Math-Net.Ru

Общероссийский математический портал

А. А. Болотов, С. Б. Гашков, О быстром умножении
в нормальных базисах конечных полей, *Дискрет. ма-
тем.*, 2001, том 13, выпуск 3, 3–31

DOI: <https://doi.org/10.4213/dm294>

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

Параметры загрузки:

IP: 54.198.55.26

26 апреля 2023 г., 15:23:43

УДК 519.7

О быстром умножении в нормальных базисах конечных полей

© 2001 г. А. А. Болотов, С. Б. Гашков

В статье оценивается сложность переходов от нормальных базисов к стандартным и обсуждаются связанные с этим вопросы эффективной реализации арифметических вычислений в конечных полях высокой размерности.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 99-01-01175, Программы поддержки ведущих научных школ РФФИ, проект 00-15-96103, Программы «Университеты России» и ЦЦП «Интеграция», объединенный проект A0110.

1. Введение

Э. Берлекемп в своей книге [1] написал в шестидесятые годы, что большие конечные поля представляют собой только академический интерес. Сейчас интерес к большим конечным полям с малой характеристикой уже не академический. Без этих полей, к примеру, немыслима современная криптография с открытым ключом (да и с секретным тоже). Вследствие этого, за последние 20 лет существенно возрос интерес к эффективной реализации арифметики конечных полей высокой размерности (от 100 до 1000 и выше), причем как к схемной, так и программной имплементации.

Эффективность реализации арифметических операций в конечных полях заметно зависит от выбора представлений элементов поля, в частности, для этой цели могут быть использованы различные базисы конечных полей.

Особо привлекательно с этой точки зрения выглядят нормальные базисы, поскольку операция возведения в степень q в поле $GF(q^n)$ в этих базисах сводится просто к циклическому сдвигу координат. Хотя нормальные базисы были известны в алгебре уже давно (они были открыты более века тому назад) и многие исследования, проведенные за это время, группировались здесь вокруг вопроса, как их построить (см., например, комментарий к списку литературы в [18]), однако только примерно 12 лет назад алгебраистами-криптографами из Канады ([19]) были открыты оптимальные нормальные базисы, которые позволили по новому подойти к другому важному вопросу, относящемуся к нормальным базисам, как их использовать, что привело к новому всплеску исследований и публикаций на эту тему (см. [6, 13, 14, 15, 18]).

Так как оптимальные нормальные базисы существуют не во всех полях, активно начался также поиск близких к ним нормальных базисов малой сложности (см. [6, 13, 21, 22]).

Отметим, что впервые подобные базисы были обнаружены еще в 1985 г. (до открытия оптимальных нормальных базисов) В. М. Сидельниковым [23], который доказал, что для любого t , делящего $p, q - 1$ или $q + 1$, где $q = p^u$, в поле $GF(q^t)$ существует нормальный базис ω_i с таблицей умножения

$$\omega_i \omega_j = \alpha_{i-j} \omega_i + \alpha_{i+j} \omega_j + \gamma, \quad i \neq j,$$

где индексы у α вычисляются по модулю t , α_k и γ принадлежат $GF(q)$, и выделены случаи, когда $\gamma = 0$.

Интерес к оптимальным нормальным базисам, в частности, связан с их возможными применениями в имплементации криптографии эллиптических кривых (см., например, [2]).

Известные конструкции схем для умножения в конечных полях (как в нормальных, так и в других базисах, см., например, [6]) обычно представляются в виде конечно-автоматных схем, составленных из логических элементов и регистров сдвига с обратной связью. Сложность этих схем (понимаемая как число составляющих их элементов) линейна, но и время вычисления (измеряемое, как правило, в так называемых клок-циклах) тоже линейно зависит от длины входа (размерности поля). Если же представить эти конструкции в виде логических (булевых) схем, то их сложность, естественно, оказывается квадратичной, а время вычисления (задержка) этих схем будет определяться их глубиной и оказывается логарифмически зависящей от числа входов схемы. В случае же программной имплементации указанных алгоритмов время работы будет оцениваться упомянутой булевой (иногда называемой битовой) сложностью этих алгоритмов. Кроме булевой сложности рассматривают также арифметическую сложность, понимаемую обычно как число арифметических операций (в базисном поле) в рассматриваемом алгоритме.

Для указанных мер сложности, однако, известны более быстрые, чем квадратичные, алгоритмы умножения в стандартных базисах, например алгоритм Карацубы или асимптотически более быстрый алгоритм Шенхаге [20]. Основная идея предлагаемой статьи состоит в одновременном использовании в арифметических вычислениях двух базисов — стандартного и нормального — с тем, чтобы использовать их преимущества друг перед другом, а именно, умножение удобно проводить в стандартном базисе (см., например, [8, 9, 10]), а нормальные базисы использовать для того, чтобы быстро возводить в степень q . Естественно, что переходы между двумя базисами также должны выполняться при этом быстро.

Для этой цели в статье исследуется сложность переходов от нормальных базисов к стандартным и обратно, которую мы называем далее транзитивной сложностью нормальных базисов.

Оказывается, что низкой транзитивной сложностью обладают оптимальные нормальные базисы, хотя, вообще говоря, не только они.

Далее мы называем нормальные базисы с низкой транзитивной сложностью нормальными базисами с быстрым умножением. Для быстрого выполнения умножения в таких базисах сперва переходим к подходящему стандартному базису, быстро выполняем там умножение и возвращаемся обратно.

Использование указанных базисов позволяет ускорить стандартные компьютерные алгоритмы экспоненцирования (возведения в произвольную заданную степень) и инвертирования (вычисления обратного элемента). Отметим, что алгоритмы экспоненцирования играют центральную роль во многих криптографических протоколах.

2. Базисы конечных полей

В этом параграфе кратко приводятся основные сведения о стандартных и нормальных (в том числе и оптимальных) базисах. За более полными сведениями читатель отсылается к [6].

2.1. Стандартные и нормальные базисы

Напомним понятия стандартного базиса и нормального базиса в конечных полях. Будем придерживаться стандартных обозначений, принятых в теории конечных полей (см., например, [1, 5, 6, 7]). Через $GF(q^n)$ обозначаем конечное поле порядка q^n , рассматриваемое как расширение степени n поля $GF(q)$ порядка q . В качестве представления элементов поля $GF(q^n)$ используем многочлены степени не более $n - 1$ с коэффициентами из поля $GF(q)$. Если многочлены записаны в стандартном базисе

$$B_\alpha = \{\alpha^0, \alpha^1, \dots, \alpha^{n-1}\}$$

(в этом случае элемент α называем генератором базиса), то сложение элементов поля $GF(q^n)$ сводится к покомпонентному сложению в поле $GF(q)$ векторов коэффициентов, соответствующих данным многочленам, а умножение элементов поля есть умножение соответствующих многочленов над полем $GF(q)$, выполняемое по модулю неприводимого над полем $GF(q)$ многочлена $g(x)$, определяющего рассматриваемое представление поля.

Иногда вместо стандартного базиса удобнее так называемый нормальный базис, то есть базис вида

$$B^\alpha = \{\alpha^{q^0}, \alpha^{q^1}, \dots, \alpha^{q^{n-1}}\},$$

который порождается генератором α стандартного базиса — корнем неприводимого над полем $GF(q)$ многочлена $g(x)$ в своем поле разложения $GF(q^n)$. Нормальный базис существует для любого n (см., например, [1, 6], где подсчитано их количество), но порождается не всяким неприводимым многочленом $g(x)$, так как составляющие его степени элемента α должны быть линейно независимыми над полем $GF(q)$.

Если система степеней

$$\{\alpha^{q^0}, \alpha^{q^1}, \dots, \alpha^{q^{n-1}}\},$$

образует нормальный базис, то любой элемент ζ поля $GF(q^n)$ однозначно представляется в виде

$$\zeta = x_0\alpha + x_1\alpha^q + x_2\alpha^{q^2} + \dots + x_{n-1}\alpha^{q^{n-1}},$$

где $x_0, \dots, x_{n-1}$ — коэффициенты из поля $GF(q)$.

Сложение в нормальном базисе, как и в стандартном, есть покомпонентное сложение векторов коэффициентов в поле $GF(q^n)$.

Возведение в степень q (а значит, и в любую степень q^m) в нормальном базисе представляет собой циклический сдвиг коэффициентов, так как

$$\zeta^q = x_{n-1}\alpha + x_0\alpha^q + x_1\alpha^{q^2} + \dots + x_{n-2}\alpha^{q^{n-1}}.$$

Рассмотрим умножение в нормальных базисах.

Согласно [19] сложностью C_B произвольного нормального базиса

$$B = \{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$$

называется число ненулевых элементов в матрице T , i -я строка которой есть вектор коэффициентов элемента $\alpha\alpha^{q^i}$ поля $GF(q^n)$ относительно базиса B , то есть

$$\alpha\alpha^{q^i} = \sum_{j=0}^{n-1} t_{i,j}\alpha^{q^j}.$$

Это определение мотивируется следующим алгоритмом умножения в нормальном базисе B (алгоритмом Масси–Омуры, см., например, [6]).

Пусть

$$\xi = \sum_{i=0}^{n-1} x_i\alpha^{q^i}, \quad \zeta = \sum_{j=0}^{n-1} y_j\alpha^{q^j}$$

— произвольные элементы поля $GF(q^n)$, разложенные по нормальному базису B . Тогда их произведение можно вычислить по формуле

$$\pi = \xi\zeta = \sum_{i,j=0}^{n-1} x_i y_j \alpha^{q^j + q^i} = \sum_{i,j=0}^{n-1} x_i y_j \alpha^{(q^{i-j} + 1)q^j},$$

где разность $i - j$ вычисляется по модулю n , а так как

$$\begin{aligned} \alpha^{(q^{i-j} + 1)q^j} &= (\alpha^{q^{i-j} + 1})^{q^j} = \left(\sum_{k=0}^{n-1} t_{i-j,k} \alpha^{q^k} \right)^{q^j} \\ &= \sum_{k=0}^{n-1} t_{i-j,k} \alpha^{q^{k+j}} = \sum_{m=0}^{n-1} t_{i-j,m-j} \alpha^{q^m}, \end{aligned}$$

где разность $m - j$ и сумма $k + j$ тоже вычисляются по модулю n , то

$$\pi = \sum_{m=0}^{n-1} p_m \alpha^{q^m},$$

где

$$p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j.$$

Определив матрицу A равенствами $a_{i,j} = t_{i-j,-j}$, где $i - j$ и $m - j$ вычисляются по модулю n , замечаем, что предыдущую формулу можно переписать в виде

$$\begin{aligned} p_m &= \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j = \sum_{k,l=0}^{n-1} t_{k-l,-l} x_{k+m} y_{l+m} \\ &= \sum_{i,j=0}^{n-1} a_{i,j} x_{i+m} y_{j+m} = \sum_{i,j=0}^{n-1} a_{i,j} S^m(x_i) S^m(y_j), \end{aligned}$$

где S^m — операция циклического сдвига координат вектора на m компонент, а

$$A(x, y) = \sum_{i,j=0}^{n-1} a_{i,j} x_i y_j$$

— билинейная форма, связанная с матрицей A .

Матрица A симметрическая и число C_B ее ненулевых элементов, а также сумма элементов такие же, как и у матрицы T . Для вычисления билинейной формы $A(x, y)$ достаточно выполнить $2C_B + n - 1$ сложений и умножений в поле $GF(q)$. Если пренебречь временем выполнения циклических сдвигов, то сложность выполнения умножения над нормальным базисом поля $GF(q^n)$ оценивается сверху как $n(2C_B + n - 1)$ операций в поле $GF(q)$, что видно из следующей основной формулы:

$$\xi\zeta = A(\xi, \zeta)\alpha + A(\xi^{q^{n-1}}, \zeta^{q^{n-1}})\alpha^q + A(\xi^{q^{n-2}}, \zeta^{q^{n-2}})\alpha^{q^2} + \dots + A(\xi^q, \zeta^q)\alpha^{q^{n-1}}.$$

Таким образом, арифметическая сложность умножения зависит только от количества ненулевых элементов C_B в матрице A . Верхняя граница сложности умножения в произвольном нормальном базисе является кубической.

Матрица A (таблица умножения в базисе B) однозначно определяет операцию умножения в рассматриваемом поле.

О сложности нормальных базисов известно следующее ([19]).

Теорема 1. *Для любого нормального базиса B поля $GF(q^n)$ его сложность C_B не меньше $2n - 1$. Более того, если $q = 2$, то сложность нечетна.*

Нормальные базисы, для которых достигается эта граница, называют оптимальными.

2.2. Оптимальные нормальные базисы и нормальные базисы низкой сложности

Оптимальные нормальные базисы были описаны в [19]. Они удачно могут быть использованы в мультиплере Масси–Омуры. Впоследствии в ([14]) было показано, что других оптимальных нормальных базисов, кроме найденных в [19], не существует.

Поскольку оптимальные нормальные базисы существуют не во всех полях, представляют интерес базисы, если и не оптимальные, но имеющие низкую сложность, то есть такие, у которых $C_B(n) = O(n)$. Использование этих базисов в мультиплере Масси–Омуры также приводит к оценке арифметической сложности $O(n^2)$.

В статье [13] такие базисы построены с помощью гауссовых периодов, изучению криптографических приложений которых посвящены статьи [15, 16]. Еще один метод получения базисов с низкой сложностью указан в [21] (см. также [22]).

Базисы Сидельникова [23], вообще говоря, не совсем подходят для использования в мультиплере Масси–Омуры, но его модификация также дает в случае использования этих базисов оценку сложности $O(n^2)$.

Различают три типа оптимальных нормальных базисов в поле $GF(q^n)$ по типу их построения.

Первый тип оптимальных нормальных базисов можно построить, когда $n + 1 = p$ — простое число, а q — примитивный корень по модулю p . В этом случае генератором оптимального нормального базиса будет один из примитивных корней p -й степени из единицы в поле $GF(q^n)$.

Второй тип оптимальных нормальных базисов возникает, когда $2n + 1 = p$ — простое число, а элемент q , как и в первом случае, — примитивный корень по модулю p . Генератором этого базиса служит элемент $\alpha = \zeta + \zeta^{-1}$, где ζ — примитивный корень p -й степени из единицы в поле $GF(q^{2n})$.

Третий тип оптимальных нормальных базисов порождается, когда $2n + 1 = p$ — простое число, $p \equiv 3 \pmod{4}$, а q — квадратичный вычет по модулю p и любой квадратичный вычет представляется в виде степени q по модулю p (или, другими словами, порядок элемента q по модулю p равен n). Как и в случае базиса второго типа в качестве порождающего элемента базиса третьего типа берется $\alpha = \zeta + \zeta^{-1}$, где ζ — примитивный корень p -й степени из единицы в поле $GF(q^{2n})$.

3. О транзитивной сложности оптимальных нормальных базисов

3.1. Оценка сложности перехода от оптимальных нормальных базисов первого типа к стандартным и обратно

Имплементированные стандартные алгоритмы умножения в оптимальных нормальных базисах оказались медленнее ([10]) алгоритмов умножения в стандартных базисах даже в полях небольших размерностей (в диапазоне 150–350), а с ростом размерности они становятся еще хуже. Сравнение двух типов базисов, стандартного и нормального, наводит на мысль об ускорении арифметики в конечных полях за счет использования преимуществ каждого из них. Действительно, умножение быстрее производить в стандартном представлении поля $GF(q^n)$, а возведение в степень — в нормальном представлении.

Для реализации этой идеи понадобятся матрицы перехода от нормального базиса к стандартному и обратно, которые могут оказаться не разреженными, а плотными, и тогда сложность перехода от одного базиса к другому в худшем случае будет $O(n^2 / \log n)$ (даже если использовать для умножения матрицы на вектор метод Лупанова–Коновальцева [12]).

Но в удачном случае сложность перехода может оказаться даже не выше линейной, например, в случае, если число ненулевых элементов в матрицах переходов будет $O(n)$. Таким образом, возникает задача поиска нормальных базисов с легко вычисляемыми матрицами переходов к стандартным базисам и обратно.

Эта задача легко решается в случае оптимальных нормальных базисов первого типа. Напомним, что первый тип нормальных базисов возникает лишь в случае, когда $n + 1 = p$ — простое число и q — примитивный корень по модулю p .

Далее под сложностью понимается арифметическая сложность в классе схем из операций сложения и умножения в основном подполе $GF(q)$.

Теорема 2. *Переход от стандартного базиса поля $GF(q^n)$ к соответствующему (с тем же генератором) оптимальному нормальному базису первого типа (если, конечно, он существует для данного n) и обратно можно выполнить с линейной сложностью.*

Доказательство. Легко видеть, что в этом случае базис $\{\zeta, \dots, \zeta^n\}$ (не совсем стандартный) совпадает с точностью до перестановки с оптимальным нормальным базисом

$$\{\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{n-1}}\},$$

так как последовательность чисел $1, q, q^2, \dots, q^{n-1}$, вычисленных по модулю p , совпадает с некоторой перестановкой последовательности $\{1, 2, \dots, n\}$ в силу того, что

ζ есть примитивный корень p -й степени из единицы в поле $GF(q^n)$, а q — примитивный корень по модулю p .

Поэтому, очевидно, переход от базиса $\{\zeta, \dots, \zeta^n\}$ к нормальному базису

$$\{\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{n-1}}\}$$

и обратно выполняется со сложностью, не большей, чем n .

Отметим попутно, что ζ является корнем неприводимого над полем $GF(q)$ многочлена

$$1 + x + \dots + x^n = \frac{x^p - 1}{x - 1}.$$

Стандартным базисом для перехода будет базис $\{1, \zeta, \dots, \zeta^{n-1}\}$. Очевидно, он с линейной сложностью выражается через базис $\{\zeta, \dots, \zeta^n\}$, поскольку

$$\zeta^n = 1 + \zeta + \dots + \zeta^{n-1},$$

и обратно, базис $\{\zeta, \dots, \zeta^n\}$, благодаря формуле

$$1 = \zeta + \dots + \zeta^{n-1} + \zeta^n,$$

с линейной сложностью выражается через базис $\{1, \zeta, \dots, \zeta^{n-1}\}$. В результате, переход от оптимального нормального базиса

$$\{\zeta, \zeta^q, \zeta^{q^2}, \dots, \zeta^{q^{n-1}}\}$$

к стандартному базису $\{1, \zeta, \dots, \zeta^{n-1}\}$ и обратно выполняется с линейной сложностью.

Умножение в стандартном базисе $\{1, \zeta, \dots, \zeta^{n-1}\}$, как обычно, сводится к умножению многочленов над полем $GF(q)$ и последующей редукции по модулю неприводимого многочлена

$$f(x) = 1 + x + \dots + x^n,$$

соответствующего этому базису. Отметим, что деление с остатком на этот многочлен можно выполнить с линейной сложностью.

Действительно, пусть многочлен $g(x)$ степени $2n - 2$ надо разделить на $f(x)$ и найти остаток (только он нам и нужен), то есть надо представить $g(x)$ в виде

$$g(x) = f(x)h(x) + r(x),$$

где степень $r(x)$ меньше n . Умножив обе части равенства на $x - 1$, получим

$$g(x)(x - 1) = (x^p - 1)h(x) + r(x)(x - 1),$$

а так как степень $r(x)(x - 1)$ меньше $n + 1 = p$, то $r(x)(x - 1)$ — остаток от деления $g(x)(x - 1)$ на $x^p - 1$.

Для умножения $g(x)$ на $x - 1$ достаточно сделать $2n - 2$ сложений (в поле $GF(q)$), а для деления результата на $x^p - 1$ достаточно выполнить $n - 3$ сложений и, наконец, для деления полученного остатка $r(x)(x - 1)$ на $x - 1$ с помощью схемы Горнера достаточно сделать n сложений.

3.2. Оценка сложности перехода от оптимальных нормальных базисов второго и третьего типа к стандартным и обратно (бинарный случай)

Вначале докажем несколько вспомогательных утверждений (первая лемма выполняется также и для общего случая).

Пусть $\alpha = \alpha_1$ — генератор оптимального нормального базиса

$$\{\alpha_1, \dots, \alpha_n\}$$

второго типа поля $GF(q^n)$, он же — генератор соответствующего стандартного базиса

$$\{\alpha^0, \dots, \alpha^{n-1}\}$$

то есть $\alpha_1 = \alpha = \zeta + \zeta^{-1}$, и при любом $k \leq n$

$$\alpha_k = \alpha^{q^{k-1}} = \zeta^{q^{k-1}} + \zeta^{-q^{k-1}},$$

где ζ — примитивный корень из 1 степени $p = 2n + 1$ в поле $GF(q^{2n})$.

Пусть $q = p^r$, где p — простое число и $\alpha = \zeta + \zeta^{-1}$. Рассмотрим вспомогательную последовательность $a_0, a_1, \dots$, порожденную элементом α . Положим $a_0 = 2$ (в случае $p = 2$ естественно $a_0 = 0$) и, далее,

$$a_k = \zeta^k + \zeta^{-k}, \quad k = 1, 2, \dots, \quad a_1 = \alpha_1.$$

Лемма 1. Для любого $k \geq 1$ имеют место следующие рекуррентные соотношения:

$$a_{k+1} = a_k a_1 - a_{k-1},$$

$$a_{p^k} = a^{p^k},$$

$$a_{p^k+i} = a_i a^{p^k} - a_{p^k-i}.$$

Доказательство. Для доказательства первой формулы заметим, что

$$(\zeta^k + \zeta^{-k})(\zeta + \zeta^{-1}) = \zeta^{k-1} + \zeta^{-k+1} + \zeta^{k+1} + \zeta^{-k-1},$$

то есть $a_k a_1 - a_{k-1} = a_{k+1}$.

Вторая формула очевидна.

Третья формула проверяется непосредственно:

$$\begin{aligned} a_{p^k+i} &= \zeta^{p^k+i} + \zeta^{-p^k-i} = (\zeta^{p^k} + \zeta^{-p^k})(\zeta^i + \zeta^{-i}) - (\zeta^{p^k-i} + \zeta^{-p^k+i}) \\ &= a_{p^k} a_i - a_{p^k-i} = a^{p^k} a_i - a_{p^k-i}. \end{aligned}$$

Рекуррентные соотношения, доказанные в лемме, позволяют записать формулы перехода от нормального базиса к почти стандартному базису

$$\{\alpha^1, \dots, \alpha^n\}.$$

Действительно, из леммы следует, что для любого $i \geq 1$ элемент нормального базиса α_i выражается в виде значения некоторого многочлена степени i над полем $GF(q)$, то есть

$$\alpha_i = f_i(\alpha) = \sum_{j=1}^i f_{i,j} \alpha^j.$$

Выразив таким образом все α_i в нормальном базисе, получим матрицу перехода $F_n = (f_{i,j})$ от почти стандартного базиса к нормальному.

Следующие две вспомогательные теоремы относятся к бинарному случаю. В этом случае (то есть, когда $p = 2$) плотность $S(F_n)$ (количество ненулевых элементов) матрицы F_n оценивается следующим образом.

Теорема 3. *Плотность матрицы перехода от стандартного базиса поля $GF(2^n)$ к нормальному базису второго или третьего типа есть $O(n^{\log_2 3})$.*

Доказательство. Согласно формулам леммы 1, матрица F_n , построенная с их помощью, имеет при $n = 2^k - 1$ вид

$$\begin{pmatrix} F_n & o_n & O_n \\ 0 \dots 0 & 1 & 0 \dots 0 \\ G_n & o_n & F_n \end{pmatrix},$$

где o_n — нулевой вектор-столбец высоты n , O_n — нулевая $n \times n$ матрица, матрица G_n есть симметричное отражение матрицы F_n относительно средней строки, то есть $G_n = I_n F_n$, где $I_n = (\delta_{i,n-i+1})$ — матрица с единицами на побочной диагонали и нулями в остальных местах. Например, матрица F_7 имеет вид

$$F_7 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Если разбить матрицу на 4 квадратных подматрицы, удалив среднюю строку и средний столбец, получим, что левый верхний квадрат 3×3 симметричен относительно горизонтали левому нижнему и равен нижнему правому квадрату. Средняя строка и средний столбец содержат ровно одну единицу, лежащую на их пересечении. Матрица является нижнетреугольной с единицами на главной диагонали.

Действительно, в общем случае согласно лемме 1 при $0 \leq i \leq 2^k$

$$\begin{aligned} \sum_{j=1}^{2^k+i} f_{2^k+i,j} \alpha^j &= a_{2^k+i} = a_i a^{2^k} + a_{2^k-i} \\ &= \sum_{j=1}^i f_{i,j} \alpha^{2^k+j} + \sum_{j=1}^{2^k-i} f_{2^k-i,j} \alpha^j, \end{aligned}$$

откуда, $f_{2^k+i,j} = f_{2^k-i,j}$, при $0 \leq j \leq 2^k$, и $f_{2^k+i,2^k+j} = f_{i,j}$, при $1 \leq j \leq 2^k$.

Опираясь на это представление, можно получить следующую рекуррентную формулу для вычисления плотности последовательности матриц F_n :

$$S(F_{2n+1}) = 3S(F_n) + 1, \quad n \geq 3, \quad S(F_3) = 4,$$

из которой вытекает рекуррентная формула

$$S(F_{2^k-1}) = 3S(F_{2^{k-1}-1}) + 1, \quad k \geq 2, \quad S(F_3) = 4.$$

Полагая $l(k) = S(F_{2^k-1})$, перейдем к линейному рекуррентному соотношению

$$l(k) = 3l(k-1) + 1, \quad l(2) = 4,$$

решением которого будет

$$l(k) = (3^k - 1)/2.$$

Полагая $n = 2^k - 1$ и используя представление $3^k = (2^k)^{\log_2 3} = (n+1)^{\log_2 3}$, получим, что

$$S(F_n) = l(k) = ((n+1)^{\log_2 3} - 1)/2 = O(n^{\log_2 3}).$$

В общем случае равенство

$$S(F_n) = O(n^{\log_2 3})$$

сохраняется, так как выбрав k таким образом, что

$$2^k - 1 < n \leq 2^{k+1} - 1,$$

можно заметить, что матрица F_n является главной подматрицей матрицы F_m , $m = 2^k - 1$, откуда следует, что

$$S(F_n) \leq S(F_m) = O(m^{\log_2 3}) = O(n^{\log_2 3}).$$

Оценим теперь плотность матрицы F'_n перехода от стандартного базиса поля $GF(2^n)$ к нормальному. Обозначим B_n матрицу перехода от стандартного базиса к почти стандартному, тогда $F'_n = F_n B_n$, и непосредственно проверяется, что в матрице B_n все элементы нулевые, кроме наддиагональных элементов $b_{i,i+1} = 1$ и некоторых элементов нижней строки $b_{n,j}$, и справедливы следующие равенства для элементов матрицы F'_n :

$$\begin{aligned} f'_{i,1} &= f_{i,n} b_{n,1} = \delta_{i,n} b_{n,1}, \\ f'_{i,j} &= f_{i,j-1} + f_{i,n} b_{n,j} = f_{i,j-1} + \delta_{i,n} b_{n,j}, \end{aligned}$$

так как в силу нижнетреугольности матрицы F_n для ее элементов справедливы равенства $f_{i,n} = \delta_{i,n}$, где $\delta_{i,n}$ — символ Кронекера. Складывая эти равенства, получим, что

$$\begin{aligned} S(F'_n) &= \sum_{i=1, j=1}^{n, n-1} f_{i,j} + \sum_{j=1}^n b_{n,j} = S(F_n) - 1 + \sum_{j=1}^n b_{n,j} \\ &\leq S(F_n) - 1 + n = O(n^{\log_2 3}). \end{aligned}$$

Обозначим $L(F_n)$ сложность линейного преобразования, определяемого матрицей F_n (в данном случае — это наименьшее число операций сложения по модулю два, необходимых для вычисления этого преобразования).

Теорема 4. *Справедлива оценка*

$$L(F_n) \leq \frac{n}{2} \log_2 n + 2n = O(n \log_2 n).$$

Доказательство. Нам будет удобно оценивать сложность преобразования, задаваемого транспонированной матрицей F_n^T , которая равна $L(F_n)$ согласно известной лемме о взаимосвязи сложности транспонированных матриц (см., например, [17]). Впрочем, для дальнейшего нам нужно будет оценить сложность перехода от координат в нормальном базисе $\sum_{i=1}^n x_i \alpha_i$ к координатам в почти стандартном базисе $\sum_{i=1}^n y_i \alpha^i$, которое определяется как раз матрицей F_n^T . Пусть $2^k \leq n < 2^{k+1} - 1$, тогда с использованием формул из леммы 1

$$\begin{aligned} \sum_{i=1}^n y_i \alpha^i &= \sum_{i=1}^n x_i a_i = \sum_{i=1}^{2^k} x_i a_i + \sum_{i=2^k+1}^n x_i a_i \\ &= \sum_{i=1}^{2^k} x_i a_i + \sum_{i=1}^{n-2^k} x_{i+2^k} a_{i+2^k} \\ &= \sum_{i=1}^{2^k} x_i a_i + \sum_{i=1}^{n-2^k} x_{i+2^k} (a^{2^k} a_i + a_{2^k-i}) \\ &= x_{2^k} a_{2^k} + \sum_{i=1}^{2^{k+1}-n-1} x_i a_i + \sum_{i=2^{k+1}-n}^{2^k-1} (x_i + x_{2^{k+1}-i}) a_i + a^{2^k} \sum_{i=1}^{n-2^k} x_{i+2^k} \alpha_i, \end{aligned}$$

определяя векторы-столбцы

$$\begin{aligned} X &= \{x_1, \dots, x_n\}^T, \\ X_1 &= \{x_1, \dots, x_{2^{k+1}-n-1}, x_{2^{k+1}-n} + x_n, \dots, x_{2^k-1} + x_{2^k+1}, x_{2^k}\}^T, \\ X_2 &= \{x_{1+2^k}, \dots, x_n\}^T, \end{aligned}$$

и векторы-строки

$$\begin{aligned} Y_2 &= \{y_{1+2^k}, \dots, y_n\}, \\ Y_1 &= \{y_1, \dots, y_{2^k}\}, \end{aligned}$$

получим, что

$$\begin{aligned} \sum_{i=1}^n y_i \alpha^i &= \sum_{i=1}^n x_i a_i = \sum_{i=1}^{2^k} X_{1,i} a_i + \alpha^{2^k} \sum_{i=1}^{n-2^k} X_{2,i} a_i \\ &= \sum_{i=1}^{2^k} Y_{1,i} a^i + \sum_{i=1}^{n-2^k} Y_{2,i+2^k} a_{i+2^k}, \end{aligned}$$

и значит,

$$F_n^T \otimes X = (y'_1 \dots y'_n) = (Y_1, Y_2) = (F_{2^k}^T \otimes X_1, F_{n-2^k}^T \otimes X_2), \quad (1)$$

где $\otimes$ — операция умножения матрицы на вектор в поле $GF(2)$. Разумеется, последнее равенство можно было получить, основываясь только на структуре матрицы F_n .

Осталось индуктивно оценить сложность преобразования координат, определяемого матрицей F_n^T . Согласно равенству (1)

$$L(2^{m+1}) \leq 2^m - 1 + 2L(2^m), \quad m \leq k-1, \quad L(2) = 2.$$

По индукции непосредственно проверяется, что

$$L(2^m) = 2^{m-1}m + 1.$$

Для произвольного n в пределах $2^k < n < 2^{k+1}$ получим, что

$$L(n) \leq L(2^k) + L(n - 2^k) + n - 2^k.$$

Записывая n в двоичной системе

$$n = 2^{k_s} + \dots + 2^{k_1},$$

где $k_s > \dots > k_1$, получаем, что

$$\begin{aligned} L(n) &\leq 2^{k_s-1}k_s + \dots + 2^{k_1-1}k_1 + s - 1 + (n - 2^{k_s}) + \dots + (n - 2^{k_s} - \dots - 2^{k_2}) \\ &\leq \frac{n}{2} \log_2 n + c \frac{n}{2}, \end{aligned}$$

где

$$c = 1\frac{2}{2} + \frac{3}{4} + \frac{4}{8} + \frac{5}{16} + \dots < 4.$$

Теорема 5. Сложность $B(n)$ перехода в поле $GF(2^n)$ от оптимального нормального базиса второго или третьего типа к соответствующему стандартному базису и наоборот удовлетворяет неравенству

$$B(n) \leq \frac{n}{2} \log_2 n + 3n.$$

Доказательство. Обозначим $\alpha = \zeta + \zeta^{-1}$ генератор стандартного базиса

$$A = \{1, \alpha^1, \dots, \alpha^{n-1}\}$$

и базиса второго или третьего типа

$$B = \{\alpha^{2^0}, \alpha^{2^1}, \dots, \alpha^{2^{n-1}}\}.$$

Переход от нормального базиса к стандартному будет осуществляться через цепочку из четырех базисов

$$B \rightarrow B' \rightarrow A' \rightarrow A$$

и преобразования координат элемента f поля $GF(2^n)$ в этих базисах

$$f = \sum_{i=1}^n x_i \alpha^{2^{i-1}} = \sum_{i=1}^n x'_i a_i = \sum_{i=1}^n y'_i \alpha^i = \sum_{i=1}^n y_i \alpha^{i-1},$$

где

$$a_i = \zeta^i + \zeta^{-i}, \quad B' = \{a_1, \dots, a_n\}, \quad A' = \{\alpha^1, \dots, \alpha^n\}.$$

Переход от базиса B к базису B' и преобразование координат $\tilde{x}$ к координатам $\tilde{x}'$ осуществляется перестановкой базисных элементов, и действительно, существует такая перестановка $\pi(i)$ чисел $\{1, \dots, n\}$, что для любого $i = 1, \dots, 2n$ выполняется равенство

$$2^i \pmod{p} = \pm \pi(i) \in \{1, \dots, n\}. \quad (2)$$

В самом деле, для базиса второго типа последовательность степеней

$$1, 2, 2^2, \dots, 2^{2n-1},$$

вычисленных по модулю p , совпадает с некоторой перестановкой

$$\pi(1), \dots, \pi(2n)$$

множества чисел $\{1, \dots, 2n\}$ в силу того, что 2 — примитивный корень по модулю p . А в силу равенства

$$2^{k+n} = -2^k \pmod{p}.$$

(по теореме Ферма $2^{2n} = 1 \pmod{p}$, значит, $2^n = -1 \pmod{p}$) окончательно получим формулу (2).

В случае базиса третьего типа число 2 является квадратичным вычетом по модулю p , поэтому все степени

$$2^k \pmod{p}, \quad k = 1, \dots, n-1,$$

образуют перестановку множества всех квадратичных вычетов по модулю p , так как их ровно n штук. Добавив к этому тот факт, что p равно 3 по модулю 4, и поэтому -1 является квадратичным невычетом по модулю p , так как в противном случае, существовало бы такое число r , что $-1 = r^2 \pmod{p}$, а это бы приводило к противоречию с теоремой Ферма:

$$r^{p-1} = (r^2)^{(p-1)/2} = (-1)^{(p-1)/2} = -1 \pmod{p},$$

и тот факт, что произведение вычета на невычет является невычетом, получаем, что последовательность $-2^k \pmod{p}$, $k = 0, 1, \dots, n-1$ образует перестановку множества всех квадратичных невычетов по модулю p , в итоге получаем, что и в этом случае верна формула (2).

Таким образом, мы получили, что базис $\{a_1, \dots, a_n\}$ есть просто перестановка базиса $\{\alpha, \dots, \alpha^{2^{n-1}}\}$. Отрицательные индексы можно заменить на соответствующие положительные благодаря равенству $a_i = \zeta^i + \zeta^{-i} = a_{-i}$ по формуле $\alpha^{2^i} = a_{|\pi(i)|}$ (или для координат $x_i = x'_{|\pi(i)|}$). Поэтому далее везде будем считать индексы положительными, и знак модуля числа будем опускать.

Очевидно, что B' — тоже базис, так как он есть просто перестановка базиса B . Можно считать, что сложность перехода $L_{BB'}(n) = O(n)$, а если рассматривать не программную, а схемную имплементацию, то даже $L_{BB'}(n) = 0$.

Переход от базиса B' к базису A' и преобразование координат $\tilde{x}'$ к координатам $\tilde{y}'$. Согласно теореме 4, для сложности этого перехода справедлива оценка

$$L(n) \leq \frac{n}{2} \log_2 n + 2n.$$

Переход от базиса A' к базису A и преобразование координат $\tilde{y}'$ к координатам $\tilde{y}$. По рекуррентной формуле 1 можно в явном виде построить минимальный аннулирующий многочлен m_α (он строится лишь однажды, до применения алгоритма перехода, поэтому сложность его построения в сложности алгоритма не учитывается), то есть

$$m_\alpha = f_n(\alpha) = b_1 \alpha^0 + \dots + b_n \alpha^n = 0, \quad (3)$$

где α — генератор этих базисов и не все коэффициенты b_i равны нулю. Сделаем явный переход от координат $\tilde{y}'$ в почти стандартном базисе A' к координатам $\tilde{y}$ в стандартном A . Учитывая выражение (3), находим, что

$$\sum_{i=1}^n y'_i \alpha^i = \sum_{i=1}^{n-1} y'_i \alpha^i + y'_n \left(\sum_{i=0}^{n-1} b_i \alpha^i \right),$$

и после перегруппировки коэффициентов получаем, что

$$\sum_{i=1}^n y'_i \alpha^i = \sum_{i=1}^{n-1} \alpha^i (y'_i + b_i y'_n) + y'_n \alpha^0 = \sum_{i=1}^{n-1} y_i \alpha^i + y_0 \alpha^0,$$

откуда видно, что для сложности перехода от почти стандартного базиса A' к стандартному A справедлива оценка $L_{A'A}(n) \leq n - 1$.

Итак, мы оценили сложность каждого преобразования, теперь осталось их сложить:

$$L_{BA}(n) = L_{BB'}(n) + L_{B'A'}(n) + L_{A'A}(n) \leq \frac{n}{2} \log_2 n + 3n.$$

Переход от стандартного базиса к нормальному. Теперь покажем, что теорема верна и при обратном переходе, то есть при переходе от стандартного базиса A к базису второго или третьего типа B . Опять определим цепочку переходов, но уже в обратном порядке:

$$A \rightarrow A' \rightarrow B' \rightarrow B.$$

Переход от базиса A к базису A' и от координат $\tilde{y}$ к $\tilde{y}'$. Опять в силу рекуррентной формулы (1) у нас есть минимальный аннулирующий многочлен (3), из явного вида которого мы можем выразить α^0 , а именно,

$$\alpha^0 = \sum_{i=1}^n b_i \alpha^i. \quad (4)$$

Сделаем явный переход от координат $\tilde{y}$ в стандартном базисе A к координатам $\tilde{y}'$ в почти стандартном A' . Приняв во внимание выражение (4)

$$\sum_{i=0}^{n-1} y_i \alpha^i = \sum_{i=1}^{n-1} y_i \alpha^i + y_0 \left(\sum_{i=1}^n b_i \alpha^i \right),$$

после перегруппировки коэффициентов получим, что

$$\sum_{i=0}^{n-1} y_i \alpha^i = \sum_{i=1}^{n-1} \alpha^i (y_i + b_i y_0) + y_0 \alpha^n = \sum_{i=1}^{n-1} y'_i \alpha^i + y'_n \alpha^0,$$

откуда видно, что для сложности перехода от стандартного базиса A к почти стандартному базису A' справедлива оценка $L_{AA'}(n) \leq n - 1$.

Переход от базиса A' к базису B' и преобразование координат $\tilde{y}'$ к координатам $\tilde{x}'$. Рассмотрим преобразование

$$(x'_1 \dots x'_n) = (F_n^{-1})^T \otimes \begin{pmatrix} y''_1 \\ \dots \\ y''_n \end{pmatrix},$$

умножения вектора Y^T на матрицу $(F_{2^{k+1}}^{-1})^T$ (обратную к матрице из теоремы 4) с помощью (1). В этой формуле рекуррентно выполнялись преобразования с векторами X_1 и X_2 , переводящие их в векторы

$$Y_1 = (y_1'', \dots, y_{2^k}''), \quad Y_2 = (y_{2^k+1}', \dots, y_n'),$$

составляющие вектор $Y = (y_1', \dots, y_n')$. Естественно, что обратное преобразование $(F_{n-2^k}^{-1})^T \otimes Y_2^T$ переведет вектор Y_2 в вектор X_2 , а чтобы получить вектор X_1 , надо сделать преобразование $(F_{2^k}^{-1})^T \otimes Y_1^T$. Так как

$$X_1 = \{x_1, \dots, x_{2^{k+1}-n-1}, x_{2^{k+1}-n} + x_n, \dots, x_{2^k-1} + x_{2^k+1}, x_{2^k}\}^T, \\ X_2 = \{x_{1+2^k}, \dots, x_n\}^T,$$

для восстановления вектора $X = \{x_1, \dots, x_n\}$ по этим векторам достаточно к соответствующим $n - 2^k$ компонентам вектора X_1 прибавить (по модулю 2) компоненты вектора X_2 .

Индуктивно продолжая описанное преобразование, мы перейдем к координатам $\tilde{x}'$ в почти нормальном базисе B' со сложностью перехода

$$L^{-1}(n) \leq n - 2^k + L^{-1}(2^k) + L^{-1}(n - 2^k),$$

и, как и раньше, придем к оценке

$$L_{B'A'}(n) \leq \frac{n}{2} \log_2 n + 2n.$$

Переход от базиса B' к базису B и координат $\tilde{x}'$ к $\tilde{x}$ получается посредством перестановки, обратной к $\pi(i)$, (см. (3)), а его сложность оценивается, как и раньше, то есть $L_{B'B}(n) = 0$.

В результате

$$L_{AB}(n) = L_{AA'}(n) + L_{A'B'}(n) + L_{B'B}(n) \leq \frac{n}{2} \log_2 n + 3n.$$

Заметим, что при вычислении обратного преобразования $(F_n^{-1})^T$ при $n = 2^{k+1} - 1$ мы фактически получили матричное тождество

$$(F_n^T)^{-1} = \begin{pmatrix} (F_m^T)^{-1} & o_m & G_m \\ 0 \dots 0 & 1 & 0 \dots 0 \\ O_m & o_m & (F_m^T)^{-1} \end{pmatrix},$$

где $m = (n-1)/2$, а матрица $G_m = I_m(F_m^T)^{-1}$ есть симметричное отражение матрицы $(F_m^T)^{-1}$ относительно средней строки.

Отметим, что это тождество так же, как и аналогичное тождество

$$F_n^{-1} = \begin{pmatrix} F_m^{-1} & o_m & O_m \\ 0 \dots 0 & 1 & 0 \dots 0 \\ G_m & o_m & F_m^{-1} \end{pmatrix}$$

(здесь $m = (n-1)/2$, а матрица $G_m = F_m^{-1}I_m$ есть симметричное отражение матрицы F_m^{-1} относительно среднего столбца) можно проверить и непосредственно. С помощью этих тождеств так же, как и в теореме 3, можно доказать, что плотность обратной матрицы

$$S(F_n^{-1}) = O(n^{\log_2 3})$$

и такую же плотность имеет матрица перехода от нормального базиса второго или третьего типа к стандартному базису поля $GF(2^n)$.

3.3. О явном вычислении формул перехода и минимальных многочленов для оптимальных нормальных базисов

Рассмотрим теперь общий случай $q = p^r$. Определим последовательность многочленов $f_i(x)$ над полем $GF(q)$ рекуррентным соотношением

$$f_{i+1}(x) = x f_i(x) - f_{i-1}(x), \quad f_1(x) = x \quad f_0 = 2.$$

По индукции легко доказать, что

$$f_i(\zeta + \zeta^{-1}) = \zeta^i + \zeta^{-i}$$

для любого элемента ζ .

Как уже отмечалось, эти многочлены задают формулы перехода от стандартных базисов к нормальным в случае базисов второго и третьего типов.

Последовательность $f_i(x)$ можно формально продолжить и для отрицательных индексов, при этом, очевидно, $f_{-i}(x) = f_i(x)$.

Указанная последовательность является некоторым аналогом последовательности многочленов Чебышева, и так же, как и для них, легко проверяется, что многочлены с четными номерами сами четные, то есть содержат только одночлены с четными степенями, а многочлены с нечетными номерами сами нечетные. Поэтому их удобно представлять в виде

$$f_i(x) = \sum_{j=0}^{\lfloor i/2 \rfloor} a_{i,j} (-1)^j x^{i-2j},$$

где коэффициенты будут указаны в лемме 2.

Для рассматриваемой последовательности справедливо тождество Чебышева

$$f_{ij}(x) = f_i(f_j(x)) = f_j(f_i(x)),$$

для проверки которого достаточно положить $x = \zeta + \zeta^{-1}$:

$$f_i(f_j(\zeta + \zeta^{-1})) = f_i(\zeta^j + \zeta^{-j}) = \zeta^{ij} + \zeta^{-ij} = f_{ij}(\zeta + \zeta^{-1}).$$

Легко проверить справедливость еще одного тождества Чебышева

$$f_{i+j}(x) + f_{i-j}(x) = f_i(x) f_j(x).$$

Действительно,

$$\zeta^{i+j} + \zeta^{-i-j} + \zeta^{i-j} + \zeta^{-i+j} = (\zeta^i + \zeta^{-i})(\zeta^j + \zeta^{-j}).$$

Лемма 2. Справедливы следующие равенства (в которых все коэффициенты вычисляются по модулю p):

$$f_i(x) = \sum_{j=0}^{\lfloor i/2 \rfloor} a_{i,j} (-1)^j x^{i-2j},$$

$$a_{i,j} = \binom{i-j}{j} + \binom{i-j-1}{j-1}, \quad x^i = \sum_{j=0}^{\lfloor i/2 \rfloor} \binom{i}{j} f_{i-2j},$$

где для удобства положено $f_0 = 1$.

Доказательство. База индукции проверяется непосредственно. Для обоснования шага индукции ввиду тождества

$$f_{i+1}(x) = xf_i(x) - f_{i-1}(x)$$

достаточно проверить, что $a_{i+1,j} = a_{i,j} + a_{i-1,j-1}$, а это вытекает из тождества Паскаля:

$$\begin{aligned} a_{i,j} + a_{i-1,j-1} &= \binom{i-j}{j} + \binom{i-j-1}{j-1} + \binom{i-j}{j-1} + \binom{i-j-1}{j-2} \\ &= \binom{1+i-j}{j} + \binom{i-j}{j-1} = a_{i+1,j}. \end{aligned}$$

Для доказательства второго тождества достаточно умножить обе его части на x и опять применить тождество Паскаля:

$$\begin{aligned} x^{i+1} = xx^i &= \sum_{j=0}^{\lfloor i/2 \rfloor} \binom{i}{j} x f_{i-2j} = \sum_{j=0}^{\lfloor i/2 \rfloor} \binom{i}{j} (f_{1+i-2j} + f_{i-2j-1}) \\ &= f_{i+1} + \sum_{j=1}^{\lfloor i/2 \rfloor} \left(\binom{i}{j} + \binom{i}{j-1} \right) f_{i-2j-1} = \sum_{j=0}^{\lfloor i/2 \rfloor} \binom{i+1}{j} f_{1+i-2j}. \end{aligned}$$

Для полноты сформулируем известную теорему (см. [6]) о минимальном аннулирующем многочлене генераторов оптимальных нормальных базисов второго и третьего типов.

Теорема 6. Пусть $2n+1$ — простое число и $q = p^r$ — примитивный корень по модулю $2n+1$ или $2n+1 \equiv 3 \pmod{4}$ и q порождает все квадратичные вычеты по модулю $2n+1$, тогда многочлен $g_n(x)$ над $GF(q)$, определенный рекуррентной формулой

$$g_0 = 1, \quad g_1(x) = x + 1, \quad g_k(x) = xg_{k-1}(x) - g_{k-2}(x), \quad k \geq 2,$$

совпадает с минимальным аннулирующим элементом α многочленом m_α и его корни образуют оптимальный нормальный базис второго или, соответственно, третьего типа поля $GF(q^n)$.

В дополнение к этой теореме мы укажем, как можно явно вычислить коэффициенты минимального многочлена. Действительно, используя указанную рекуррентную формулу, по индукции можно проверить, что $g_k(x) - g_{k-1}(x) = f_k(x)$ при $k > 0$, то есть

$$g_k(x) = f_k(x) + \dots + f_1(x) + 1,$$

а поэтому, если

$$g_n(x) = \sum_{j=0}^n g_{n,j} x^j,$$

то согласно теореме 6

$$g_{n,j} = \sum_{i=0}^{\lfloor (n-j)/2 \rfloor} a_{2i+j,i} (-1)^i = (-1)^{\lfloor (n-j)/2 \rfloor} \binom{\lfloor (n+j)/2 \rfloor}{j}$$

(все вычисления проводятся по модулю p). В случае $p = 2$ множитель $(-1)^{\lfloor (n-j)/2 \rfloor}$, естественно, можно опустить.

В силу известной теоремы Люка (см., например, [3]) биномиальный коэффициент $\binom{a}{b}$ по модулю p можно вычислить за $O(\nu_p(b))$ операций в поле $GF(p)$ по формуле

$$\prod_{i=1}^m \binom{a_i}{b_i},$$

где $0 \leq a_i, b_i < p, 1 \leq i \leq m$, — цифры p -ичного разложения a и b соответственно,

$$\nu_p(b) = \sum_{i=1}^m b_i.$$

Поэтому, последовательно вычисляя путем прибавления единицы p -ичные разложения $\lfloor (n+j)/2 \rfloor$ и j и используя сделанное замечание, можно вычислить все коэффициенты многочлена $g_n(x)$ со сложностью $O(pn \log_p n)$.

Такое же утверждение, естественно, справедливо и для сложности вычисления многочлена $f_n(x)$. Для вычисления всей последовательности многочленов $f_1(x), \dots, f_n(x)$ или $g_1(x), \dots, g_n(x)$ естественно, конечно, использовать определяющую ее рекуррентную формулу с квадратичной оценкой сложности.

3.4. Оценка сложности перехода от оптимальных нормальных базисов второго и третьего типа к стандартным в общем случае

Пусть теперь $2n+1$ — простое число, а $q = p^r$ — или примитивный корень по модулю $2n+1$, или $2n+1 \equiv 3 \pmod{4}$ и q порождает все квадратичные вычеты по модулю $2n+1$. Пусть ζ — примитивный корень из единицы степени $2n+1$ в поле $GF(q^{2n})$, $\alpha_i = \zeta^i + \zeta^{-i}, \alpha = \alpha_1$. Тогда, как отмечалось выше, $\{\alpha_1, \dots, \alpha_n\}$ является оптимальным нормальным базисом (точнее, его перестановкой) в поле $GF(q^n)$, которое можно рассматривать как векторное пространство над полем $GF(q)$.

Рассмотрим в нем m -мерное, $m \leq n$, подпространство, порожденное базисом $\{\alpha_0, \dots, \alpha_{m-1}\}$ или эквивалентным базисом $\{1, \alpha, \dots, \alpha^{m-1}\}$. Обозначим $L(m)$ сложность преобразования координат от базиса $\{\alpha_0, \dots, \alpha_{m-1}\}$ к базису $\{1, \alpha, \dots, \alpha^{m-1}\}$ и обратно (под сложностью понимается число арифметических операций в поле $GF(q)$).

Теорема 7. При $m \leq n$

$$L(m) = O(pm \log_p m).$$

Доказательство. Сначала докажем для $s = p^k s', m \leq s$ неравенство

$$L(s+m) \leq L(s) + L(m) + m(3s'/2 + 2). \quad (5)$$

Заметим, что $\alpha_i = f_i(\alpha)$ и положим $\alpha_0 = 1$. Возьмем разложение произвольного элемента в базисе $\{\alpha_0, \dots, \alpha_{s+m-1}\}$

$$\sum_{i=0}^{s-1} x_i \alpha_i + \sum_{i=0}^{m-1} x_{i+s} \alpha_{i+s}. \quad (6)$$

Так как $\alpha_{i+s} = \alpha_s \alpha_i - \alpha_{s-i}$, разложение (6) можно переписать в виде

$$\sum_{i=0}^{s-1} y_i \alpha_i + \alpha_s \sum_{i=0}^{m-1} z_i \alpha_i, \quad (7)$$

где $y_i = x_i - x_{2s-i}$, $i \geq s - m + 1$, $y_i = x_i$ в остальных случаях, $z_i = x_{i+s}$, $i > 0$, $z_0 = x_s/2$, $i > 0$. Преобразование от (6) к (7) можно выполнить со сложностью m и с той же сложностью выполняется обратное преобразование.

Со сложностью $L(s) + L(m)$ можно вычислить векторы коэффициентов (y'_i) , (z'_j) такие, что рассматриваемый элемент можно записать в виде

$$\sum_{i=0}^{s-1} y'_i \alpha^i + \alpha_s \sum_{i=0}^{m-1} z'_i \alpha_i. \quad (8)$$

Согласно лемме 2

$$\alpha_s = \alpha_{p^k s'} = f_{s'}(\alpha_{p^k}) = f_{s'}(\alpha^{p^k}) = \sum_{j=0}^{\lfloor s'/2 \rfloor} a_{s',j} (-1)^j \alpha^{(s'-2j)p^k}, \quad (9)$$

причем в этой формуле число коэффициентов, отличных от единицы, не более $\lfloor s'/2 \rfloor$. Используя (9) можно при $m < s$ преобразовать (8) к виду

$$\sum_{i=0}^{s+m-1} x'_i \alpha^i \quad (10)$$

со сложностью $(s' + 1)m$. В результате сложность прямого преобразования оценивается сверху величиной

$$L(s) + L(m) + m(s' + 2).$$

Обратно, со сложностью $L(s) + L(m)$ можно вычислить векторы коэффициентов (v_i) , (w_j) такие, что (10) преобразовываются к виду

$$\sum_{i=0}^{s-1} v_i \alpha_i + \alpha^s \sum_{i=0}^{m-1} w_i \alpha_i. \quad (11)$$

Согласно лемме 2

$$\begin{aligned} \alpha^s &= (\alpha_{p^k})^{s'} = \sum_{j=0}^{\lfloor s'/2 \rfloor} \binom{s'}{j} f_{s'-2j}(\alpha_{p^k}) \\ &= \sum_{j=0}^{\lfloor s'/2 \rfloor} \binom{s'}{j} \alpha_{(s'-2j)p^k}. \end{aligned} \quad (12)$$

Используя (12) (и заменяя, если нужно, α_0 на 2) можно преобразовать (11) к виду

$$\sum_{i=0}^{s-1} v_i \alpha_i + \sum_{i=0}^{m-1} \sum_{j=0}^{\lfloor s'/2 \rfloor} b_j w_i \alpha_i \alpha_{(s'-2j)p^k} \quad (13)$$

со сложностью $(\lfloor s'/2 \rfloor)m$ и, заменяя произведение $\alpha_i \alpha_{(s'-2j)p^k}$ на

$$\alpha_{i+(s'-2j)p^k} + \alpha_{i-(s'-2j)p^k},$$

преобразуем (13) к виду

$$\sum_{i=0}^{s+m-1} x_i \alpha_i$$

со сложностью $(2(\lfloor s'/2 \rfloor) + 1)m$. В результате сложность и обратного преобразования оценивается сверху величиной

$$L(s) + L(m) + m(3s'/2 + 2),$$

значит, неравенство (5) доказано.

Докажем теперь рекуррентное неравенство

$$L(p^{k+1}) \leq pL(p^k) + \frac{3}{4}p^{k+2} + p^{k+1} \lceil \log_2 p \rceil. \quad (14)$$

Для этого представим p в виде $s + m$, где $s = \lceil p/2 \rceil$, $m = \lfloor p/2 \rfloor$, и, применяя (5), получим, что

$$L(p^{k+1}) \leq L(p^k s) + L(p^k m) + p^k(3sm/2) + p^k(s + m).$$

Применяя (5) и тот же прием деления пополам к оценкам $L(p^k s)$, $L(p^k m)$ и далее, получаем по индукции, что при любом $s \leq p$

$$L(p^k s) \leq sL(p^k) + p^k \lambda(s),$$

где функция λ удовлетворяет неравенству

$$\lambda(s + m) \leq \lambda(s) + \lambda(m) + 3sm/2 + s + m, \quad \lambda(1) = 0.$$

Далее по индукции проверяется, что

$$\lambda(s) \leq \frac{3}{4}s^2 + s \lceil \log_2 s \rceil,$$

откуда и следует (14).

Из (14) по индукции выводится неравенство

$$L(p^k) \leq \frac{3}{4}p^{k+1}k + p^k k \lceil \log_2 p \rceil,$$

а из него неравенство

$$\begin{aligned} L(p^k s) &\leq sL(p^k) + p^k \lambda(s) \\ &\leq \frac{3s}{4}p^{k+1}k + p^k s k \lceil \log_2 p \rceil + \frac{3}{4}s^2 p^k + p^k s \lceil \log_2 s \rceil \\ &\leq \frac{3s}{4}p^{k+1}k + p^k s k \lceil \log_2 p \rceil + O(p^{k+1}). \end{aligned} \quad (15)$$

Разлагая n в p -ичной системе

$$n = n_0 p^k + \dots + n_k = N_0 + N_1, \quad N_0 = n_0 p^k,$$

и применяя (5) и (15), находим, что

$$\begin{aligned} L(n) &\leq L(N_0) + L(N_1) + N_1(3n_0/2 + 2) \\ &\leq L(N_1) + n_0 p^k (3pk/4 + k \lceil \log_2 p \rceil) + O(p^{k+1}). \end{aligned}$$

Повторяя указанный прием, получаем неравенства

$$\begin{aligned} L(n) &\leq (n_0 p^k + \dots + n_k) k (3p/4 + \lceil \log_2 p \rceil) + O(p^{k+1}) \\ &\leq nk(3p/4 + \lceil \log_2 p \rceil) + O(pn) = O(pnk). \end{aligned}$$

Обозначим $B(n)$ сложность перехода от оптимального нормального базиса второго или третьего типа к соответствующему стандартному или наоборот в поле $GF(q^n)$.

Справедливо следующее обобщение теоремы 5.

Теорема 8. *Справедлива оценка*

$$B(n) = O(pn \log_p n).$$

Доказательство. Доказательство в целом аналогично доказательству теоремы 5. Переход от нормального базиса

$$B_\alpha = \{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$$

к базису $\{\alpha_1, \dots, \alpha_n\}$ делается путем перестановки элементов, как и при доказательстве теоремы 5. Так как суммы элементов обоих базисов равны и равны следу элемента α , эта сумма принадлежит полю $GF(q)$ и не равна нулю (иначе элементы базиса были бы линейно зависимы). Поэтому базис $\{\alpha_1, \dots, \alpha_n\}$ эквивалентен базису $\{\alpha_0, \dots, \alpha_{n-1}\}$ и переход от одного из них к другому выполняется с линейной сложностью подобно переходу от стандартного базиса к почти стандартному в доказательстве теоремы 5.

Для оценки сложности перехода от базиса $\{\alpha_0, \dots, \alpha_{n-1}\}$ к стандартному базису $\{1, \dots, \alpha^{n-1}\}$ и обратно используем вместо теоремы 4 теорему 7.

3.5. О мере близости нормальных базисов к стандартным

Обозначим $C_{q,\beta}^\alpha(n)$ сложность перехода в поле $GF(q^n)$ от нормального базиса B^α к стандартному базису B_β , точнее, максимум из сложностей прямого и обратного преобразования координат в одном базисе к координатам в другом. Тогда

$$C_q^\alpha(n) = \min C_{q,\beta}^\alpha(n)$$

есть мера близости нормального базиса B^α к стандартным базисам.

Очевидно,

$$C_q^\alpha(n) \leq C_{q,\alpha}^\alpha(n).$$

Введем еще две функции

$$c_q(n) = \min C_q^\alpha(n)$$

и

$$C_q(n) = \max C_q^\alpha(n).$$

Тогда результаты предыдущих пунктов можно переформулировать следующим образом.

Если в поле $GF(q^n)$ существует оптимальный нормальный базис первого типа, то

$$c_q(n) \leq n - 1,$$

а если нет, но существует базис второго или третьего типа, то

$$c_q(n) \leq O(n \log_2 n).$$

Используя метод Лупанова–Коновальцева (см. [12]) для оценки сложности произвольного n -мерного линейного оператора над полем $GF(q)$, можно показать, что

$$C_q(n) = O(n^2 / \log_q n).$$

Теорема 9. *Справедлива оценка*

$$C_q(n) - c_q(n) \leq 2M_q(n) + n = O(n \log n \log \log n).$$

Доказательство. Пусть

$$c_q(n) = C_{q,\beta}^\alpha(n), \quad C_q(n) = C_{q,B}^A(n).$$

Тогда

$$C_q(n) - c_q(n) \leq C_{q,\beta}^A(n) - C_{q,\beta}^\alpha(n).$$

Очевидно, что сложность произведения линейных операторов не превосходит сумму их сложностей, поэтому

$$C_q(n) - c_q(n) \leq C_q^{A,\alpha}(n),$$

где $C_q^{A,\alpha}(n)$ — сложность перехода от нормального базиса B^α к нормальному базису B^A . Если базисы совпадают, то сложность, очевидно, равна нулю. В противном случае, как известно ([5, 6]), матрица перехода от нормального базиса к другому нормальному базису является циклической, также как и транспонированная к ней матрица замены координат в этих базисах.

Сложность оператора с циклической матрицей равна сложности оператора так называемой циклической свертки, которая, как известно (см. например [3]), сводится к двум преобразованиям обычной свертки и n операциям сложения, а обычная свертка — это не что иное, как операция умножения двух многочленов степени $n - 1$. Отсюда и вытекает утверждение теоремы.

Поведение функции $c_q(n)$ в общем случае авторам неизвестно.

4. О сложности имплементации арифметических операций в конечных полях

4.1. Об оценках сложности арифметических операций в конечных полях

Пусть конечное поле $GF(q^n)$ представлено стандартным базисом B_α , порожденным корнем α неприводимого над $GF(q)$ многочлена $g(x)$ степени n . Сложность операции умножения многочленов степени $n - 1$ над полем $GF(q)$ обозначим $M_q(n)$. Согласно [20],

$$M_q(n) = O(n \log n \log \log n).$$

Обозначим $M_{q,g}^s(n)$ сложность операции умножения в указанном представлении поля $GF(q^n)$. Так как умножение в рассматриваемом случае сводится к умножению многочленов над полем $GF(q)$ и последующему делению результата на многочлен $g(x)$ с остатком, то независимо от выбора $g(x)$ известна оценка

$$M_{q,g}^s(n) = 3M_q(n) + O(n),$$

если пренебречь сложностью предварительного вычисления некоторого многочлена $f(x)$, зависящего только от $g(x)$. Далее иногда будем опускать индексы в формуле $M_{q,g}^s(n)$.

В некоторых случаях эту оценку можно улучшить. Действительно, если $g(x)$ содержит k одночленов, то сложность редукции по модулю $g(x)$ оценивается как kn и поэтому

$$M_{q,g}^s(n) \leq M_q(n) + (2k + 1)n,$$

а в случае $q = 2$ соответственно

$$M_{q,g}^s(n) \leq M_q(n) + kn.$$

С высокой вероятностью в качестве k можно взять 3, а если неприводимого трехчлена степени n не существует, то, как проверено экспериментально, но не доказано теоретически, всегда можно взять $k = 5$, так как существует неприводимый пятичлен. О сложности алгоритмов генерации неприводимых малочленов см., например, [11].

В указанных выше оценках сложность аддитивных операций и умножения в поле $GF(q)$ принимается за единицу. В случае $q = 2$ это естественно. Если же $q = p^k$, где p — простое число, то естественно также оценить битовую сложность операции умножения в поле $GF(q)$ как

$$\begin{aligned} M(GF(q)) &\leq M(GF(p))M_q^s(k), \\ M(GF(p)) &\leq 3M(\log_2 p) + O(\log_2 p), \end{aligned}$$

где $M(m) = O(m \log m \log \log m)$ — битовая сложность умножения m -разрядных двоичных чисел. Отметим еще, что для p , являющихся простыми Мерсенна или Ферма, справедлива оценка

$$M(GF(p)) \leq M(\log_2 p) + O(\log_2 p).$$

Для битовой сложности операции умножения в поле $GF(q^n)$ (при условии задания элементов поля их координатами в данном базисе B над полем $GF(q)$) справедлива оценка

$$M(GF(q^n)) \leq M(GF(q))M_{q,g}^s(n).$$

Возведение в степень q элемента поля $GF(q^n)$ производится путем вставки нулей в последовательность коэффициентов полинома, представляющего этот элемент, после чего производится редукция по модулю g , в результате (с учетом сделанного выше замечания) получаем (теоретически не доказанную) оценку сложности возведения в степень $K_q(n) = O(n)$.

Оценим сложность умножения в поле $GF(q^n)$ в случае использования оптимального нормального базиса первого типа и операций из поля $GF(q)$. Для выполнения умножения переходим к стандартному базису согласно теореме 2 со (схемной) сложностью $2n - 2$, затем делаем умножение в стандартном базисе и переходим обратно к нормальному базису со сложностью $n - 1$.

Согласно сделанному после теоремы 2 замечанию, получаем оценку

$$M^{O1}(GF(q^n)) \leq M_q^s(n) + 7n - 8.$$

В случае базисов второго и третьего типа аналогично получаем оценку

$$M^{O2}(GF(q^n)) \leq 3M_q^s(n) + \frac{3n}{2} \log_2 n + O(n),$$

которая оказывается асимптотически в три раза хуже, так как в соответствующих стандартных базисах порождающий их неприводимый многочлен (вычисленный в теореме 6) оказывается нетривиальным и для редукции по его модулю приходится использовать для оценки $M_g(n)$ указанную выше общую оценку.

Далее через $M^O(GF(q^n))$ обозначаем минимальную сложность умножения в поле $GF(q^n)$ при условии задании элементов поля в некотором нормальном базисе.

4.2. Об оценках сложности экспоненцирования и инвертирования в конечных полях

Заметим, что сложность возведения произвольного элемента поля $GF(q^n)$ в степень $d < q^n$ (при использовании операций из поля $GF(q)$) можно оценить, применяя некоторые результаты об аддитивных цепочках [4], как

$$O\left(n \log_q d + \frac{M(GF(q^n)) \log_q d}{\log_q \log_q d}\right),$$

так как для возведения в степень d достаточно $\log_q d + O(1)$ возведений в степень q и асимптотически $\log_q d / \log_q \log_q d$ нетривиальных умножений.

Известно, что для почти всех d второе слагаемое по порядку нельзя уменьшить, но, например, для $d = q^n - 2$ это сделать можно, опираясь на равенства

$$\begin{aligned} q^n - 2 &= q(q^{n-1} - 1) + q - 2, \\ q^{2m} - 1 &= (q^m - 1)(q^m + 1), \\ q^{2m+1} - 1 &= q(q^{2m} - 1) + q - 1. \end{aligned}$$

Так как согласно тождеству Ферма $f^{-1} = f^{q^n-2}$, для операции инвертирования в поле понадобится не более

$$\lambda_2(n-1) + \nu_2(n-1) + \log_2 q + o(\log_2 q)$$

умножений и $n-1$ возведение в q -ю степень, где $\lambda_2(n) = \lceil \log_2(n-1) \rceil$, а $\nu_2(n)$ — число единиц в двоичной записи числа n . Поэтому для сложности инвертирования в стандартном базисе справедлива оценка

$$I(GF(q^n)) \leq (n-1)K_q(n) + (\lambda_2(n-1) + \nu_2(n-1) + \log_2 q + o(\log_2 q))M(GF(q^n)),$$

и так же оценивается сложность деления $D(GF(q^n))$.

Оценим сложность инвертирования в оптимальных нормальных базисах (случай стандартных базисов изучался в [9]).

Возведение в степень q выполняется бесплатно, поэтому справедлива оценка

$$I^O(GF(q^n)) \leq (\lambda_2(n-1) + \nu_2(n-1) + \log_2 q + o(\log_2 q))M^O(GF(q^n)),$$

которая справедлива только для тех n , для которых существуют такие базисы. Аналогично, сложность возведения в произвольную степень $d < q^n$ в оптимальных нормальных базисах оценивается как

$$O\left(\frac{M^O(GF(q^n)) \log d}{\log \log d}\right).$$

4.3. Еще об оценках сложности умножения в нормальных базисах

Выше было показано, что сложность умножения в конечных полях при использовании оптимальных нормальных базисов асимптотически остается такой же, как и в стандартных базисах. Но такие базисы существуют не для всех значений n . Далее мы приведем примеры других нормальных базисов, для которых сложность умножения все еще остается меньшей, чем тривиальная квадратичная оценка.

В [13] были приведены примеры нормальных базисов B , у которых функция сложности S_B является линейной. Стандартный алгоритм умножения для таких базисов имеет квадратичную оценку сложности. Указанные базисы B^α порождаются в полях $GF(q^n)$ элементами вида $\alpha = \zeta + \zeta^\gamma + \dots + \zeta^{\gamma^{k-1}}$, где $p = kn + 1$ — простое число, ζ — примитивный корень p -й степени из единицы в поле $GF(q^{kn})$, являющемся расширением поля $GF(q^n)$, γ — примитивный корень k -й степени из единицы в кольце вычетов порядка p , который вместе с q порождает всю мультипликативную группу ненулевых вычетов по модулю p , то есть каждое число от 1 до kn представимо единственным образом в виде $q^i \gamma^j$, $0 \leq j < k$, $0 \leq i < n$.

Известно, что в этом случае минимальным аннулирующим элементом m_ζ над полем $GF(q)$ является круговой многочлен

$$F_{p-1} = x^{p-1} + \dots + 1,$$

и поле $GF(q^n)$ порождается стандартным базисом $B_\zeta = \{1, \zeta, \dots, \zeta^{kn-1}\}$.

Так как элементы базиса B^α имеют вид $\alpha^{q^i} = \zeta^{q^i} + \zeta^{\gamma q^i} + \dots + \zeta^{\gamma^{k-1} q^i}$, то есть являются суммами разных элементов почти стандартного базиса $B'_\zeta = \{\zeta, \dots, \zeta^{kn}\}$, матрица перехода от координат в базисе B^α к координатам в базисе B'_ζ имеет по одной единице в каждой строке и поэтому соответствующее преобразование имеет нулевую схемную сложность (и линейную сложность в случае программной имплементации). Обратное преобразование (определенное, конечно, только на соответствующем подпространстве) также по тем же причинам имеет нулевую схемную сложность. Сложность прямого и обратного перехода от стандартного базиса B_ζ к почти стандартному базису B'_ζ над полем $GF(q)$ была фактически оценена в доказательстве теоремы 2 и равна в рассматриваемом случае $kn - 1$.

Согласно сделанному после теоремы 2 замечанию, получаем оценку сложности умножения в базисе B_ζ

$$M_{q, F_{kn}}^s(kn) \leq (M_q^s(kn) + 4kn - 5),$$

откуда получаем оценку сложности умножения в нормальном базисе B^α

$$M^O(GF(q^n)) \leq (M_q^s(kn) + 7kn - 8)M(GF(q)). \quad (16)$$

В случае $k = 1, 2$ рассматриваемые базисы являются базисами первого и второго типов и при $k = 1$ полученная оценка превращается в оценку, приведенную в предыдущем пункте. Отметим, что идея использования в этом случае перехода к стандартному базису B_ζ впервые, видимо, появилась в сообщении Д. Дама (представленном в Интернете). При $k = 2$ указанная оценка асимптотически несколько лучше оценки

$$M^{O^2}(GF(q^n)) \leq (3M_q^s(n) + \frac{3n}{2} \log_2 n + O(n))M(GF(q)),$$

полученной выше для базисов как второго, так и третьего типов, так как $M_q^s(2n)$ асимптотически меньше $3M_q^s(n)$, но практически вопрос сравнения этих оценок не так очевиден. При больших k эффективность оценки (16) ухудшается, но при $k = O(n^{1-\varepsilon})$ она еще остается бесконечно малой в сравнении с квадратичной оценкой.

4.4. О произведениях базисов

Известна следующая конструкция (кронекерова) произведения базисов (см., например, [5, 6]). Пусть m и n — взаимно простые числа, а

$$B_1 = \{\alpha_1, \dots, \alpha_n\}, \quad B_2 = \{\beta_1, \dots, \beta_m\}$$

— произвольные базисы в полях $GF(q^n)$ и $GF(q^m)$ соответственно. Тогда пересечение этих полей совпадает с полем $GF(q)$, и оба поля содержатся в поле $GF(q^{nm})$, базисом в котором (над полем $GF(q)$) будет произведение базисов

$$B_1 \otimes B_2 = \{\alpha_1\beta_1, \dots, \alpha_n\beta_m\}.$$

Произведение стандартных базисов не будет стандартным базисом и нетривиальной оценки меры близости этого базиса к стандартному авторам неизвестно. Однако для этого произведения базисов сложность умножения в поле $GF(q^{nm})$ легко оценивается:

$$M_{B_1 \otimes B_2}(GF(q^{nm})) \leq M_{B_1}(GF(q^n))M_{q^n, g}^s(m) \leq M_{q, f}^s(n)M_{q^n, g}^s(m), \quad (17)$$

где g — неприводимый полином степени m над полем $GF(q)$, порождающий базис B_2 , а f — неприводимый полином степени n над полем $GF(q)$, порождающий базис B_1 .

Однако, как известно [5, 6], произведение $B^\alpha \otimes B^\beta$ нормальных базисов $B^\alpha \subset GF(q^n)$ и $B^\beta \subset GF(q^m)$ с точностью до перестановки элементов совпадает с нормальным базисом

$$B^\gamma \subset GF(q^{nm}), \quad \gamma = \alpha\beta.$$

Рассмотрим также произведение стандартных базисов $B_\alpha \otimes B_\beta$. Легко видеть, что сложность перехода от базиса $B^\alpha \otimes B^\beta$ к базису $B_\alpha \otimes B_\beta$ оценивается сверху величиной

$$nC_{q, \beta}^\beta(m) + mC_{q, \alpha}^\alpha(n). \quad (18)$$

Действительно, если произвольный элемент поля $GF(q^{nm})$ записывается в обоих базисах как

$$\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x_{i,j} \alpha^{q^i} \beta^{q^j} = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j,$$

то для преобразования матрицы $(x_{i,j})$ над полем $GF(q)$ в матрицу $(x'_{i,j})$ над тем же полем достаточно n раз выполнить (в соответствующую сторону) преобразование $C_{q,\beta}^\beta(m)$ над строками матрицы $(x_{i,j})$, чтобы получить равенство

$$\sum_{i=0}^{n-1} \alpha^{q^i} \sum_{j=0}^{m-1} x_{i,j} \beta^{q^j} = \sum_{i=0}^{n-1} \alpha^{q^i} \sum_{j=0}^{m-1} x''_{i,j} \beta^j,$$

а потом m раз выполнить преобразование $C_{q,\alpha}^\alpha(n)$ над столбцами полученной матрицы $(x''_{i,j})$ над тем же полем $GF(q)$, чтобы получить равенство

$$\sum_{i=0}^{n-1} \alpha^{q^i} \sum_{j=0}^{m-1} x''_{i,j} \beta^j = \sum_{j=0}^{m-1} \beta^j \sum_{i=0}^{n-1} x''_{i,j} \alpha^{q^i} = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j.$$

Из (17) и (18) следует, что при подходящем выборе элементов α и β (или, что то же самое, многочленов f и g) и при $\gamma = \alpha\beta$ для сложности умножения в нормальном базисе в поле $GF(q^{nm})$ справедлива оценка

$$\begin{aligned} M^O(GF(q^{nm})) &\leq M_{B^\gamma}(GF(q^{nm})) \leq M_{q,f}^s(n) M_{q^n,g}^s(m) + n C_{q,\beta}^\beta(m) + m C_{q,\alpha}^\alpha(n) \\ &\leq M_{q,f}^s(n) M_{q^n,g}^s(m) + n c_q(m) + m c_q(n). \end{aligned}$$

Учитывая оценку Шенхаге [20] и указанную выше тривиальную оценку для $c_q(m)$, получаем, что

$$M^O(GF(q^{nm})) = O(nm \log n \log m \log \log n \log \log m) + O(nm)(m+n)/\log_q(n+m).$$

Для получения оценки битвой сложности нужно приведенные оценки, естественно, умножить на $M(GF(q))$.

В случае, когда для $c_q(m)$ или $c_q(n)$ имеются нетривиальные оценки, например, когда для n и m существуют оптимальные нормальные базисы, последнее слагаемое можно заменить на меньшее, например, в последнем случае его можно заменить на $O(nm) \log_q(n+m)$. Последнее утверждение очевидным образом распространяется и на случай кронекерова произведения нескольких базисов. В указанном случае последнее слагаемое очевидно поглощается первым и может быть опущено.

Кронекерово произведение базисов можно определить и в случае, когда m и n не обязательно взаимно простые числа, но тогда базис $B_2 = \{\beta_1, \dots, \beta_m\}$ выбирается в поле $GF(q^{nm})$ и над полем $GF(q^m)$.

Для произведения стандартных базисов для сложности умножения в поле $GF(q^{nm})$ опять справедлива оценка

$$M_{B_1 \otimes B_2}(GF(q^{nm})) \leq M_{q,f}^s(n) M_{q^n,g}^s(m), \quad (19)$$

но здесь g — неприводимый полином степени m над полем $GF(q^n)$, порождающий базис B_2 .

Рассмотрим произведение $B^\alpha \otimes B^\beta$ нормальных базисов $B^\alpha \subset GF(q^n)$ и $B^\beta \subset GF(q^{mn})$, последний из которых — базис над полем $GF(q^n)$. Это произведение базисов само не является нормальным базисом, но очевидно, что возведение в степень q^n в нем тоже сводится к перестановке координат, но уже не циклической. Поэтому схемная сложность возведения в степень q^n в этом базисе, как и в нормальном, равна нулю, и такой базис тоже можно использовать для уменьшения сложности экспоненцирования и инвертирования в поле $GF(q^{nm})$, если получить для него алгоритм умножения невысокой сложности.

Для этого, как и выше, рассмотрим произведение соответствующих стандартных базисов $B_\alpha \otimes B_\beta$. В рассматриваемом случае сложность перехода от базиса $B^\alpha \otimes B^\beta$ к базису $B_\alpha \otimes B_\beta$ оценивается сверху величиной

$$C_{q^n, \beta}^\beta(m) + mC_{q, \alpha}^\alpha(n). \quad (20)$$

Действительно, если произвольный элемент поля $GF(q^{nm})$ записывается в обоих базисах как

$$\sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x_{i,j} \alpha^{q^i} \beta^{q^{jn}} = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j,$$

то для преобразования матрицы $(x_{i,j})$ над полем $GF(q)$ в матрицу $(x'_{i,j})$ над тем же полем достаточно m раз выполнить преобразование $C_{q, \alpha}^\alpha(n)$ над строками матрицы $(x_{i,j})$, чтобы получить равенство

$$\sum_{i=0}^{n-1} \alpha^{q^i} \sum_{j=0}^{m-1} x_{i,j} \beta^{q^j} = \sum_{j=0}^{m-1} \beta^{q^j} \sum_{i=0}^{n-1} x''_{i,j} \alpha^i,$$

а потом один раз выполнить преобразование $C_{q^n, \beta}^\beta(m)$ над столбцами полученной матрицы $(x''_{i,j})$ над полем $GF(q^n)$, чтобы получить равенство

$$\sum_{j=0}^{m-1} \beta^{q^j} \sum_{i=0}^{n-1} x''_{i,j} \alpha^i = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} x'_{i,j} \alpha^i \beta^j.$$

Из (19) и (20) следует, что при подходящем выборе элементов α и β (или, что то же самое, многочленов f и g) сложность умножения в поле $GF(q^{nm})$ в некотором базисе с бесплатным возведением в q -ю степень оценивается сверху величиной

$$M_{q,f}^s(n)M_{q^n,g}^s(m) + c_{q^n}(m) + mc_q(n).$$

Учитывая оценку из [20] и указанную выше тривиальную оценку для $c_{q^n}(m)$, отсюда опять получаем, что

$$M^O(GF(q^{nm})) = O(nm \log n \log m \log \log n \log \log m) + O(nm)(m+n)/\log_q(n+m).$$

Для получения оценок битовой сложности нужно приведенные выше оценки умножить на $M(GF(q))$.

Список литературы

1. Берлекемп Е., *Алгебраическая теория кодирования*. Мир, Москва, 1971.
2. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. Б., *Алгоритмические основы эллиптической криптографии*. Изд-во МЭИ, Москва, 2000.
3. Гашков С. Б., Чубариков В. Н., *Арифметика. Алгоритмы. Сложность вычислений*. Высшая школа, Москва, 2000.
4. Кнут Д., *Искусство программирования на ЭВМ*, т. 2. Мир, Москва, 1977.
5. Лидл Р., Нидеррайтер Г., *Конечные поля*. Мир, Москва, 1988.
6. Jungnickel D., *Finite fields: structure and arithmetics*. B.I.-Wissenschaftsverlag, Mannheim, 1993.
7. von zur Gathen J., Gerhard J., *Modern computer algebra*. Cambridge Univ. Press, Cambridge, 1999.
8. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. Б., О методах реализации умножения многочленов над конечными полями. *Вестник МЭИ* (2000), №3, 33–40.
9. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. Б., О методах имплементации арифметических операций в конечных полях. *Вестник МЭИ* (2000), №4, 24–32.
10. Болотов А. А., Гашков С. Б., Фролов А. Б., Часовских А. Б., Программные и схемные методы умножения многочленов для эллиптической криптографии. *Известия РАН. Теория и системы управления* (2000), №5, 66–75.
11. Болотов А. А., Гашков С. Б., Хохлов Р. А., О сложности алгоритмов построения неприводимых трехчленов и пятичленов над конечными полями. *Интеллектуальные системы* (1999) 4, №3-4, 12–34.
12. Коновальцев И. В., Об одном алгоритме решения линейных уравнений в конечных полях. *Пробл. киберн.* (1967) 19, 269–274.
13. Ash D. W., Blake I. F., Vanstone S. A., Low complexity normal bases. *Discrete Appl. Math.* (1989) 25, 191–210.
14. Gao S., Lenstra H. W., Optimal normal bases. *Design, Codes and Cryptography* (1992) 2, 315–323.
15. Gao S., Vanstone S. A., On orders of optimal normal basis generators. *Math. Comput.* (1995) 64, 1227–1233.
16. Gao S., von zur Gathen J., Panario D., Gauss periods: orders and cryptografical applications. *Math. Comput.* (1998) 67, 343–352.
17. Gashkov S., Kochergin V., On addition chains of vectors, gate circuits, and the complexity of computation of power. *Syberian Adv. Math.* (1994) 4, 1–16.
18. von zur Gathen J., Giesbrecht M., Constructing normal bases in finite fields. *J. Symbolic Comput.* (1990) 10, 547–579.
19. Mullin R. C., Onyszchuk I. M., Vanstone S. A., Wilson R. M., Optimal normal bases in $GF(p^n)$. *Discrete Appl. Math.* (1988/89) 22, 149–161.
20. Schönhage A., Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica* (1977) 7, 395–398.
21. Seguin J. E., Low complexity normal bases. *Discrete Appl. Math.* (1990) 28, 309–312.
22. Семаев И. А. Конструкция неприводимых полиномов над конечными полями с линейно независимыми корнями. *Матем. сб.* (1989) 63, 507–519.
23. Сидельников В. М., О нормальных базисах конечного поля. *Матем. сб.* (1987) 133, №4, 497–507.