)/2}(1 + \imath), \qquad \imath\varepsilon = 2^{(p-1)/2}(-1 + \imath)$$

требует 2 действительных сложений-вычитаний и 4 умножений на степени двойки, то есть сдвигов массива двоичных цифр, которые выполняются существенно быстрее, чем общее умножение.

И, наконец, вычисление

$$f_{8k+1} = (a(x) \pmod{x^{n/8} - \varepsilon}) \pmod{x - \omega_n\omega_{n/8}^k}, \quad \omega_{n/8} = \omega_n^8, \quad \omega_{n/8}^{n/16} = -1$$

по формуле

$$f_{8k+1} = g(x) \pmod{x - \omega_n\omega_{n/8}^k} = g(\omega_n x) \pmod{x - \omega_{n/8}^k}$$

требует вначале $n/8-1$ комплексных умножений коэффициентов многочлена $g(x) = f(x) \pmod{x^{n/8} - \varepsilon}$ на заранее известные скаляры ω_n^i, $i = 1, \ldots n/8 - 1$, каждое из которых выполняется, как известно [2], за три действительных умножения и три действительных сложения, а потом ДПФ порядка $n/8$. Аналогично вычисляются и компоненты

$$f_{8k+3}, \quad f_{8k+5}, \quad f_{8k+7}, \quad k = 0, \ldots n/8 - 1.$$

В результате имеем следующие рекуррентные оценки числа действительных сложений, умножений и сдвигов:

$$\begin{aligned}
MF(n) &\leqslant MF(n/2) + 4MF(n/8) + 3n/2 - 12,\\
AF(n) &\leqslant AF(n/2) + AMF(n/8) + 23n/4,\\
SF(n) &\leqslant SF(n/2) + 4SF(n/8) + n/2.
\end{aligned}$$

Рекуррентное соотношение вида

$$K(n) = K(n/2) + 4K(n/8) + a_1 n + a_2$$

имеет, как легко проверить, частное решение

$$K(n) = \frac{a_1}{2} n \log_2 n - \frac{a_2}{4}.$$

Для нахождения общего решения нужно прибавить к указанному частному решению общее решение однородного рекуррентного соотношения

$$K(n) - K(n/2) - 4K(n/8) = 0,$$

которое после замены $k(n) = K(2^n)$ принимает вид

$$k(n) = k(n-1) + 4k(n-3),$$

и имеет общее (действительное) решение

$$k(n) = (a+bi)(-1/2 + i\sqrt{7}/2)^n + (a-bi)(-1/2 - i\sqrt{7}/2)^n + c2^n.$$

Коэффициенты подбираются так, чтобы значения функций $MF(n)$, $AF(n)$, $SF(n)$ при $n = 2, 4, 8$, вычисленные по указанным формулам, совпадали со следующими легко проверяемыми значениями:

$$MF(n) = SF(n) = 0, \qquad n = 2, 4, 8,$$
$$AF(2) = 4, \quad AF(4) = 16, \quad AF(8) = 34.$$

Например, в случае $MF(n)$ эти коэффициенты будут равны

$$c = -39/16, \quad a = -9/32, \quad b = -3/(32\sqrt{7}).$$

Окончательная оценка в этом случае имеет вид

$$MF(n) \leqslant \frac{3}{4}\left(n\log_2 n - \frac{13}{4}\right) + \frac{3}{16}\sqrt{n}\left(\frac{1}{\sqrt{7}}\sin(\varphi\log_2 n) - 3\cos(\varphi\log_2 n)\right) + 3, \quad (5)$$

где

$$\varphi = \arccos(-1/(2\sqrt{2})).$$

Остальные оценки приведем в упрощенном виде:

$$SF(n) \leqslant \frac{1}{4}n\log_2 n + O(n),$$
$$AF(n) \leqslant \frac{23}{8}n\log_2 n + O(n),$$

и окончательно

$$F(n) \leqslant \frac{31}{8}n\log_2 n + O(n). \quad (6)$$

В [4] по непонятной причине вместо указанных выше формул приведены без обоснования неверные приближенные формулы.

Отметим еще, что в случае действительного ДПФ (то есть применяемого к векторам над полем $\mathrm{GF}(q)$, а не над полем $\mathrm{GF}(q^2)$), как и в предыдущих разделах сложность уменьшается в два раза и ее оценка приобретает вид

$$F(n) \leqslant \frac{31}{16}n\log_2 n + O(n).$$

Такая же оценка получается и для действительного ДПХ.

В [4] для ДПХ (в рассматриваемой ситуации) приведены несколько разных алгоритмов, которые все имеют худшие оценки сложности, чем приведенная выше.

Сложность умножения многочленов степени, меньшей $q/2$, над полем $\mathrm{GF}(q)$ теперь может быть с помощью (2), (6) оценена как

$$\frac{93}{8} q \log_2 q + O(q),$$

где под элементарными операциями понимаются арифметические операции по модулю q. Для мультипликативной сложности в силу (2), (5) получаем оценку

$$\frac{9}{4} q \log_2 q + O(q).$$

9. О БПФ порядка степени тройки в конечных полях

В предыдущих разделах отмечалось, что при $q \pmod 4 = 3$ квадратичное расширение $\mathrm{GF}(q^2)$ поля $\mathrm{GF}(q)$ аналогично полю комплексных чисел, и для этого поля был приведен алгоритм БПФ порядка степени двойки. В некоторых случаях, когда это условие не выполнено, возможно построение БПФ порядка степени тройки.

Пусть $n = 3^k$ и $q+1$ кратно n. Например, это возможно, когда $q = 2^{n/3}$ (среди степеней двойки это число наименьшее, удовлетворяющее указанному условию, в чем можно убедиться индукцией), или когда q — простое число вида $a3^k - 1$ (таких чисел бесконечно много согласно теореме Дирихле, встречаются среди них, например, и числа вида $2 \cdot 3^k - 1$).

Выберем $\xi \in \mathrm{GF}(q^2)$ так, чтобы $\xi^3 = 1$, $\xi \neq 1$ (если $\alpha \in \mathrm{GF}(q^2)$ — первообразный корень, то можно взять $\xi = \alpha^{(q^2-1)/3}$). Тогда элементы поля $\mathrm{GF}(q^2)$ можно представлять в виде $a + b\xi$, а операции над ними проводить по формулам

$$\begin{aligned}(a + b\xi) + (c + d\xi) &= a + c + (b + d)\xi,\\ (a + b\xi)(c + d\xi) &= ac + bd\xi^2 + (bc + ad)\xi\\ &= ac - bd + (bc + ad - bd)\xi\end{aligned}$$

(ввиду равенства $1 + \xi + \xi^2 = 0$).

Указанный базис в рассматриваемом расширении обычно связывают с именем Эйзенштейна (см. [4]). Умножение в нем, если его выполнять по формуле

$$(a + b\xi)(c + d\xi) = ac - bd + (ac - (a - b)(c - d))\xi,$$

требует 3 умножений и 4 сложений (вычитаний) в поле $\mathrm{GF}(q)$. Одно вычитание можно сэкономить в случае, когда умножается произвольный элемент поля $\mathrm{GF}(q^2)$ на фиксированный элемент того же поля, так как это вычитание можно выполнить раз и навсегда заранее. Особенно просто выполняется умножение на элементы ξ и $\xi^2 = -1 - \xi$. Для этого требуется лишь одно вычитание в поле $\mathrm{GF}(q)$.

Отметим еще, что для умножения одного числа $(a + b\xi)$ одновременно на ξ и ξ^2 требуется лишь одна операция вычитания согласно формулам

$$(a + b\xi)\xi = -b + (a - b)\xi, \qquad (a + b\xi)\xi^2 = (b - a) - a\xi$$

(сложность операции смены знака считаем нулевой.)

Пользуясь разложением

$$x^n - 1 = (x^{n/3} - 1)(x^{2n/3} + x^{n/3} + 1) = (x^{n/3} - 1)(x^{n/3} - \xi)(x^{n/3} - \xi^2)$$

ДПФ порядка n можно вычислять по формулам

$$\begin{aligned}
f_{3i} &= (a(x) \pmod{x^{n/3} - 1}) \pmod{x - \omega_n^{3i}},\\
f_{3i+1} &= ((a(x) \pmod{x^{2n/3} + x^{n/3} + 1}) \pmod{x^{n/3} - \xi}) \pmod{x - \omega_n^{3i+1}},\\
f_{3i+2} &= ((a(x) \pmod{x^{2n/3} + x^{n/3} + 1}) \pmod{x^{n/3} - \xi^2}) \pmod{x - \omega_n^{3i+2}},
\end{aligned}$$

где $i = 0, 1, \ldots n/3 - 1$ и ω_n — первообразный корень n-й степени из единицы.

Последние две формулы можно переписать в виде

$$\begin{aligned}
f_{3i+1} &= h_1(x) \pmod{x - \omega_n^{3i}},\\
h_1(x) &= g_1(\omega_n x),\\
g_1(x) &= (a(x) \pmod{x^{2n/3} + x^{n/3} + 1}) \pmod{(x^{n/3} - \xi)},\\
f_{3i+2} &= h_2(\omega_n^2 x) \pmod{x - \omega_n^{3i}},\\
h_2(x) &= g_2(\omega_n x),\\
g_2(x) &= (a(x) \pmod{x^{2n/3} + x^{n/3} + 1}) \pmod{(x^{n/3} - \xi^2)},
\end{aligned}$$

где $0 \leqslant i < n/3$.

Оценим сложность вычисления ДПФ по этой схеме над полем $\mathrm{GF}(q)$. Сложность вычисления остатка $a(x) \pmod{x^{2n/3} + x^{n/3} + 1}$ равна $4n/3$, так как если разбить вектор коэффициентов многочлена $a(x)$ на три вектора a_0, a_1, a_2 длины $n/3$ каждый, так что $a(x)$ будет выражаться через соответствующие многочлены по формуле

$$a(x) = a_0(x) + x^{n/3} a_1(x) + x^{2n/3} a_2(x),$$

то

$$a(x) \pmod{x^{2n/3} + x^{n/3} + 1} = a_0(x) - a_2(x) + (a_1(x) - a_2(x))x^{n/3} \tag{7}$$

(напомним, что сложность вычитания в поле $\mathrm{GF}(q^2)$ равна 2).

Сложность вычисления остатка $a(x) \pmod{x^{n/3} - 1}$ тоже равна $4n/3$, так как

$$a(x) \pmod{x^{n/3} - 1} = a_0(x) + a_1(x) + a_2(x).$$

В случае четного q (поля характеристики два) формула (7) принимает вид

$$a(x) \pmod{x^{2n/3} + x^{n/3} + 1} = a_0(x) + a_2(x) + (a_1(x) + a_2(x))x^{n/3},$$

и если вычислять $a_0(x) + a_1(x) + a_2(x)$ по формуле $(a_0(x) + a_2(x)) + a_1(x)$, то $2n/3$ сложений можно сэкономить.

Для вычисления многочленов $g_i(x)$ нужно $2n/3$ сложений и $n/3$ одновременных умножений на ξ и ξ^2, то есть всего $5n/3$ сложений-вычитаний в поле $\mathrm{GF}(q)$. Указанные вычисления проводятся по формулам

$$\begin{aligned}
g_1(x) &= a_0(x) - a_2(x) + (a_1(x) - a_2(x))\xi,\\
g_2(x) &= a_0(x) - a_2(x) + (a_1(x) - a_2(x))\xi^2,
\end{aligned}$$

которые равносильны стандартным формулам ДПФ третьего порядка

$$g_1(x) = a_0(x) + a_1(x)\xi + a_2(x)\xi^2,$$
$$g_2(x) = a_0(x) + a_1(x)\xi^2 + a_2(x)\xi.$$

Для вычисления каждого из многочленов $h_i(x)$ нужно $n/3-1$ умножений коэффициентов многочлена $g_i(x)$ на корни из единицы ω_n^i, $i = 1, \ldots n/3-1$, что требует $n-3$ умножений и $n-3$ сложений в поле $\mathrm{GF}(q)$. После этого остается 3 раза применить ДПФ порядка $n/3$.

В результате для мультипликативной сложности ДПФ получаем рекуррентную оценку

$$MF(n) \leqslant 3MF(n/3) + 2n - 6,$$

а для аддитивной сложности оценку

$$AF(n) \leqslant 3AF(n/3) + 19n/3 - 6.$$

В случае поля характеристики два последнее соотношение имеет вид

$$AF(n) \leqslant 3AF(n/3) + 17n/3 - 6.$$

Решая рекуррентное соотношение

$$k(n) = 3k(n-1) + a3^n + b,$$

находим, что

$$k(n) = a3^n n + c3^n - b/2.$$

Отсюда выводим оценки

$$MF(n) = 2n\log_3 n + O(n),$$
$$AF(n) = \frac{19}{3} n\log_3 n + O(n),$$
$$F(n) = \frac{25}{3} n\log_3 n + O(n).$$

В случае поля характеристики два последние два равенства имеют вид

$$AF(n) = \frac{17}{3} n\log_3 n + O(n),$$
$$F(n) = \frac{23}{3} n\log_3 n + O(n).$$

В первой оценке мультипликативная константа лучше, а в остальных, кроме последней, хуже, чем в алгоритме [14] (см. также [4]) для ДПФ порядка степени тройки над полем комплексных чисел.

Перенесем и на этот случай результаты предыдущего раздела статьи о ДПФ и ДПХ. Для этого достаточно заметить, что в поле $\mathrm{GF}(q^2)$ можно определить аналог операции комплексного сопряжения равенством

$$\overline{a + b\xi} = a + b\xi^2 = (a-b) - b\xi.$$

Очевидно, что квадрат операции сопряжения, как ему и положено, является тождественным преобразованием и сопряжение сохраняет операции сложения-вычитания и умножения. Например, последнее следует из цепочки сравнений

$$(a+b\xi)(c+d\xi) \equiv e+f\xi \pmod{1+\xi+\xi^2} \Rightarrow$$
$$(a+b\xi^2)(c+d\xi^2) \equiv e+f\xi^2 \pmod{1+\xi^2+\xi^4} \Rightarrow$$
$$(a+b\xi^2)(c+d\xi^2) \equiv e+f\xi^2 \pmod{1+\xi+\xi^2}$$

в силу сравнений

$$\xi^3 \equiv 1 \pmod{1+\xi+\xi^2},$$
$$1+\xi^2+\xi^4 \equiv 0 \pmod{1+\xi+\xi^2}.$$

Через операцию сопряжения стандартным образом определяется норма

$$\|a+b\xi\| = (a+b\xi)\overline{a+b\xi} = (a+b\xi)(a+b\xi^2)$$
$$= a^2+b^2\xi^3+ba(\xi+\xi^2) = a^2+b^2-ba,$$

которая всегда принадлежит полю $\mathrm{GF}(q)$ и благодаря мультипликативному свойству операции сопряжения сама обладает аналогичным свойством.

Благодаря этому свойству для любого $\alpha \in \mathrm{GF}(q^2)$ такого, что $\alpha^n = 1$, его норма $\|\alpha\| \in \mathrm{GF}(q)$ и $\|\alpha\|^n = 1$. Ввиду кратности $q+1$ числу n, числа $q-1$ и n взаимно просты, и, значит, порядок элемента $\|\alpha\|$ равен 1 (ведь согласно малой теореме Ферма он должен быть делителем $q-1$), то есть $\|\alpha\| = 1$ (здесь мы просто проверили, что в поле $\mathrm{GF}(q)$ уравнение $x^n = 1$ имеет только единичное решение). Но у любого элемента с единичной нормой обратный по умножению элемент совпадает с сопряженным, поэтому любой корень n-й степени из единицы в поле $\mathrm{GF}(q^2)$ имеет обратный элемент равный сопряженному, благодаря чему для действительного и комплексного ДПФ порядка n в рассматриваемой ситуации справедливы и все указанные в разделе 7 соотношения между их действительными и комплексными сложностями (иногда при дополнительных ограничениях на q, указываемых далее по ходу дела).

Для обоснования этого утверждения нужно внести лишь небольшие изменения в старые доказательства. Действительно, сохранив старые обозначения (в том числе $\Re z = a$, $\Im z = b$ для $z = a+\xi b$) находим, что

$$F^{\mathbf{C}}(n) \leqslant 2F^{\mathbf{R}}(n) + O(n), \qquad \mathrm{comp}(F_n^{\mathbf{R}}(x), F_n^{\mathbf{R}}(y)) \leqslant F^{\mathbf{C}}(n) + O(n),$$

(где под $\mathrm{comp}(F_n^{\mathbf{R}}(x), F_n^{\mathbf{R}}(y))$ понимается действительная сложность совместного вычисления двух действительных ДПФ), в силу тождеств

$$F_n(z) = F_n(\Re z) + \xi F_n(\Im z),$$
$$F_n^*(z) = \overline{F_n(\bar{z})} = \overline{F_n(\Re z) + \xi^2 F_n(\Im z)},$$
$$\overline{F_n^*(z)} = F_n(\Re z) + \xi^2 F_n(\Im z),$$
$$F_n(\Re z) = \frac{\xi F_n(z) - \overline{F_n^*(z)}}{\xi - 1},$$
$$F_n(\Im z) = \frac{F_n(z) - \overline{F_n^*(z)}}{\xi - \xi^2}.$$

В случае нечетного q над полем $\mathrm{GF}(q^2)$ кроме ДПФ порядка n существует и ДПФ порядка $2n$, поэтому из неравенства Кули–Тьюки ([2]) вытекает, что для действительной сложности действительных ДПФ $F(2n) \leqslant 2F(n)+O(n)$, где под $2F(n)$ можно понимать, в частности, сложность совместного вычисления двух действительных ДПФ порядка n. Отсюда,

$$F^{\mathbf{C}}(n) \leqslant 2F^{\mathbf{R}}(n) + O(n),$$
$$F^{R}(2n) \leqslant F^{\mathbf{C}}(n) + O(n).$$

Для комплексной сложности комплексного ДПФ порядка n, равного степени тройки, справедлива известная оценка

$$F^{\mathbf{C}}(n) = \frac{10}{3} n \log_3 n - 2n/3,$$

вытекающая по индукции из рекуррентного соотношения Кули–Тьюки

$$F^{\mathbf{C}}(n) = 3F^{\mathbf{C}}(n/3) + (n/3)F^{\mathbf{C}}(3) + 2n/3,$$

которое удобно переписать для этого в виде

$$\frac{F^{\mathbf{C}}(n)}{n} + \frac{2}{3} = \frac{F^{\mathbf{C}}(n/3)}{n/3} + \frac{2}{3} + \frac{F^{\mathbf{C}}(3)}{3} + \frac{2}{3},$$

если заметить, что $F^{\mathbf{C}}(3) = 8$, согласно схеме, приведенной, например, в [1].

Следовательно, комплексная сложность действительного ДПФ в рассматриваемом случае не превосходит $(5/3)n \log_3 n + O(n)$.

В случае четного q предыдущее замечание теряет силу, однако с помощью неравенства Кули–Тьюки можно получить более слабую оценку

$$F^{\mathbf{R}}(n) \leqslant 2F^{\mathbf{C}}(n/3) + O(n),$$

которая все же лучше тривиальной оценки

$$F^{\mathbf{R}}(n) \leqslant F^{\mathbf{C}}(n).$$

Кроме того, в этом случае, как известно, $F^{\mathbf{C}}(3) = 7$, и поэтому справедлива оценка $F^{\mathbf{C}}(n) = 3n \log_3 n - 2n/3$, откуда следует, что комплексная сложность действительного ДПФ в этом случае не превосходит $2n \log_3 n + O(n)$.

Можно попытаться определить в рассматриваемой ситуации и ДПХ. Естественно для этого использовать равенство $H_n = aF_n + bF_n^*$ с подходящими $a, b \in \mathrm{GF}(q^2)$. Однако для выполнения условия $H_n^2 = cE_n \in \mathrm{GF}(q^2)$ согласно равенству

$$\begin{aligned} H_n^2 &= (aF_n + b\bar{F}_n)^2 \\ &= a^2F_n^2 + b^2\overline{F_n^2} + ab(F_n\bar{F}_n + \bar{F}_nF_n) = (a^2 + b^2)nI_n + 2abnE_n \end{aligned}$$

необходимо выполнение условия $a^2 + b^2 = 0$, которое влечет разрешимость в поле $\mathrm{GF}(q^2)$ уравнения $x^2 + 1 = 0$, что возможно лишь при нечетном q. Далее пусть q нечетно и $\imath \in \mathrm{GF}(q^2)$ — корень этого уравнения.

Так как матрицы преобразований F_n и F_n^* не пропорциональны, они линейно независимы, и преобразование $H_n = aF_n + bF_n^*$ будет действительным лишь когда

$$aF_n + b\bar{F}_n = H_n = \bar{H}_n = \bar{a}\bar{F}_n + \bar{b}F_n,$$

то есть при условии $a = \bar{b}$, но тогда равенство $a^2 + b^2 = 0$ имеет при подходящих $c, d \in \mathrm{GF}(q)$ вид

$$\begin{aligned} 0 &= (c + d\xi)^2 + (c + d\xi^2)^2 \\ &= c^2 - d^2 + (2cd - d^2)\xi + c^2 + d^2\xi - 2cd\xi - 2cd \\ &= 3c^2 - (c + d)^2, \end{aligned}$$

откуда следует разрешимость в $\mathrm{GF}(q)$ уравнения $x^2 = 3$.

Но если a — корень этого уравнения, то элемент $(a\imath - 1)/2 \in \mathrm{GF}(q^2)$ является кубическим корнем из единицы, так как

$$((a\imath - 1)/2)^3 = (-3a\imath - 3a\imath(a\imath - 1) - 1)/8 = (3a^2 - 1)/8 = 1,$$

причем не равным 1 (так как $3 \neq -9$ в поле $\mathrm{GF}(q)$), значит, он равен либо ξ, либо ξ^2, а элемент $(-a\imath - 1)/2 = ((a\imath - 1)/2)^2$ тогда равен наоборот либо ξ^2, либо ξ, а так как по нашему предположению в поле $\mathrm{GF}(q)$ кубических корней не было, значит, $\imath$ тоже не принадлежит этому полю и его расширение $\mathrm{GF}(q^2)$ имеет также базис $\{1, \imath\}$, причем в силу отмеченных равенств операция сопряжения относительно этого базиса совпадает с операцией сопряжения относительно базиса $\{1, \xi\}$, рассматриваемой в этом разделе.

Благодаря этому в рассматриваемую ситуацию можно перенести и определение ДПХ и все утверждения о нем, а также утверждения, доказываемые с его помощью, аналогично тому, как это сделано в предыдущем разделе.

Можно также без каких-либо изменений перенести в рассматриваемую ситуацию оценку из [14] (см. также [4])

$$F(n) = 8n \log_3 n + O(n),$$

из которой следует оценка для действительного ДПФ

$$F(n) = 4n \log_3 n + O(n),$$

при $n = 2 \cdot 3^k$ и 3^k, делящем $q + 1$.

В частности, можно заметить, что из полученных выше результатов вытекает, что сложность ДПХ оценивается так же, как и сложность действительного ДПФ, то есть

$$H(n) = 4n \log_3 n + O(n),$$

а сложность умножения многочленов той же степени, как обычно, будет в 6 раз больше.

Остается выяснить условие разрешимости в $\mathrm{GF}(q)$ уравнения $x^2 = 3$. Оно совпадает с равенством единице символа Лежандра $\left(\frac{3}{q}\right)$, что в силу квадратичного закона взаимности (его формулировку см., например, в [1]) возможно, лишь когда

$$\left(\frac{q}{3}\right) = (-1)^{(q-1)/2},$$

но

$$\left(\frac{q}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

значит, искомое условие имеет вид $q \equiv 3 \pmod 4$.

В заключение автор выражает глубокую благодарность А. В. Чашкину за ценные советы и полезные обсуждения, в частности, за замечание, позволившее уменьшить в оценке сложности мультипликативную константу с 29/2 до 27/2.

Список литературы

1. Ноден П., Китте К., *Алгебраическая алгоритмика*. Мир, Москва, 1999.
2. Блейхут Р., *Быстрые алгоритмы цифровой обработки сигналов*. Мир, Москва, 1989.
3. Ахо А., Хопкрофт Е., Ульман Д., *Построение и анализ вычислительных алгоритмов*. Мир, Москва, 1979.
4. Власенко В. А., Лаппа Ю. М., Ярославский Л. П., *Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов*. Наука, Москва, 1990.
5. Sorensen H. V., Burrus C. S., Fast DFT and convolution algoritms. In: *Handbook for Digital Signal Processing (Mitra S. K., Ed.)*. Wiley, New York, 1993, pp. 491–610.
6. Брейсуэлл Р., *Преобразование Хартли*. Мир, Москва, 1990.
7. Макклеллан Дж., Рейдер Ч., *Применение теории чисел в цифровой обработке сигналов*. Радио и связь, Москва, 1983.
8. Дэвенпорт Дж., Сирэ И., Турнье Э., *Компьютерная алгебра*. Мир, Москва, 1991.
9. Карацуба А. А., Офман Ю. П., Умножение многозначных чисел на автоматах. *Докл. АН СССР* (1962) **145**, №2, 293–294.
10. Карацуба А. А., Сложность вычислений. *Труды Матем. ин-та им. В. А. Стеклова* (1995) **211**, 1–17.
11. Шенхаге А., Штрассен В., Быстрое умножение больших чисел. *Киберн. сб.* (1973) **10**, 87–98.
12. Schönhage A., Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica* (1977) **7**, 395–398.
13. Гашков С. Б., О сложности интегрирования рациональных дробей. *Труды Матем. ин-та им. В. А. Стеклова* (1997) **218**, 122–133.
14. Suzuki Y., Sone T., Kido K., A new FFT algorithm of radix 3, 6, 12. *IEEE Trans. A.S.S.P.* (1986) **34**, №2, 380–383.

Статья поступила 22.12.1999.