Быстрые вычисления в конечных полях с использованием стандартных и оптимальных нормальных базисов

А.А. Болотов, С.Б. Гашков, Р.А. Хохлов*

1. Введение

Известный специалист по кодированию и конечным полям Элвин 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).

Актуальной стала задача быстрой имплементации арифметики в этих полях, для чего около десяти лет назад группой канадских математиков были изобретены оптимальные нормальные базисы.

2. 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 [2], [3]). Через $GF(q^n)$ обозначаем конечное поле порядка q^n, рассматриваемое как

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-01175), Программы поддержки ведущих научных школ РФФИ (проект 00-15-96103), Программы «Университеты России» и ФЦП «Интеграция» (объединенный проект А0110).

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*

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

(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 представляет из себя 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

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

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, [2], [3], где даже 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

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

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

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

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

Сложение в нормальном базисе, как и в стандартном, представляет из себя покомпонентное сложение векторов коэффициентов в поле $GF(q)$.

Благодаря тождеству Ферма $x^q = x$, справедливому для любого x из поля $GF(q)$, и тождеству Фробениуса $(x+y)^q = x^q + y^q$, справедливому для любых x и y из поля $GF(q^n)$, *возведение в степень* q (а значит, и в любую степень q^m) в нормальном базисе представляет собой циклический сдвиг коэффициентов, так как

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

Рассмотрим *умножение* в нормальных базисах. Иногда для простоты будем рассматривать нормальные базисы в практически наиболее важном случае q, равного степени двойки.

Согласно [3], сложностью C_B произвольного нормального базиса

$$B = \{\alpha, \alpha^q, \alpha^{q_2}, \ldots, \alpha^{q^{n-1}}\}$$

называется число ненулевых элементов в матрице T, произвольная i-я строка которой есть просто 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 Massey-Omura, см., например, [3]): пусть

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

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

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

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

где разность $s-j$ и сумма $k+j$ тоже вычисляются по модулю n, тогда

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

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 $-j$ тоже вычисляются по модулю n, замечаем, что предыдущую формулу можно переписать в виде

$$p_m = \sum_{i,j=0}^{n-1} t_{i-j,m-j} x_i y_j = \sum_{k,l=0}^{n-1} t_{k-l,-l} x_{k+m} y_{l+m} =$$

$$= \sum_{i,j=0}^{n-1} a_{i,j} x_{i+m} y_{j+m} = \sum_{i,j=0}^{n-1} a_{i,j} S^m(x_i) S^m(y_j)\,,$$

где S^m — операция циклического сдвига 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.

Ясно, что матрица A симметрическая, так как координаты произведения не зависят от перестановки сомножителей, и число ее ненулевых элементов, а также их сумма таковы же, как и у матрицы T. Для вычисления билинейной формы $A(x,y)$ достаточно выполнить $C_B + n - 1$ операций в поле GF(q), но реальная сложность иногда может оказаться и меньше. Если пренебречь временем выполнения циклических сдвигов, то сложность выполнения умножения над нормальным базисом поля $GF(q^n)$ оценивается сверху как $n(C_B + n - 1)$ операций в поле $GF(q)$, что видно из следующей формулы:

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

то есть сложность умножения зависит от количества ненулевых элементов в матрице C_B.

Заметим, что связанная с базисом матрица A — «таблица умножения» в этом базисе, однозначно определяет операцию умножения в рассматриваемом поле, а так как сложение элементов поля в любом базисе это просто обычное сложение векторов их координат, то все операции поля $GF(q^n)$ однозначно определены, если только вычислена эта матрица, значит мы имеем новое представление поля, связанное с указанным базисом, и нам нет необходимости вычислять разложения элементов нового базиса по старому стандартному полиномиальному базису этого поля. В дальнейшем все операции в этом поле мы можем проводить в рассматриваемом нормальном базисе.

Известна следующая теорема о сложности нормальных базисов.

Теорема 1. (см. [3]) *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.*

Приведем доказательство ввиду его простоты. Напомним, что в матрице T произвольная i-я строка есть просто вектор коэффициентов элемента $\alpha\alpha^{q^i}$ поля $GF(q^n)$ относительно базиса B. Таким образом, сумма всех строк матрицы T есть вектор коэффициентов следующего элемента $\alpha(\alpha+\alpha^q+\cdots+\alpha^{q^{n-1}}) = \alpha Tr(\alpha)$, то есть $(Tr(\alpha),0,\ldots,0)$. Заметим, что след не равен нулю, так как элементы базиса B линейно независимы. С другой стороны, строки T тоже линейно независимы, таким образом, вектор $\alpha,\alpha\alpha^q,\ldots,\alpha\alpha^{q^{n-1}}$ тоже является базисом в $GF(q^n)$, таким образом, столбцы в матрице тоже линейно независимы, в частности нет нулевых строк в матрице. Но суммы элементов в каждом столбце, кроме первого, равны нулю. Таким образом, в каждом столбце, кроме первого, стоит, как минимум, по два ненулевых элемента. А в первом может стоять, как минимум, один ненулевой элемент, главное, чтобы их сумма была ненулевой. То есть $C_B \geqslant 2n-1$. В частном случае $q=2$ количество единиц в первом столбце — нечетно, а во всех остальных — четно. Итак, установлено, что для любого нормального B его сложность не меньше $2n-1$. Базисы, для которых достигается эта граница, и называются оптимальными.

3. Оптимальные нормальные базисы и алгоритмы их генерации

Оптимальные нормальные базисы были обнаружены Mullin, Onyszchuk, Vanstone, Wilson в работе [4]. Они удачно могут быть использованы в мультиплере, предложенном Massey и Omura. Впоследствии Gao и Lenstra [5] показали, что других оптимальных нормальных базисов, кроме найденных в [4], не существует.

Так как указанные базисы существуют не во всех полях, то представляют интерес базисы не оптимальные, но имеющие низкую сложность. Им посвящена статья [5]. Строятся эти базисы с помощью так называемых гауссовых периодов, изучению криптографических приложений которых посвящены статьи [6], [7].

Так как в доступной литературе на русском языке оптимальные нормальные базисы видимо еще не появлялись, далее мы кратко излагаем с необходимыми доказательствами все три существующие конструкции этих базисов и алгоритмы их построения.

Определение 1. Первый тип оптимальных нормальных базисов конечного поля $GF(q^n)$ возникает, когда $n+1=p$ — простое и q — примитивный корень по модулю p.

В этом случае генератором базиса первого типа будет один из примитивных корней ζ p-й степени из единицы поля $GF(q^n)$.

Для поиска значений n, при которых существует базис первого типа, надо сгенерировать таблицу простых чисел от 1 до заданной границы поиска N с помощью решета Эратосфена и для очередного простого p проверить, что

$$q^{(p-1)/\delta} \bmod p \neq 1$$

для каждого простого делителя δ числа $p-1$. Факторизация этого числа тривиальным методом требует времени $O(\sqrt{p})$ (с учетом уже построенной таблицы простых), а проверка всех $O(\log p)$ указанных неравенств — времени $O(\log^2 p)$. Общее время работы этого подалгоритма — $O(N^{3/2})$.

Далее для каждого найденного $n=p-1$ ищем в поле $GF(q^n)$ примитивный корень ζ p-й степени из 1. Так как в силу простоты p все неединичные корни указанной степени являются примитивными,

а $q^n - 1$ кратно p согласно выбору n, то для любого ненулевого элемента β из поля $GF(q^n)$ его степень $\beta^{(q^n-1)/p}$, в случае если она не равна 1, будет искомым корнем, так как $\beta^{q^n-1} = 1$ по малой теореме Ферма. Вероятность того, что для случайного β будет справедливо равенство $\beta^{(q^n-1)/p} = 1$, равна $1/p$, так как количество корней $(q^n - 1)/p$ степени из 1 равно $(q^n - 1)/p$, значит нужный нам корень после, например 5 попыток, мы получим с почти единичной вероятностью за время $O(n \log q)^3$, если использовать стандартный быстрый алгоритм возведения в степень и алгоритм сложности $O(n \log q)^2$ для умножения в поле $GF(q^n)$. В качестве представления элементов поля можно взять многочлены степени $n - 1$ с коэффициентами из поля $GF(q)$, а операции проводить по модулю неприводимого полинома, желательно «малочлена».

Приведем доказательство оптимальности базисов первого типа. Заметим, что система $\{\zeta, \ldots, \zeta^n\}$ совпадает с точностью до перестановки с нормальным базисом

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

так как последовательность степеней $1, q, q^2, \ldots, q^{n-1}$, вычисленных по модулю p, совпадает с некоторой перестановкой $\pi(1), \ldots, \pi(n)$ множества чисел $\{1, \ldots, n\}$ в силу того, что q — примитивный корень по модулю p, значит равенство q^i и q^j при $0 \geqslant i < j < n$ по модулю p невозможно, так как иначе q^{j-i} было бы равно 1 по модулю p, что противоречило бы примитивности q по этому модулю.

Линейная независимость системы $\{\zeta, \ldots, \zeta^n\}$ вытекает из того, что ζ не может быть корнем никакого многочлена над полем $GF(q)$ степени меньшей n, так как ζ является корнем неприводимого над полем $GF(q)$ многочлена

$$1 + x + \ldots + x^n = \frac{x^p - 1}{x - 1},$$

который неприводим в силу того, что если он имеет собственный делитель $f(x)$, то его корнем будет один из корней ζ^{q^i} многочлена $1 + x + \ldots + x^n$, а значит его корнями будут все элементы вида $\alpha^{q^i}, i = 1, 2, \ldots$, где $\alpha = \zeta^{q^k}$, а значит и все элементы $\zeta^{q^{i+k}}, i = 1, 2, \ldots$, где сумма $i + k$ вычисляется по модулю n, так как

$$q^n = 1 \bmod p, \zeta^{q^n} = \zeta,$$

и поэтому корнями многочлена $f(x)$ являются все n корней многочлена $1 + x + \ldots + x^n$, что невозможно.

Вычислим теперь матрицу T. Для этого надо найти разложение

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

Согласно равенствам $\zeta\zeta^m = \zeta^{m+1}, m = 1, \ldots, n$ при $m < n$ сумма

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

будет равна ζ^{m+1} только если при i таком, что $q^i = m \bmod p$, (то есть при $i = \pi^{-1}(m)$) равенство $t_{i,j} = 1$ будет справедливо лишь при j таком, что $q^j = m + 1 \bmod p$, то есть при

$$j = \pi^{-1}(m + 1) = \pi^{-1}(\pi(i) + 1),$$

а остальные коэффициенты $t_{i,j}$ будут равны нулю.

Если же $m = n$, то

$$\zeta\zeta^m = \zeta^{n+1} = \zeta^p = 1 = \sum_{k=1}^{n} \zeta^k = \sum_{j=0}^{n-1} \zeta^{q^j},$$

значит при $i = \pi^{-1}(n)$ все коэффициенты $t_{i,j} = 1$. В итоге общее число ненулевых коэффициентов равно $2n - 1$, значит построенный базис оптимальный нормальный.

Приведем еще в явном виде следующий алгоритм.

Алгоритм построения оптимальных нормальных базисов первого типа и таблицы умножения в них при $q = 2$.

Пусть надо построить оптимальный нормальный базис в поле $GF(2^n)$.

1. Проверяем, является ли $p = n + 1$ простым числом.

2. Если да, то проверяем, является ли 2 примитивным корнем по модулю p. Для этого проверяем, что

$$2^{(p-1)/\delta} \bmod p \neq 1$$

для каждого простого делителя δ числа $p-1$. Если это выполнено, то 2 является примитивным корнем по модулю p.

3. Ищем в поле $GF(2^n)$ примитивный корень ζ p-й степени из 1. Для этого случайным образом генерируем ненулевой элемент β из поля $GF(2^n)$ и вычисляем его степень $\beta^{(q^n-1)/p}$. Если эта степень не равна 1, то полагаем ζ равным этой степени, в противном случае генерируем новый элемент β, и так далее, пока не получим $\beta^{(q^n-1)/p} \neq 1$, после чего полагаем $\zeta = \beta^{(q^n-1)/p}$.

Заметим однако, что для вычисления нужной нам матрицы T пункт 3 не нужен.

4.Вычисляем матрицу $T = (t_{i,j})$. Выбираем очередной индекс i, $0 \leqslant i < n$. Сначала находим $m = 2^i \bmod p$. Если $m < n$, то находим $0 \leqslant j < n$, такое что $2^j = m+1 \bmod p$, и полагаем $t_{i,j} = 1$, а при $k \neq j$ $t_{i,k} = 0$. Если же $m = n$, то полагаем $t_{i,j} = 1$ при всех j, $0 \leqslant j < n$.

5. Вычисление матрицы A осуществляется с помощью равенств $a_{i,j} = t_{i-j,-j}$, где $i-j$ и $-j$ вычисляются по модулю n. Эта матрица является выходом алгоритма, так как именно она используется в алгоритме умножения Massey-Omura.

Определение 2. Второй тип оптимальных нормальных базисов конечного поля $GF(q^n)$ возникает, когда $2n+1 = p$ — простое и q — примитивный корень по модулю p.

Генератором этого базиса является элемент $\alpha = \zeta + \zeta^{-1}$, где ζ — примитивный корень p-й степени из единицы в поле $GF(q^{2n})$.

Приведем доказательство оптимальности базисов второго типа. Базис второго типа возникает, когда $2n+1 = p$ — простое число, а условие на q такое же, как в первом случае, где роль числа n играет число $2n$. Элемент ζ тогда будет примитивным корнем степени p из 1 в поле $GF(q^{2n})$, но в качестве порождающего элемента оптимального нормального базиса нужно взять $\alpha = \zeta + \zeta^{-1}$. Так как

$$q^n = -1 \bmod p,$$

то

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

значит

$$\alpha^{q^n} = \alpha,$$

поэтому α принадлежит подполю $GF(q^n)$ поля $GF(q^{2n})$. Система

$$\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$$

линейно независима, так как

$$\alpha^{q^k} = \zeta^{q^k} + \zeta^{-q^k} = \zeta^{q^k} + \zeta^{q^{k+n}}$$

в силу равенства

$$q^{k+n} = -q^k \bmod p,$$

а система

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

линейно независима. Можно проверить, что при $n > k > 0$

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

$$= \alpha^{q^s} + \alpha^{q^t},$$

значит соответствующая этому базису матрица T при $q = 2^l$ содержит $2n-1$ единицу, потому что при $k = 0$ разложение произведения $\alpha\alpha^{q^0}$ по базису состоит из одного слагаемого, ведь

$$\alpha^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} = \alpha^{q^s}.$$

Для выполнения указанной проверки заметим, что согласно определению, последовательность $q^k \bmod p, k = 0, \ldots, 2n-1$ является перестановкой $\pi(1), \ldots, \pi(2n)$ множества чисел $\{1, \ldots, 2n\}$ в силу того, что q — примитивный корень по модулю $p = 2n+1$, причем в силу соотношения

$$q^{k+n} = -q^k \bmod p, k = 0, \ldots, n-1$$

справедливо равенство

$$\pi(k) + \pi(k+n) = p, k = 0, \ldots, n-1,$$

а так как все неупорядоченные пары

$$(1 + q^k \bmod p, -1 - q^k \bmod p)$$

при любом $k = 0, \ldots, n-1$, отличны от пары $(0,0)$, то их последовательность состоит из пар

$$(\pi(k), \pi(k+n)), k = 0, \ldots, n-1,$$

то есть из неупорядоченных пар вида $(u, p-u), 0 < u \geqslant n$, значит существует такое отображение $(\sigma(1), \ldots, \sigma(n))$ множества чисел $1, \ldots, n$ в себя, что

$$(1 + q^k \bmod p, -1 - q^k \bmod p) = (\pi(\sigma(k+1)), p - \pi(\sigma(k+1))),$$

и значит

$$\zeta^{1+q^k} + \zeta^{-1-q^k} = \zeta^{q^{\sigma(k+1)}} + \zeta^{-q^{\sigma(k+1)}} = \alpha^{q^{\sigma(k+1)}}.$$

Аналогично определяется отображение $(\mu(1), \ldots, \mu(n))$ множества $1, \ldots, n$, в себя такое, что

$$\zeta^{1-q^k} + \zeta^{-1+q^k} = \zeta^{q^{\mu(k)}} + \zeta^{-q^{\mu(k)}} = \alpha^{q^{\mu(k)}}$$

при любом $n \geqslant k > 0$.

Так как

$$1 - q^k \neq 1 + q^k, 1 - q^k \neq -1 - q^k$$

по модулю p, то при любом $n > k > 0$ справедливо неравенство

$$\mu(k) \neq \sigma(k+1).$$

Вспоминая определение матрицы T посредством равенств

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

и сравнивая их с полученными равенствами

$$\alpha\alpha^{q^i} = \alpha^{q^{\sigma(i+1)}} + \alpha^{q^{\mu(i)}}, i > 0,$$

$$\alpha\alpha^{q^0} = \zeta^{1+q^0} + \zeta^{-1-q^0} + \zeta^{1-q^0} + \zeta^{-1+q^0} =$$

$$= \zeta^{1+q^0} + \zeta^{-1-q^0} + \zeta^0 + \zeta^0 = \zeta^{1+q^0} + \zeta^{-1-q^0} = \alpha^{q^{\sigma(1)}},$$

имеем

$$t_{i,j} = \delta_{\sigma(i+1),j} + \delta_{\mu(i),j}, i \neq 0,$$
$$t_{0,j} = \delta_{\sigma(1),j},$$

где $\delta_{k,s}$ — дельта-символ Кронекера, равный 1 при $k = s$ и нулю в противном случае.

Отметим, что в случае нечетного q указанный базис не будет, строго говоря, оптимальным, но будет иметь линейную сложность. Действительно, тогда

$$\alpha^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = \alpha^{q^s} + 2,$$

а элемент 2 из поля $GF(q)$ представим в виде

$$c\sum_{k=0}^{n-1} \alpha^{q^k}$$

при ненулевом c из поля $GF(q)$.

Приведем также в явном виде еще один алгоритм.

Алгоритм построения оптимальных нормальных базисов второго типа и таблицы умножения в них при $q = 2$.

Пусть надо построить оптимальный нормальный базис в поле $GF(2^n)$.

1. Проверяем, является ли $p = 2n + 1$ простым числом.

2. Если да, то проверяем, является ли 2 примитивным корнем по модулю p.

3.Если да, то вычисляем матрицу $T = (t_{i,j})$.

Для этого сначала строим массив

$$\pi(k) = 2^k \bmod q, k = 0, \ldots, 2n - 1.$$

Потом строим массив $(\sigma(1), \ldots, \sigma(n))$ такой, что $1 \leqslant \sigma(k) \leqslant n$ и

$$(1 + 2^k \bmod p, -1 - 2^k \bmod p) = (\pi(\sigma(k+1)), p - \pi(\sigma(k+1))),$$
$$k = 0, \ldots, n - 1.$$

Затем строим массив $(\mu(1), \ldots, \mu(n))$, такой что $1 \leqslant \mu(k) \leqslant n$ и

$$(1 - 2^k \bmod p, -1 + 2^k \bmod p) = (\pi(\mu(k)), p - \pi(\mu(k))), k = 1, \ldots, n.$$

И наконец вычисляем для всех $0 < i < n$ и всех j, $0 \leqslant j < n$

$$t_{i,j} = \delta_{\sigma(i+1),j} + \delta_{\mu(i),j},$$

$$t_{0,j} = \delta_{\sigma(1),j},$$

где $\delta_{k,s}$ — дельта-символ Кронекера, равный 1 при $k = s$ и нулю в противном случае.

Определение 3. Третий тип оптимальных нормальных базисов конечного поля $GF(q^n)$ возникает когда $2n + 1 = p$ — простое $\equiv 3 \pmod 4$, а q — квадратичный вычет по модулю p (то есть существует такое r, что $q = r^2 \pmod p$, и при любом $0 < k < n$ $2^k \neq 1 \bmod p$.

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 $GF(q^{2n})$.

Приведем доказательство оптимальности и в этом случае. Базис третьего типа возникает, когда n нечетно, $2n + 1 = p$ — простое число, а условие на q заменяется на то, что $q^n = 1 \bmod p$, и при любом $0 < k < n$ $q^k \neq 1 \bmod p$ (другими словами, число q имеет по модулю p порядок n, а не $2n$, как во втором случае, и тогда автоматически существует такое r, что $q = r^2 \bmod p$, то есть q — квадратичный вычет по модулю p, и поэтому все его степени $q^k \bmod p$, $k = 0, \ldots, n-1$ образуют перестановку множества всех квадратичных вычетов по модулю p, так как их ровно n штук).

А так как p равно 3 по модулю 4, то -1 является квадратичным невычетом по модулю p, так как в противном случае существовало бы такое число r, что $-1 = r^2 \bmod p$, и тогда получилось бы противоречие с малой теоремой Ферма:

$$r^{p-1} = (r^2)^{(p-1)/2} = (-1)^{(p-1)/2} = -1 \bmod p.$$

Поэтому из того, что произведение вычета на невычет является невычетом, следует, что последовательность $-q^k \bmod p$, $k = 0, \ldots, n-1$ образуют перестановку множества всех квадратичных невычетов по модулю p.

Как и в случае базиса второго типа в качестве элемента ζ берется примитивный корень степени p из 1 в поле $GF(q^{2n})$, а в качестве порождающего элемента оптимального нормального базиса — элемент $\alpha = \zeta + \zeta^{-1}$.

Однако доказательство линейной независимости системы

$$\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$$

отличается от второго случая. Допустим противное, то есть

$$\sum_{j=0}^{n-1} a_j \alpha^{q^j} = 0$$

для некоторого ненулевого вектора (a_j) с координатами из поля $GF(q)$. Подставляя равенства

$$\alpha^{q^i} = \zeta^{q^i} + \zeta^{-q^i},$$

получаем, что

$$\sum_{j=0}^{n-1} a_j (\zeta^{q^j} + \zeta^{-q^j}) = 0.$$

Последнее равенство можно переписать в виде

$$\sum_{i=0}^{2n-1} b_i \zeta^i = 0,$$

если определить b_i как a_j, где $i = \pm q^j \bmod p$ (как было указано выше, последнее условие определяет число j однозначно; знак плюс соответствует случаю, когда число i — вычет, а знак минус — случаю, когда i является квадратичным невычетом по модулю p), значит многочлен

$$f(x) = \sum_{i=0}^{2n-1} b_i x^i$$

имеет корни ζ и ζ^{-1} в поле $GF(q^{2n})$, а так как эти элементы имеют минимальные многочлены степени n каждый, причем они взаимно просты (в указанном поле корнями первого из них являются $\zeta^{q^i}, i = 0, \ldots, n-1$, а корнями второго — элементы $\zeta^{-q^i}, i = 0, \ldots, n-1$), то многочлен $f(x)$ над полем $GF(q)$ должен делится на их произведение, что невозможно, так как его степень меньше $2n$.

Проверка оптимальности построенного базиса почти ничем не отличается от второго случая. Достаточно проверить, что при $k < n$

$$1 + q^k = \pm q^{\sigma(k+1)} \bmod p$$

и

$$1 - q^k = \pm q^{\mu(k)} \bmod p$$

(в последнем случае только при $k > 0$), тогда

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

$$\zeta^{1-q^k} + \zeta^{-1+q^k} = \zeta^{q^{\mu(k)}} + \zeta^{-q^{\mu(k)}} = \alpha^{q^{\mu(k)}}, k > 0.$$

Так же, как и в случае второго типа, при $n > k > 0$ имеем

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

$$= \alpha^{q^{\sigma(k+1)}} + \alpha^{q^{\mu(k)}},$$

а при $k = 0$

$$\alpha\alpha^{q^0} = \zeta^{1+q^0} + \zeta^{-1-q^0} + \zeta^{1-q^0} + \zeta^{-1+q^0} =$$

$$= \zeta^{1+q^0} + \zeta^{-1-q^0} + \zeta^0 + \zeta^0 = \zeta^{1+q^0} + \zeta^{-1-q^0} = \alpha^{q^{\sigma(1)}}.$$

Опять, как и в случае второго типа, вспоминая определение матрицы T посредством равенств

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

и сравнивая их с полученными равенствами

$$\alpha\alpha^{q^i} = \alpha^{q^{\sigma(i+1)}} + \alpha^{q^{\mu(i)}}, i > 0,$$

$$\alpha\alpha^{q^0} = \alpha^{q^{\sigma(1)}},$$

имеем

$$t_{i,j} = \delta_{\sigma(i+1),j} + \delta_{\mu(i),j}, i \neq 0,$$

$$t_{0,j} = \delta_{\sigma(1),j},$$

где $\delta_{k,s}$ — дельта-символ Кронекера, равный 1 при $k = s$ и нулю в противном случае.

Отметим, что при нечетном q указанный базис не будет, как и в случае второго типа, оптимальным, но будет иметь линейную сложность.

Алгоритм построения оптимальных нормальных базисов третьего типа и таблицы умножения в них при $q = 2$

Пусть надо построить оптимальный нормальный базис в поле $GF(2^n)$.

1. Проверяем, что n нечетно. Если да, то проверяем, является ли $p = 2n + 1$ простым числом.

2. Если да, то проверяем, что

$$2^n = 1 \bmod p,$$

и

$$2^{n/\delta} \bmod p \neq 1$$

для каждого простого делителя δ числа n.

3. Если да, то вычисляем матрицу $T = (t_{i,j})$.

Сначала строим массив

$$\pi(k) = 2^k \bmod q,\ k = 0, \ldots, 2n - 1.$$

Потом строим массив $(\sigma(1), \ldots, \sigma(n))$ такой, что $1 \leqslant \sigma(k) \leqslant n$ и

$$1 + 2^k \bmod p = \pm\pi(\sigma(k + 1)), k = 0, \ldots, n - 1.$$

Затем строим массив $(\mu(1), \ldots, \mu(n - 1))$, такой что $1 \leqslant \mu(k) \leqslant n$ и

$$1 - 2^k \bmod p = \pi(\mu(k)), k = 1, \ldots, n - 1.$$

И наконец как и в случае второго типа вычисляем для всех $0 < i < n$ и всех j, $0 \leqslant j < n$

$$t_{i,j} = \delta_{\sigma(i+1),j} + \delta_{\mu(i),j},$$

$$t_{0,j} = \delta_{\sigma(1),j},$$

где $\delta_{k,s}$ — дельта-символ Кронекера, равный 1 при $k = s$ и нулю в противном случае.

На основе указанных алгоритмов авторами была написана программа, которая генерирует оптимальные нормальные базисы вместе с их «таблицами умножения».

4. Оценка сложности перехода от оптимального нормального базиса первого типа к стандартному и обратно

Имплементированные стандартные алгоритмы умножения в оптимальных нормальных базисах оказались медленнее алгоритмов умножения в стандартных базисах даже в небольших размерностях, 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 «выгодных» сторон каждого из них. Действительно, умножение быстрее производить в стандартном представлении поля $GF(2^n)$, а возведение в степень — в нормальном представлении. Но для этого понадобятся матрицы перехода от нормального базиса к стандартному базису и обратно, которые могут оказаться не «разряженными», а «плотными», и тогда сложность перехода от одного базиса к другому будет $O(n^2/\log n)$ (даже если использовать для умножения матрицы на вектор метод Лупанова).

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

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

Теорема 2. *Переход от стандартного базиса поля $GF(2^n)$ к соответствующему (с тем же генератором) оптимальному нормаль-*

ному первого типа (если, конечно он существует для данного n) и обратно можно выполнить с линейной сложностью, не более, чем $2n-1$.

Доказательство. Заметим, 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 степеней $1,q,q^2,\dots,q^{n-1}$, вычисленных по модулю p, совпадает с некоторой перестановкой

$$\pi(1),\dots,\pi(n) \text{ множества чисел } \{1,\dots,n\} \tag{1}$$

в силу того, что q — примитивный корень по модулю p, значит равенство q^i и q^j при $0\leqslant i<j<n$ по модулю p невозможно, так как иначе бы q^{j-i} было бы равно 1 по модулю p, что противоречило бы примитивности q по этому модулю).

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 с оценкой сложности не более, чем n.

Линейная независимость системы $\{\zeta,\dots,\zeta^n\}$ вытекает из того, что ζ является корнем неприводимого над полем $GF(q)$ многочлена

$$1+x+\ldots+x^n=\frac{x^p-1}{x-1},$$

ведь если бы система была линейно зависимой, то существовала бы равная нулю нетривиальная линейная комбинация ее элементов, значит существовал бы минимальный аннулирующий элемент ζ многочлен степени меньше, чем n, что не возможно, так как он был бы тогда нетривиальным делителем неприводимого многочлена $1+x+\ldots+x^n$, также аннулирующего элемент ζ, который неприводим в силу того, что если он имеет собственный делитель $f(x)$, то его корнем будет один из корней ζ^{q^i} многочлена $1+x+\ldots+x^n$, а значит его корнями будут все элементы вида $\alpha^{q^i}, i=1,2,\dots$, где $\alpha=\zeta^{q^k}$, а

значит и все элементы $\zeta^{q^{i+k}}, i = 1, 2, \ldots$, где сумма $i + k$ вычисляется по модулю n, так как

$$q^n = 1 \bmod p, \quad \zeta^{q^n} = \zeta,$$

и поэтому корнями многочлена $f(x)$ являются все n корней многочлена $1 + x + \ldots + x^n$, что невозможно, если они были бы линейно зависимы, то существовала бы нетривиальная линейная комбинация одного из них, то есть существовал бы другой аннулирующий многочлен степени меньше, чем n, что не возможно.

Стандартным является базис $\{1, \zeta, \ldots, \zeta^{n-1}\}$. Он с линейной сложностью выражается через базис $\{\zeta, \ldots, \zeta^n\}$, благодаря формуле

$$\zeta^n = 1 + \zeta + \ldots + \zeta^{n-1}, \tag{2}$$

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

$$1 = \zeta + \ldots + \zeta^{n-1} + \zeta^n, \tag{3}$$

с линейной сложностью выражается через базис $\{1, \zeta, \ldots, \zeta^{n-1}\}$. Для доказательства явно выпишем формулы перехода. Пусть элемент записан в почти стандартном базисе, тогда, учитывая равенство (3), получаем равенство

$$\sum_{i=1}^{n} x_i \zeta^i = \sum_{i=1}^{n-1} x_i \zeta^i + x_n (\sum_{i=0}^{n-1} \zeta^i),$$

которое после группировки коэффициентов переписываем в виде

$$\sum_{i=1}^{n} x_i \zeta^i = \sum_{i=1}^{n-1} (x_i + x_n) \zeta^i + x_n \zeta^0 = \sum_{i=1}^{n-1} y_i \zeta^i + y_0 \zeta^0 \tag{4}$$

(где y_i — координаты соответствующие стандартному базису), откуда следует, что сложность перехода от почти стандартного базиса к стандартному не более, чем $n - 1$. С помощью аналогичных преобразований с учетом равенства (3) получим формулу перехода от стандартного к почти стандартному базису

$$\sum_{i=0}^{n-1} y_i \zeta^i = \sum_{i=1}^{n-1} y_i \zeta^i + y_0 (\sum_{i=1}^{n} \zeta^i),$$

которая после группировки коэффициентов преобразуется в равенство

$$\sum_{i=0}^{n-1} y_i\zeta^i = \sum_{i=1}^{n-1}(y_i + y_0)\zeta^i + y_0\zeta^n = \sum_{i=1}^{n-1} x_i\zeta^i + x_n\zeta^n,$$

(где x_i — координаты в почти стандартном базисе). То есть и обратный переход выполняется со сложностью $n-1$.

В результате имеем, что переход от оптимального нормального базиса

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

к стандартному базису $\{1, \zeta, \ldots, \zeta^{n-1}\}$ и обратно выполняется со сложностью не более чем $2n-1$.

Замечание. Умножение в стандартном базисе сводится к обычному умножению многочленов над полем $GF(q)$ и последующей редукции по модулю неприводимого многочлена $f(x) = 1+x+\ldots+x^n$, соответствующего этому базису. На первый взгляд кажется, что деление с остатком на этот многочлен требует времени столько же, как и деление на произвольный многочлен. Но его 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. Умножим обе части равенства на $x-1$, тогда $g(x)(x-1) = (x^p-1)h(x) + r(x)(x-1)$, 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 выполнить $2n-2$ сложений в поле $GF(q)$, для деления результата на x^p-1 достаточно выполнить $n-3$ сложений в поле $GF(q)$, и для деления полученного остатка $r(x)(x-1)$ на $x-1$ с помощью схемы Горнера достаточно выполнить n сложений в поле $GF(q)$.

Пример к теореме 2.

Приведем пример к теореме 2, который также иллюстрирует алгоритм перехода от оптимального базиса первого типа к стандартному и обратно.

Переход от оптимального нормального базиса первого типа поля $GF(2^4)$ к стандартному.

Пусть дано: $n = 4$, оптимальный нормальный базис первого типа $B = \{\zeta^{2^k}, k = 0, ..., 3\}$, элемент, записанный в этом базисе, $f = 1\cdot\zeta^{2^0} +$

$0 \cdot \zeta^{2^1} + 1 \cdot \zeta^{2^2} + 1 \cdot \zeta^{2^3}$.

Надо найти: запись f в стандартном базисе $A = \{1, \zeta, \zeta^2, \zeta^3\}$.

Шаг 1. *Переход от базиса нормального к почти стандартному базису* $A' = \{\zeta, \ldots, \zeta^n\}$.

В начале найдем перестановку $\pi(i)$ (см. (1)) множества чисел $\{1, \ldots, n\}$, совпадающей с последовательностью степеней $1, 2, 2^2, \ldots, 2^{n-1}$, вычисленной по модулю $p = n + 1$:

$$\pi = \begin{pmatrix} 2^0 & 2^1 & 2^2 & 2^3 & \pmod 5 \\ 1 & 2 & 4 & 3 & \pmod 5 \end{pmatrix}, \tag{5}$$

то есть в базисе A' многочлен f запишется следующим образом:

$$f = 1 \cdot \zeta + 0 \cdot \zeta^2 + 1 \cdot \zeta^4 + 1 \cdot \zeta^3.$$

Шаг 2. *Переход от почти стандартного базиса к стандартному базису.* Благодаря формуле (4) выразим единицу, и тогда в стандартном базисе A многочлен f запишется следующим образом:

$$f = (1+1)\zeta + (0+1)\zeta^2 + (1+1)\zeta^3 + 1 \cdot \zeta^0,$$

то есть

$$f = 1 + \zeta^2$$

– многочлен в стандартном базисе.

Переход от стандартного базиса поля $GF(2^4)$ *к оптимальному нормальному базису* 1*-го типа.*

Пусть дано: $n = 4$, стандартный базис $A = \{1, \zeta, \zeta^2, \zeta^3\}$, многочлен, записанный в этом базисе, $f = 1 + x^2 + x^3$.

Надо найти: запись f в оптимальном нормальном базисе 1-го типа $B = \{\zeta^{2^k}, k = 0, \ldots, 3\}$.

Шаг 1. *Переход от стандартного базиса к почти стандартному базису.*

Благодаря формуле (3), выразим коэффициент при ζ^n, и тогда в почти стандартном базисе A' многочлен f запишется следующим образом:

$$f = (0+1)\zeta + (1+1)\zeta^2 + (1+1)\zeta^3 + 1 \cdot \zeta^4,$$

то есть

$$f = \zeta + \zeta^4.$$

Шаг 2. Переход от почти стандартного базиса к оптимальному нормальному базису.

Благодаря перестановке (5), сделав обратную перестановку, перейдем к записи многочлена в оптимальном нормальном базисе B:

$$f = \zeta + \zeta^{2^2}$$

— многочлен в оптимальном нормальном базисе.

Далее покажем, что сложность перехода и для оптимальных нормальных базисов 2-го и 3-го типа тоже невысока.

5. Оценка сложности перехода от оптимального нормального базиса второго или третьего типа к стандартному и обратно

Рассмотрим последовательность $\alpha_i = \zeta^i + \zeta^{-i}$, где ζ — примитивный корень из единицы степени $p = 2n + 1$ в поле $GF(2^{2n})$.

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

1) $\alpha_{k+1} = \alpha_k \alpha_1 + \alpha_{k-1}$;
2) $\alpha_{2^k} = \alpha^{2^k}$;
3) $\alpha_{2^k+i} = \alpha_i \alpha^{2^k} + \alpha_{2^k-i}$, *для любого i такого, что* $0 \leqslant i \leqslant 2^k$.

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

$$\alpha_k \alpha_1 + \alpha_{k-1} = \alpha_{k+1}.$$

Вторая формула проверяется непосредственно по определению

$$\alpha_{2^k} \equiv \zeta^{2^k} + \zeta^{-2^k}$$

и

$$\alpha^{2^k} \equiv (\zeta + \zeta^{-1})^{2^k} = \zeta^{2^k} + \zeta^{-2^k},$$

учитывая то, что операции проводятся в поле $GF(2)$.

Третью формулу можно вывести из первых двух по индукции, но проще проверить непосредственно:

$$\alpha_{2^k+i} = \zeta^{2^k+i} + \zeta^{-2^k-i} = (\zeta^{2^k} + \zeta^{-2^k})(\zeta^i + \zeta^{-i}) + (\zeta^{2^k-i} + \zeta^{-2^k+i}) =$$

$$= \alpha_{2^k}\alpha_i + \alpha_{2^k-i}\alpha^{2^k}\alpha_i + \alpha_{2^k-i}.$$

На самом деле рекуррентные соотношения, доказанные в предыдущей лемме, есть не что иное, как формулы перехода от нормального базиса к почти стандартному базису

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

Из леммы следует, что для любого $i \geqslant 1$ элемент α_i выражается в виде значения некоторого многочлена степени i, 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.

Плотность $S(F_n)$ (количество ненулевых элементов) матрицы F_n можно вычислить, используя следующую теорему.

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

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

$$F_{2n+1} = \begin{pmatrix} F_n & o_n & O_n \\ 0\ldots0 & 1 & 0\ldots0 \\ G_n & o_n & F_n \end{pmatrix},$$

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 клетках. На примере матрицы F_7 это выглядит так:

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

Если разбить матрицу на 4 квадратных подматрицы, удалив среднюю строку и средний столбец, получим, что левый верхний квадрат 3x3 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 (см. формулу п. 2).

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

$$\sum_{j=1}^{2^k+i} f_{2^k+i,j}\alpha^j = \alpha_{2^k+i} = \alpha_i\alpha^{2^k} + \alpha_{2^k-i} =$$

$$= \sum_{j=1}^{i} f_{i,j}\alpha^{2^k+j} + \sum_{j=1}^{2^k-i} f_{2^k-i,j}\alpha^j,$$

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

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

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

из которой вытекает рекуррентная формула

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

Полагая $l(k) = S(F_{2^k-1})$, перейдем к линейному рекуррентному соотношению $l(k) = 3l(k-1)+1, l(2) = 4$, решением которого будет

$$l(k) = (3^k - 1)/2. \tag{6}$$

Обозначив $n = 2^k - 1$, выразим $3^k = (2^k)^{\log_2 3} = (n+1)^{\log_2 3}$, и подставим это в (6), получим, что

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

В общем случае равенство

$$S(F_n) = O(n^{\log_2 3}) \tag{7}$$

сохраняется, так как выбрав k таким образом, что $2^k - 1 < n \leqslant 2^{k+1} - 1$, можно заметить, что матрица F_n является главной подматрицей матрицы $F_m, m = 2^k - 1$, откуда имеем

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

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

$$f'_{i,1} = f_{i,n}a_{n,1} = \delta_{i,n}a_{n,1},\ f'_{i,j} = f_{i,j-1} + f_{i,n}a_{n,j} = f_{i,j-1} + \delta_{i,n}a_{n,j},$$

так как в силу нижней треугольности матрицы F_n ее элементы $f_{i,n} = \delta_{i,n}$ — дельта-символу Кронекера. Складывая эти равенства, имеем, что

$$S(F'_n) = \sum_{i=1,j=1}^{n,n-1} f_{i,j} + \sum_{j=1}^{n} a_{n,j} = S(F_n) - 1 + \sum_{j=1}^{n} a_{n,j} \leqslant$$
$$\leqslant S(F_n) - 1 + n = O(n^{\log_2 3}).$$

Обозначим через $L(F_n)$ сложность линейного преобразования, определяемого матрицей F_n (то есть наименьшее число операций сложения по модулю два, необходимых для вычисления этого преобразования).

Теорема 4. $L(F_n) \leqslant (\frac{n}{2}) \log_2 n + 2n = O(n \log_2 n)$.

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 [8]). 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 $2^k \leqslant n < 2^{k+1} - 1$, тогда согласно п. 3

$$\sum_{i=1}^{n} y_i\alpha^i = \sum_{i=1}^{n} x_i\alpha_i =$$

$$= \sum_{i=1}^{2^k} x_i\alpha_i + \sum_{i=2^k+1}^{n} x_i\alpha_i = \sum_{i=1}^{2^k} x_i\alpha_i + \sum_{i=1}^{n-2^k} x_{i+2^k}\alpha_{i+2^k} =$$

$$= \sum_{i=1}^{2^k} x_i\alpha_i + \sum_{i=1}^{n-2^k} x_{i+2^k}(\alpha^{2^k}\alpha_i + \alpha_{2^k-i}) =$$

$$= x_{2^k}\alpha_{2^k} + \sum_{i=1}^{2^{k+1}-n-1} x_i\alpha_i + \sum_{i=2^{k+1}-n}^{2^k-1} x_i + x_{2^{k+1}-i})\alpha_i + \alpha^{2^k} \sum_{i=1}^{n-2^k} x_{i+2^k}\alpha_i,$$

и, определяя вектора-столбцы

$$X = \{x_1, \ldots, x_n\}^T,$$

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

$$X_2 = \{x_{1+2^k}, \ldots, x_n\}^T,$$

и вектора-строки

$$Y_2 = \{y_{1+2^k}, \ldots, y_n\},$$

$$Y_1 = \{y_1, \ldots, y_{2^k}\},$$

отсюда имеем

$$\sum_{i=1}^{n} y_i\alpha^i = \sum_{i=1}^{n} x_i\alpha_i = \sum_{i=1}^{2^k} X_{1,i}\alpha_i + +\alpha^{2^k} \sum_{i=1}^{n-2^k} X_{2,i}\alpha_i =$$

$$= \sum_{i=1}^{2^k} Y_{1,i}\alpha^i + \sum_{i=1}^{n-2^k} Y_{2,i+2^k}\alpha_{i+2^k},$$

значит

$$F_n^T \otimes X = (y'_1 \dots y'_n) = (Y_1, Y_2) = (F_{2^k}^T \otimes X_1, +F_{n-2^k}^T \otimes X_2.), \qquad (8)$$

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

Осталось индуктивно оценить сложность преобразования координат, определяемого матрицей F_n^T. Согласно (8)

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

По индукции непосредственно проверяется, что

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

Для произвольного n в пределах $2^k < n < 2^{k+1}$ согласно (8)

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

Записывая n в двоичной системе

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

где $k_s > \dots k_1$, получаем, что

$$L(n) \leqslant 2^{k_s-1}k_s + \dots 2^{k_1-1}k_1 + s - 1 + (n - 2^{k_s}) + \dots + (n - 2^{k_s} - \dots - 2^{k_2}) \leqslant$$

$$\leqslant (\frac{n}{2}) \log_2 n + c\frac{n}{2},$$

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

Для полноты сформулируем и докажем известную теорему о минимальном аннулирующем многочлене генератора оптимальных нормальных базисов второго и третьего типа.

Теорема 5. (см. [2]) *Пусть $2n+1 = p$ — простое, и 2 — примитивный корень по модулю p, или $2n+1$ — простое и $\equiv 3 \pmod 4$, и 2— квадратичный вычет по модулю $2n+1$, тогда многочлен $f_n(x)$ из $GF(2)[x]$, определенный рекуррентной формулой*

$$f_0 = 1, f_1 = x+1, f_k = xf_{k-1} + f_{k-2} \text{ для } k \geqslant 2 \tag{9}$$

совпадает с минимальным аннулирующим элемент α многочленом m_α, и его корни образуют оптимальный нормальный базис второго или, соответственно, третьего типа поля $GF(2^n)$.

Доказательство. Покажем, что минимальный аннулирующий многочлен m_α равенf_n. Для этого по индукции убедимся в справедливости следующей формулы:

$$f_k(y+y^{-1}) = 1 + \sum_{i=1}^{k}(y^i + y^{-i}). \tag{10}$$

Действительно, для $k = 1$ согласно (9) формула (10) верна. Предположим истинность формулы (10) для произвольного k, и сделаем переход к $k+1$. В самом деле, по формуле (9)

$$f_{k+1}(y+y^{-1}) = (y+y^{-1})f_k + f_{k-1} =$$

$$= (y+y^{-1})(1 + \sum_{i=1}^{k}(y^i + y^{-i})) + (1 + \sum_{i=1}^{k-1}(y^i + y^{-i}) =$$

$$= (y^{(k+1)} + y^{-(k+1)}) + (y^k + y^{-k}) + (1 + \sum_{i=1}^{k-1}(y^i + y^{-i}) =$$

что и заканчивает индуктивный переход:

$$= f_{k+1}(y+y^{-1}) = 1 + \sum_{i=1}^{k+1}(y^i + y^{-i}).$$

Далее заменим $y = \zeta$ в (10), и получаем

$$f_n(\alpha) = f_n(\zeta + \zeta^{-1}) = 1 + \sum_{i=1}^{n}(\zeta^i + \zeta^{-i}) = 1 + \sum_{j=1}^{2n}\zeta^j = 0,$$

где α генератор нормальных базисов второго и третьего типов, и ζ есть примитивный корень $2n+1$-й степени из единицы. То есть f_n аннулирующий многочлен для элемента α, а так как его степень равна n, то он совпадает с имеющим ту же степень многочленом m_α.

Отметим, что минимальный многочлен m_α один и тот же в случаях базисов и второго и третьего типов, а минимальные многочлены m_ζ и m_ζ^{-1} в случае базиса второго типа совпадают и равны $1 + x + \ldots + x^{2n}$, а в случае базиса третьего типа они различны и $m_\zeta m_\zeta^{-1} = 1 + x + \ldots + x^{2n}$.

Теорема 6. *Сложность перехода $B(n)$ от оптимального нормального базиса второго или третьего типа к соответствующему стандартному или наоборот в поле $GF(2^n)$ оценивается следующим образом: $B(n) \leqslant \frac{n}{2} log_2 n + 3n$.*

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

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

и базиса второго или третьего типа

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

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

$$B \to B' \to A' \to A$$

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

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

где α_i обозначает $\zeta^i + \zeta^{-i}$, базис

$$B' = \{\alpha_1, \ldots, \alpha_n\},$$

базис

$$A' = \{\alpha^1, \ldots, \alpha^n\}.$$

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

$$2^i \pmod p = \pm\pi(i) \in \{1,\dots,n\}. \tag{11}$$

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, значит равенство 2^i и 2^j при $0 \leqslant i < j < n$ по модулю p невозможно, так как иначе 2^{j-i} было бы равно 1 по модулю p, что противоречило бы примитивности 2 по этому модулю. А в силу равенства

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

(так как по теореме Ферма $2^{2n} = 1 \pmod p$, значит $2^n = -1 \pmod p$) отсюда следует (11).

В случае же базиса третьего типа 2 является квадратичным вычетом по модулю p (то есть существует такое r, что $2 = r^2 \pmod p$), поэтому все степени $2^k \pmod p$, $k = 1,\dots,n-1$ 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 $-1 = r^2 \bmod p$, а это бы приводило к противоречию с теоремой Ферма:

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

и тот факт, что произведение вычета на невычет является невычетом, откуда следует, что последовательность $-2^k \bmod p, k = 0,\dots,n-1$ образуют перестановку множества всех квадратичных невычетов по модулю p, то есть всех тех элементов, что не являются вычетами, в итоге получаем, что и в рассматриваемом случае тоже выполнено (11).

Таким образом, мы получили, что существует такая перестановка $\pi(i)$ чисел $\{1,\dots,n\}$, что для любого $i = 1\dots 2n$ выполняется равенство (11), то есть базис $\{\alpha,\dots,\alpha_n\}$ есть просто перестановка базиса $\{\alpha,\dots,\alpha^{2^{n-1}}\}$. Отрицательные индексы можно заменить на соответствующие положительные благодаря равенству $\alpha_i = \zeta^i + \zeta^{-i} = \alpha_{-i}$) по формуле

$$\alpha^{2^i} = \alpha_{|\pi(i)|}, \text{ (или для координат) } x_i = x'_{|\pi(i)|}).$$

Поэтому далее везде будем считать индексы положительными, и знак модуля писать не будем. Очевидно 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 $\widetilde{x}'$ к координатам $\widetilde{y}'$. Согласно теореме 5 его сложность оценивается как

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

Переход от базиса A' к базису A и преобразование координат $\widetilde{y}'$ к координатам $\widetilde{y}$. По рекуррентной формуле (8) 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

$$m_\alpha = f_n(\alpha) = a_1\alpha^0 + \dots + a_n\alpha^n = 0, \tag{12}$$

где α — генератор этих базисов, и не все коэффициенты a_i равны нулю. Сделаем явный переход от координат $\widetilde{y}'$ в почти стандартном базисе A' к координатам $\widetilde{y}$ в стандартном A, учитывая выражение (12)

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

и после перегруппировки коэффициентов имеем

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

откуда видно, что сложность перехода от почти стандартного базиса A' к стандартному A оценивается как $L_{A'A}(n) \leqslant (n-1)$.

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

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

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

$$A \to A' \to B' \to B.$$

Переход от базиса A к базису A' и координат $\widetilde{y}$ к $\widetilde{y}'$. Опять же в силу рекуррентной формулы (8) у нас есть минимальный аннулирующий многочлен (12), из явного вида которого мы можем выразить α^0, а именно:

$$\alpha^0 = \sum_{i=1}^{n} a_i \alpha^i. \tag{13}$$

Сделаем явный переход от координат $\widetilde{y}$ в стандартном базисе A к координатам $\widetilde{y}'$ в почти стандартном A', учитывая выражение (13)

$$\sum_{i=0}^{n-1} y_i \alpha^i = \sum_{i=1}^{n-1} y_i \alpha^i + y_0 (\sum_{i=1}^{n} a_i \alpha^i)$$

и после перегруппировки коэффициентов имеем

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

откуда видно, что сложность перехода от стандартного базиса A к почти стандартному базису A' оценивается как $L_{AA'} \leqslant (n-1)$.

Переход от базиса A' к базису B' и преобразование координат $\widetilde{y}'$ к координатам $\widetilde{x}'$. Вычислим 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 $(F^{-1}_{2^{k+1}})^T$ (обратную к матрице из теоремы 5) с помощью (8). В этой формуле рекуррентно выполнялись преобразования с векторами X_1 и X_2, переводящие их в вектора $Y_1 = (y'_1, \ldots, y''_{2^k})$ и $Y_2 = (y'_{2^k+1}, \ldots, y'_n)$, составляющие вектор $Y = (y'_1, \ldots, y'_n)$. Естественно, что обратное преобразование $(F^{-1}_{n-2^k})^T \otimes {Y_2}^T$ переведет вектор Y_2 в вектор X_2, а чтобы получить вектор X_1, надо сделать преобразование $(F^{-1}_{2^k})^T \otimes {Y_1}^T$. Так как

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

$$X_2 = \{x_{1+2^k}, \ldots, x_n\}^T,$$

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

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

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

и, как и раньше, придем к оценке

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

Переход от базиса B' к базису B и координат $\widetilde{x}'$ к $\widetilde{x}$. Переход получается посредством обратной перестановки к $\pi(i)$ (11), а его сложность оценивается, как и раньше $L_{B'B}(n) = 0$.

В результате имеем

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

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

$$(F^T_n)^{-1} = \begin{pmatrix} (F^T_m)^{-1} & o_m & G_m \\ 0 \ldots 0 & 1 & 0 \ldots 0 \\ O_m & o_m & (F^T_m)^{-1} \end{pmatrix},$$

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

Но можно и непосредственно проверить указанное тождество, так же, как и тождество

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

где $m = (n-1)/2$, матрица $G_m = F_m^{-1}I_m$ есть симметричное отражение матрицы F_m^{-1} относительно среднего столбца. 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 $GF(2^n)$.

Пример к теореме 6.

Приведем пример на применение теоремы 6, который также может служить примером алгоритмической реализации перехода от оптимального базиса 2-го или 3-го типа к стандартному и обратно.

Переход от оптимального нормального базиса второго или третьего типа к стандартному:

Пусть дано: $n = 5$, оптимальный нормальный базис второго типа $B = \{\alpha^{2^k}, k = 0,1,2,3,4\}$, элемент, записанный в этом базисе, $f = 1\cdot\alpha^{2^0} + 1\cdot\alpha^{2^1} + 0\cdot\alpha^{2^2} + 1\cdot\alpha^{2^3} + 1\cdot\alpha^{2^4}$, а то есть и вектор координат $\widetilde{x}^T = \{1,1,0,1,1\}$.

Надо найти: $\widetilde{y}$ — вектор координат f в стандартном полиномиальном базисе $A = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4\}$.

Шаг 1. *Переход от нормального базиса B к почти нормальному базису B' и координат $\widetilde{x}$ к $\widetilde{x}'$.*

а) В начале найдем перестановку $\pi(i)$ (11):

$$\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9 \pmod{11}\} = \{1,2,4,8,5,10,9,7,3,6\} =$$

$$= \{1,2,4,-3,5,-1,-2,-4,3,-5 \pmod{11}\},$$

из этого перестановка найдена:

$$2^i \pmod{11} = \pm\pi(i) \in \{1,\ldots,5\},$$

то есть

$$\pi = \begin{pmatrix} 2^0 & 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & 2^9 & (\mathrm{mod}\ 11) \\ 1 & 2 & 4 & -3 & 5 & -1 & -2 & -4 & 3 & -5 & (\mathrm{mod}\ 11) \end{pmatrix}. \quad (14)$$

b) Пользуясь перестановкой (14), найдем базис $B' = \{\alpha_1, \alpha_2, \alpha_4, \alpha_3, \alpha_5\}$, то есть элемент в этом базисе запишется так: $f = 1 \cdot \alpha_1 + 1 \cdot \alpha_2 + 0 \cdot \alpha_4 + 1 \cdot \alpha_3 + 1 \cdot \alpha_5$, (то есть поменяем местами координату 3 и 4 и от координат $(\widetilde{x})^T = (1, 1, 0, 1, 1)$ перейдем к координатам $(\widetilde{x}')^T = (1, 1, 1, 0, 1)$).

Шаг 2. *Переход от базиса* B' *к базису* B'' *и координат* $\widetilde{x}'$ *к* $\widetilde{x}''$.

Так как $2^2 < 5 < 2^3$, то перейдем к $B'' = \{\alpha_k, k = 1, ..., 8\}$ путем добавления нулей, то есть $\widetilde{x}'' = (\widetilde{x}', 0, 0, 0) = (\underbrace{1, 1, 1, 0}_{2^2}, \underbrace{1, 0, 0, 0}_{2^3 - 2^2})$.

Шаг 3. *Переход от базиса* B'' *к базису* A'' *и координат* $\widetilde{x}''$ *к* $\widetilde{y}''$. $A'' = \{\alpha^k, k = 1, \ldots, 8\}$.

По рекуррентной формуле (8) умножение матрицы $(F_8)^T$ на 8-мерный вектор $\widetilde{x}''$ сводится к двум умножениям 4-мерных векторов на матрицу $(F_4)^T$, то есть

$$(\widetilde{y}'')^T = (F_8)^T \otimes \widetilde{x}'' = (F_4)^T \otimes \begin{pmatrix} x_1'' + x_7'' \\ x_2'' + x_6'' \\ x_3'' + x_5'' \\ x_4'' \end{pmatrix} + \alpha^{2^2} (F_4)^T \otimes \begin{pmatrix} x_5'' \\ x_6'' \\ x_7'' \\ x_8'' \end{pmatrix}, \quad (15)$$

каждое из которых, в свою очередь, сводится к двум умножениям 2-мерных векторов на матрицу $(F_2)^T$, то есть

$$\widetilde{y}'' = (F_8)^T \otimes \widetilde{x}'' = (F_2)^T \otimes \begin{pmatrix} (x_1'' + x_7'') + (x_3'' + x_5'') \\ (x_2'' + x_6'') \end{pmatrix} + \alpha^2 (F_2)^T \otimes \begin{pmatrix} x_3'' + x_5'' \\ x_4'' \end{pmatrix} +$$

$$+ \alpha^4 (F_2)^T \otimes \begin{pmatrix} x_5'' + x_7 \\ x_6'' \end{pmatrix} + \alpha^6 (F_2)^T \otimes \begin{pmatrix} x_7'' \\ x_8'' \end{pmatrix},$$

где (F_2) — единичная матрица, то есть $(\widetilde{y}'') = (1, 1, 0, 0, 1, 0, 0, 0)$.

Шаг 4. *Переход от базиса* A'' *к базису* A' *и координат* $\widetilde{y}''$ *к* $\widetilde{y}'$. $A' = \{\alpha^k, k = 1, \ldots, 5\}$.

А теперь удалим последние координаты: $\widetilde{y}' = (1, 1, 0, 0, 1)$.

Шаг 5. *Переход от базиса* A' *к базису* A *и координат* $\widetilde{y}'$ *к* $\widetilde{y}$. $A = \{\alpha^k, k = 0, \ldots, 4\}$.

Построим минимальный аннулирующий многочлен m_α для генератора α. По рекуррентной формуле (9) получим:

$$\begin{aligned} f_0 &= 0 \\ f_1 &= x + 1 \\ f_2 &= x^2 + x \\ f_3 &= x^3 + x^2 + x + 1 \\ f_4 &= x^4 + x^3 \\ f_5 &= x^5 + x^4 + x^3 + x^2 + x + 1, \end{aligned}$$

то есть

$$m_\alpha := f_5(\alpha) = a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha^1 + a_0\alpha^0 = 0, \quad (16)$$

где $a_0 = a_1 = a_2 = a_3 = a_4 = a_5 = 1$. Применяя формулу (12) получим

$$\sum_{i=0}^{n-1} y_i\alpha^i = 1 \cdot \alpha^0 + (1+1)\alpha^1 + (1+1)\alpha^2 + (0+1)\alpha^3 + (0+1)\alpha^4,$$

откуда и получаем вектор координат в стандартном базисе $\widetilde{y} = (1, 0, 0, 1, 1)$. Таким образом, мы от представления многочлена в оптимальном нормальном базисе

$$f = 1 + \alpha^{2^1} + \alpha^{2^3} + \alpha^{2^4} \in B$$

перешли к представлению многочлена в стандартном базисе:

$$f = 1 + \alpha + \alpha^3 + \alpha^4 \in A.$$

Переход от стандартного базиса к оптимальному нормальному базису второго или третьего типа.

Пусть дано: $n = 5$, стандартный базис $A = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3, \alpha^4\}$, и элемент в этом базисе $f = \sum_{i=0}^{4} y_i\alpha^i$, с координатами $\widetilde{y} = \{1, 0, 0, 1, 1\}$.

Надо найти: $\widetilde{x}$ — вектор координат f в оптимальном нормальном базисе 2-го или 3-го типа $B = \{\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \alpha^{2^3}, \alpha^{2^4}\}$.

Так как условия на n удовлетворяют определению, значит для этого n существует оптимальный базис 2-го типа, следовательно, можно применять теорему.

Шаг 1. *Переход от базиса* A *к базису* A' *и координат* $\widetilde{y}$ *к* $\widetilde{y}'$. $A' = \{\alpha^{2^1}, \alpha^{2^2}, \alpha^{2^3}, \alpha^{2^4}, \alpha^{2^5}\}$.

Минимальный аннулирующий многочлен $m_\alpha = 0$ для $n = 5$ уже нами построен (то есть a_i нами найдены) (см. (16)), подставляя a_i в (12) получим

$$\sum_{i=1}^{n} y_i \alpha^i = (0+1)\alpha^1 + (0+1)\alpha^2 + (1+1)\alpha^3 + (1+1)\alpha^4 + 1 \cdot \alpha^5,$$

откуда и получается вектор координат в почти стандартном базисе A' $\widetilde{y} = (1, 1, 0, 0, 1)$.

Шаг 2. *Переход от базиса* A' *к системе* A'' *и координат* $\widetilde{y}'$ *к* $\widetilde{y}''$.

Переход осуществляется путем формального добавления нулей в конец вектора $\widetilde{y}'$: $(\widetilde{y}'')^T = (1, 1, 1, 0, 1, 0, 0, 0)$.

Шаг 3. *Переход от системы* A'' *к системе* B'' *и координат* $\widetilde{y}''$ *к координатам* $\widetilde{x}''$.

Умножение матрицы $(F_8^T)^{-1}$ на 8-мерный вектор $\widetilde{y}''$ сводится к двум умножениям 4-мерных векторов на матрицу $(F_4^T)^{-1}$ и «перепутанному» их сложению, то есть:

$$(\widetilde{x}'')^T = (\widetilde{X}_1, \widetilde{X}_2)^T = (F_8^T)^{-1} \otimes \widetilde{y}'' = (F_8^T)^{-1} \otimes (\widetilde{Y}_1, \widetilde{Y}_2)$$

(где вектор $\widetilde{Y}_1 = (y_1'', y_2'', y_3'', y_4'')^T$, а вектор $\widetilde{Y}_2 = (y_5'', y_6'', y_7'', y_8'')^T$) сводится к

$$(\widetilde{y}'') = (v_1 + w_3, v_2 + w_2, v_3 + w_1, v_4, w_1, w_2, w_3, w_4),$$

где вектора $\widetilde{v}$ и $\widetilde{w}$ считаются по формулам:

$$(v_1, v_2, v_3, v_4) = (F_4^T)^{-1} \otimes (\widetilde{X}_1) \tag{17}$$

и

$$(w_1, w_2, w_3, w_4) = (F_4^T)^{-1} \otimes (\widetilde{X}_2). \tag{18}$$

Каждая из формул (17) и (18), в свою очередь рекуррентным способом сводится также к двум умножениям 2-мерных векторов на матрицу $(F_2^T)^{-1} \equiv E$ (единичная матрица 2×2) и их «перепутанному» сложению то есть:

$$(v_1, v_2, v_3, v_4) = (p_1 + r_1, p_2, r_1, r_2),$$
$$(w_1, w_2, w_3, w_4) = (s_1 + t_1, s_2, t_1, t_2),$$

где

$$(p_1, p_2) = E \otimes (v_1, v_2)^T,$$
$$(r_1, r_2) = E \otimes (v_3, v_4)^T,$$
$$(s_1, s_2) = E \otimes (w_1, w_2)^T,$$
$$(t_1, t_2) = E \otimes (w_3, w_4)^T,$$

где $(\widetilde{y}'') = (p_1, p_2, r_1, r_2, s_1, s_2, t_1, t_2)$, то есть $p_1 = 1, p_2 = 1, r_1 = 0$, $r_2 = 0$, $s_1 = 1$, $s_2 = 0$, $t_1 = 0$, $t_2 = 0$. Поднимаясь рекурсивно вверх получим, что $(\widetilde{x}'') = (1, 1, 1, 0, 1)$.

Шаг 4. *Переход от системы* B'' *к базису* B' *и координат* $\widetilde{x}''$ *к координатам* $\widetilde{x}'$.

Удалим последние координаты: $(\widetilde{x}')^T = \{1,1,1,0,1\}$.

Шаг 5. *Переход от базиса* B' *к базису* B *и координат* $\widetilde{x}'$ *к координатам* $\widetilde{x}$.

По обратной перестановке к перестановке π (14) получим $\widetilde{x} = (1, 1, 0, 1, 1)$.

Таким образом, мы от представления многочлена в стандартном базисе

$$f = 1 + \alpha^3 + \alpha^4 \in A$$

перешли к представлению многочлена в оптимальном нормальном базисе 2-го типа:

$$f = 1 + \alpha^{2^1} + \alpha^{2^3} + \alpha^{2^4} \in B.$$

6. Оценки сложности арифметических операций в конечных полях

Пусть конечное поле $GF(2^n)$ представлено стандартным базисом, порожденным корнем неприводимого над $GF(2)$ многочлена $g(x)$ степени n. Сложность операции умножения многочленов степени $n-1$ над полем $GF(2)$ обозначим $M(n)$. Согласно [9] $M(n) =$

$O(n \log\log n)$. Как отмечалось в [10], на практике при значениях n порядка нескольких сотен лучше работает алгоритм Карацубы, имеющий теоретически худшую оценку $M(n) = O(n^{\log_2 3})$.

Оценим сложность $M_g(n)$ операции умножения в указанном представлении поля $GF(2^n)$. Так как умножение в рассматриваемом случае сводится к умножению многочленов над полем $GF(2)$ и последующему делению результата на многочлен $g(x)$ с остатком, то независимо от выбора $g(x)$ известна оценка [10] $M_g(n) = 3M(n) + O(n)$, если пренебречь сложностью предварительного вычисления некоторого многочлена $f(x)$, зависящего только от $g(x)$.

При удачном выборе $g(x)$ эту оценку можно улучшить. Действительно, если $g(x)$ содержит k одночленов, то сложность редукции по модулю $g(x)$ оценивается как kn, и поэтому имеем $M_g(n) = M(n)+kn$. 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. Далее, если не будет оговорено противное, вместо $M_g(n)$ пишем $M(n)$.

Возведение в квадрат элемента поля $GF(2^n)$ производится алгоритмом вставки нулей (в последовательность коэффициентов через каждый коэффициент вставляются по нулю), сложность которого оценивается числом n, после чего производится редукция по модулю g, в результате (с учетом сделанного выше замечания) имеем (теоретически не доказанную) оценку сложности возведения в квадрат $K(n) = 6n$.

Заметим, что, учитывая сделанные выше замечания, сложность возведения произвольного элемента поля $GF(2^n)$ в степень $d < 2^n$ можно оценить, используя некоторые результаты об аддитивных цепочках [11], как

$$O(n \log d) + O(\frac{M(n) \log d}{\log\log d}),$$

так как для возведения в степень d достаточно $\log_2 d$ возведений в квадрат и $O(\frac{\log d}{\log\log d})$ нетривиальных умножений.

Известно [11], что для почти всех d второе слагаемое по порядку нельзя уменьшить, но число нетривиальных умножений можно оценить снизу по порядку как $\log \nu(d)$, где $\nu(d)$ — число единиц в

двоичном разложении числа d, а также как $(l(d) - \log d)$, где $l(d)$ — аддитивная сложность числа d (определение см. в [11]).

Известно также [11], что оценка для второго слагаемого $M(n)\log\nu_2(d)$ по порядку достигается, например, для $d = 2^n - 2$, что можно обосновать, опираясь на равенства

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

Так как согласно формуле Ферма $f^{-1} = f^{2^n-2}$, то для операции инвертирования (вычисления обратного элемента) в поле понадобится не более $\lambda(n-1) + \nu(n-1)$ умножений и $(n-1)$-о возведение в квадрат, где $\lambda(n) = \lceil \log_2(n-1) \rceil$.

Поэтому сложность инвертирования в стандартном базисе оценивается как

$$(n-1)K(n) + (\lambda(n-1) + \nu(n-1))M(n),$$

а сложность деления $D(n)$ — как

$$(n-1)K(n) + (\lambda(n-1) + \nu(n-1) + 1)M(n).$$

Оценим сложность умножения в случае использования оптимального нормального базиса первого типа. Для выполнения умножения переходим к стандартному базису согласно теореме 2 со 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 $M_{O1}(n) \leqslant M(n) + 7n - 8$, где $M(n)$ — сложность умножения многочленов степени $n-1$.

В случае базисов второго и третьего типа аналогично получаем оценку

$$M_{O2}(n) \leqslant 3M(n) + \frac{3n}{2} log_2 n + O(n),$$

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 указанную выше общую оценку $M_g(n)$.

Оценим сложность инвертирования в оптимальных нормальных базисах. Возведение в квадрат выполняется «бесплатно», поэтому имеем оценку

$$I_O(n) \leqslant (\lambda(n-1)+\nu(n-1))(M_O(n)),$$

которая справедлива только для тех n, для которых существуют такие базисы. Аналогично, сложность возведения в произвольую степень $d < 2^n$ в оптимальных нормальных базисах оценивается как

$$O(\frac{M(n)\log d}{\log\log d}).$$

7. Приложение

В нем приведена составленная на основе компьютерных вычислений таблица размерностей полей $GF(2^n)$ при $1000 < n \leqslant 10000$, для которых существуют оптимальные нормальные базисы. В скобках после размерности указан тип базиса (если для рассматриваемого поля одновременно существуют базисы типа 1 и 2, то в скобках стоит 12; другие варианты не встречаются).

Таблицу для $n \leqslant 1000$ мы не приводим, так как она имеется, например, в [3]. Также мы не приводим вычисляемые программой для каждого оптимального нормального базиса матрицы A, T, определенные в начале статьи, и порождающие элементы этих базисов.

1013(2)	1014(2)	1018(1)	1019(3)	1026(2)	1031(3)	1034(2)
1041(2)	1043(3)	1049(2)	1055(3)	1060(1)	1065(2)	1070(2)
1090(1)	1103(3)	1106(2)	1108(1)	1110(2)	1116(1)	1118(2)
1119(3)	1121(2)	1122(1)	1133(2)	1134(2)	1146(2)	1154(2)
1155(3)	1166(2)	1169(2)	1170(1)	1178(2)	1185(2)	1186(1)
1194(2)	1199(3)	1211(3)	1212(1)	1218(2)	1223(3)	1228(1)
1229(2)	1233(2)	1236(1)	1238(2)	1251(3)	1258(1)	1265(2)
1269(2)	1271(3)	1274(2)	1275(3)	1276(1)	1278(2)	1282(1)
1289(2)	1290(1)	1295(3)	1300(1)	1306(1)	1310(2)	1323(3)
1329(2)	1331(3)	1338(2)	1341(2)	1346(2)	1349(2)	1353(2)
1355(3)	1359(3)	1370(2)	1372(1)	1380(1)	1394(2)	1398(2)
1401(2)	1409(2)	1418(2)	1421(2)	1425(2)	1426(1)	1430(2)

1439(3)	1443(3)	1450(1)	1451(3)	1452(1)	1454(2)	1463(3)
1469(2)	1478(2)	1481(2)	1482(1)	1492(1)	1498(1)	1499(3)
1505(2)	1509(2)	1511(3)	1518(2)	1522(1)	1530(1)	1533(2)
1539(3)	1541(2)	1548(1)	1559(3)	1570(1)	1583(3)	1593(2)
1601(2)	1618(1)	1620(1)	1626(2)	1636(1)	1649(2)	1653(2)
1659(3)	1661(2)	1666(1)	1668(1)	1673(2)	1679(3)	1685(2)
1692(1)	1703(3)	1706(2)	1730(2)	1732(1)	1733(2)	1734(2)
1740(1)	1745(2)	1746(1)	1749(2)	1755(3)	1758(2)	1763(3)
1766(2)	1769(2)	1773(2)	1778(2)	1779(3)	1785(2)	1786(1)
1790(2)	1791(3)	1806(2)	1811(3)	1818(2)	1821(2)	1829(2)
1835(3)	1838(2)	1845(2)	1850(2)	1854(2)	1859(3)	1860(1)
1863(3)	1866(12)	1876(1)	1883(3)	1889(2)	1898(2)	1900(1)
1901(2)	1906(1)	1923(3)	1925(2)	1926(2)	1930(1)	1931(3)
1938(2)	1948(1)	1953(2)	1955(3)	1958(2)	1959(3)	1961(2)
1965(2)	1972(1)	1973(2)	1978(1)	1983(3)	1986(1)	1994(2)
1996(1)	2001(2)	2003(3)	2006(2)	2009(2)	2010(2)	2026(1)
2028(1)	2039(3)	2045(2)	2046(2)	2049(2)	2052(1)	2055(3)
2063(3)	2066(2)	2068(1)	2069(2)	2078(2)	2079(3)	2082(1)
2098(1)	2109(2)	2114(2)	2115(3)	2121(2)	2126(2)	2129(2)
2130(12)	2140(1)	2141(2)	2163(3)	2174(2)	2178(2)	2181(2)
2186(2)	2195(3)	2198(2)	2212(1)	2220(1)	2223(3)	2225(2)
2231(3)	2236(1)	2241(2)	2242(1)	2246(2)	2253(2)	2258(2)
2266(1)	2268(1)	2273(2)	2291(3)	2292(1)	2295(3)	2301(2)
2308(1)	2310(2)	2318(2)	2319(3)	2332(1)	2338(1)	2339(3)
2345(2)	2351(3)	2356(1)	2361(2)	2370(1)	2388(1)	2391(3)
2393(2)	2394(2)	2399(3)	2406(2)	2415(3)	2436(1)	2438(2)
2451(3)	2458(1)	2459(3)	2466(12)	2471(3)	2475(3)	2476(1)
2478(2)	2483(3)	2486(2)	2493(2)	2501(2)	2505(2)	2511(3)
2519(3)	2525(2)	2529(2)	2530(1)	2538(12)	2543(3)	2548(1)
2549(2)	2553(2)	2556(1)	2559(3)	2573(2)	2578(1)	2585(2)
2589(2)	2594(2)	2613(2)	2615(3)	2620(1)	2630(2)	2651(3)
2654(2)	2658(1)	2666(2)	2675(3)	2676(1)	2682(1)	2692(1)
2693(2)	2698(1)	2699(3)	2703(3)	2706(1)	2715(3)	2721(2)
2738(2)	2739(3)	2740(1)	2741(2)	2750(2)	2753(2)	2759(3)
2763(3)	2778(2)	2781(2)	2786(2)	2788(1)	2795(3)	2796(1)
2802(1)	2811(3)	2818(1)	2819(3)	2823(3)	2825(2)	2829(2)
2836(1)	2841(2)	2842(1)	2846(2)	2850(12)	2858(2)	2860(1)

2870(2)	2871(3)	2874(2)	2889(2)	2891(3)	2895(3)	2903(3)
2906(2)	2908(1)	2913(2)	2919(3)	2921(2)	2925(2)	2934(2)
2938(1)	2939(3)	2951(3)	2956(1)	2961(2)	2962(1)	2963(3)
2969(2)	2993(2)	3005(2)	3010(1)	3014(2)	3018(1)	3023(3)
3026(2)	3033(2)	3036(1)	3050(2)	3065(2)	3066(1)	3071(3)
3082(1)	3086(2)	3098(2)	3099(3)	3101(2)	3105(2)	3114(2)
3123(3)	3131(3)	3134(2)	3138(2)	3143(3)	3149(2)	3155(3)
3158(2)	3161(2)	3171(3)	3179(3)	3183(3)	3186(1)	3189(2)
3194(2)	3198(2)	3202(1)	3234(2)	3245(2)	3252(1)	3273(2)
3275(3)	3298(1)	3299(3)	3303(3)	3306(1)	3309(2)	3318(2)
3322(1)	3326(2)	3329(2)	3345(2)	3346(1)	3350(2)	3351(3)
3354(2)	3359(3)	3366(2)	3370(1)	3381(2)	3389(2)	3390(2)
3401(2)	3411(3)	3412(1)	3413(2)	3414(2)	3431(3)	3434(2)
3441(2)	3449(2)	3453(2)	3455(3)	3458(2)	3460(1)	3466(1)
3468(1)	3473(2)	3474(2)	3485(2)	3490(1)	3491(3)	3495(3)
3498(1)	3506(2)	3509(2)	3513(2)	3516(1)	3519(3)	3521(2)
3532(1)	3534(2)	3538(1)	3539(3)	3546(1)	3551(3)	3554(2)
3556(1)	3563(3)	3570(1)	3579(3)	3580(1)	3593(2)	3603(3)
3605(2)	3609(2)	3612(1)	3614(2)	3618(2)	3621(2)	3623(3)
3626(2)	3636(1)	3641(2)	3642(1)	3653(2)	3658(1)	3665(2)
3674(2)	3676(1)	3690(1)	3700(1)	3705(2)	3708(1)	3725(2)
3729(2)	3732(1)	3738(2)	3749(2)	3753(2)	3758(2)	3761(2)
3770(2)	3773(2)	3774(2)	3778(1)	3779(3)	3786(2)	3791(3)
3794(2)	3795(3)	3796(1)	3801(2)	3802(1)	3803(3)	3810(2)
3821(2)	3834(2)	3843(3)	3845(2)	3850(1)	3851(3)	3852(1)
3858(2)	3863(3)	3876(1)	3878(2)	3879(3)	3894(2)	3906(1)
3911(3)	3914(2)	3916(1)	3922(1)	3926(2)	3930(1)	3938(2)
3939(3)	3941(2)	3946(1)	3950(2)	3953(2)	3959(3)	3966(2)
3974(2)	3975(3)	3988(1)	4002(1)	4012(1)	4018(1)	4019(3)
4020(1)	4026(2)	4034(2)	4043(3)	4046(2)	4055(3)	4058(2)
4061(2)	4073(2)	4085(2)	4089(2)	4090(1)	4092(1)	4098(1)
4109(2)	4110(2)	4115(3)	4118(2)	4121(2)	4131(3)	4132(1)
4134(2)	4138(1)	4145(2)	4146(2)	4155(2)	4156(1)	4181(2)
4193(2)	4211(2)	4214(2)	4215(3)	4218(1)	4221(2)	4223(2)
4228(1)	4233(2)	4242(1)	4252(1)	4256(2)	4258(1)	4260(1)
4263(3)	4269(2)	4271(3)	4281(2)	4282(1)	4286(2)	4298(2)
4299(2)	4304(2)	4311(3)	4313(2)	4323(3)	4331(3)	4334(2)

4338(2)	4346(2)	4348(1)	4349(2)	4356(1)	4362(1)	4365(2)
4370(2)	4372(1)	4373(2)	4391(3)	4396(1)	4401(2)	4403(2)
4409(2)	4410(2)	4418(2)	4419(3)	4430(2)	4433(2)	4443(2)
4450(1)	4461(2)	4466(2)	4475(3)	4481(2)	4482(1)	4484(2)
4485(2)	4492(1)	4499(2)	4503(3)	4505(2)	4506(1)	4514(2)
4516(1)	4524(2)	4529(2)	4546(1)	4551(3)	4563(3)	4575(2)
4580(2)	4586(2)	4590(2)	4599(3)	4601(2)	4602(1)	4610(2)
4613(2)	4619(3)	4620(1)	4628(2)	4636(1)	4641(2)	4646(2)
4655(3)	4659(3)	4661(2)	4668(2)	4670(2)	4671(2)	4674(2)
4685(2)	4690(1)	4695(3)	4698(2)	4709(2)	4710(2)	4716(2)
4718(2)	4722(1)	4733(2)	4739(2)	4745(2)	4766(2)	4769(2)
4773(2)	4775(3)	4786(1)	4788(1)	4793(2)	4800(2)	4806(2)
4809(2)	4812(1)	4814(2)	4821(2)	4830(2)	4838(2)	4839(3)
4848(2)	4866(2)	4871(3)	4874(2)	4876(1)	4883(2)	4895(3)
4901(2)	4916(2)	4925(2)	4929(2)	4932(1)	4935(3)	4941(2)
4943(3)	4950(2)	4953(2)	4956(1)	4961(2)	4970(2)	4972(1)
4974(2)	4983(3)	4986(1)				

5002(1)	5010(1)	5018(2)	5033(2)	5034(2)	5039(3)	5045(2)
5046(2)	5049(2)	5050(1)	5051(3)	5055(2)	5058(1)	5066(2)
5069(2)	5070(2)	5075(2)	5076(1)	5081(2)	5088(2)	5090(2)
5098(1)	5106(1)	5111(2)	5123(2)	5126(2)	5129(2)	5133(2)
5135(3)	5136(2)	5144(2)	5146(1)	5150(2)	5156(2)	5165(2)
5170(1)	5171(2)	5178(1)	5184(2)	5188(1)	5195(3)	5199(2)
5213(2)	5226(1)	5229(2)	5231(3)	5238(2)	5243(3)	5249(2)
5250(2)	5260(1)	5279(3)	5283(2)	5294(2)	5300(2)	5303(2)
5306(2)	5308(1)	5315(2)	5319(3)	5328(2)	5332(1)	5333(2)
5343(2)	5345(2)	5354(2)	5361(2)	5366(2)	5386(1)	5394(2)
5399(2)	5415(3)	5418(2)	5423(3)	5426(2)	5429(2)	5430(2)
5433(2)	5441(2)	5442(1)	5444(2)	5445(2)	5454(2)	5474(2)
5476(1)	5482(1)	5486(2)	5489(2)	5493(2)	5500(1)	5501(2)
5506(1)	5513(2)	5523(2)	5528(2)	5534(2)	5535(2)	5541(2)
5543(2)	5546(2)	5556(1)	5562(1)	5565(2)	5572(1)	5579(3)
5585(2)	5588(2)	5598(2)	5606(2)	5619(2)	5630(2)	5636(2)
5639(2)	5650(1)	5655(3)	5658(12)	5675(3)	5682(1)	5684(2)
5691(3)	5692(1)	5699(3)	5700(1)	5711(3)	5716(1)	5718(2)
5721(2)	5740(1)	5741(2)	5748(12)	5751(3)	5759(3)	5763(2)

5774(2)	5778(1)	5789(2)	5793(2)	5796(2)	5808(2)	5810(2)
5812(1)	5816(2)	5826(1)	5838(2)	5842(1)	5844(2)	5849(2)
5850(1)	5858(2)	5859(2)	5868(1)	5871(3)	5889(2)	5891(3)
5894(2)	5900(2)	5903(3)	5906(2)	5910(2)	5913(2)	5915(3)
5919(3)	5922(1)	5933(2)	5938(1)	5943(2)	5948(2)	5951(3)
5954(2)	5963(2)	5966(2)	5969(2)	5984(2)	5986(1)	5990(2)
5993(2)	6005(2)	6010(1)	6020(2)	6021(2)	6024(2)	6028(1)
6035(2)	6048(2)	6052(1)	6053(2)	6059(2)	6066(1)	6071(3)
6074(2)	6078(2)	6080(2)	6098(2)	6100(1)	6101(2)	6105(2)
6113(2)	6119(2)	6125(2)	6126(2)	6130(1)	6131(2)	6134(2)
6138(2)	6140(2)	6150(2)	6161(2)	6172(1)	6173(2)	6186(2)
6189(2)	6195(2)	6196(1)	6200(2)	6202(1)	6206(2)	6210(12)
6216(2)	6218(2)	6225(2)	6228(1)	6236(2)	6243(3)	6245(2)
6255(3)	6268(1)	6269(2)	6273(2)	6276(12)	6288(2)	6294(2)
6298(1)	6305(2)	6306(2)	6309(2)	6316(1)	6318(2)	6322(1)
6323(2)	6326(2)	6329(2)	6348(2)	6369(2)	6371(3)	6372(1)
6378(1)	6381(2)	6388(1)	6390(2)	6395(3)	6396(1)	6399(2)
6404(2)	6410(2)	6414(2)	6426(2)	6444(2)	6449(2)	6453(2)
6455(3)	6458(2)	6459(2)	6461(2)	6468(1)	6470(2)	6479(2)
6483(2)	6489(2)	6490(1)	6491(3)	6500(2)	6518(2)	6521(2)
6524(2)	6546(1)	6551(2)	6554(2)	6573(2)	6575(2)	6579(2)
6581(2)	6591(2)	6593(2)	6614(2)	6618(1)	6620(2)	6636(1)
6645(2)	6652(1)	6654(2)	6656(2)	6658(1)	6663(3)	6665(2)
6669(2)	6690(1)	6698(2)	6700(1)	6705(2)	6708(1)	6725(2)
6728(2)	6731(2)	6732(1)	6734(2)	6738(2)	6743(2)	6756(2)
6761(2)	6762(1)	6768(2)	6778(1)	6780(1)	6783(2)	6788(2)
6798(2)	6802(1)	6806(2)	6809(2)	6813(2)	6824(2)	6826(1)
6828(1)	6839(2)	6843(2)	6845(2)	6848(2)	6854(2)	6855(3)
6861(2)	6864(2)	6868(1)	6878(2)	6879(2)	6881(2)	6882(1)
6898(1)	6899(2)	6903(2)	6906(1)	6914(2)	6915(2)	6916(1)
6920(2)	6929(2)	6938(2)	6939(2)	6941(2)	6946(1)	6948(1)
6950(2)	6953(2)	6960(2)	6965(2)	6966(2)	6970(1)	6983(3)
6998(2)	6999(2)	7004(2)	7005(2)	7012(1)	7014(2)	7016(2)
7018(1)	7025(2)	7026(1)	7040(2)	7042(1)	7043(3)	7053(2)
7068(1)	7071(2)	7074(2)	7076(2)	7079(3)	7086(2)	7103(3)
7108(1)	7110(2)	7121(2)	7146(2)	7151(2)	7170(2)	7173(2)
7186(1)	7193(2)	7194(2)	7203(2)	7205(2)	7209(2)	7210(1)

7211(2)	7218(1)	7223(2)	7228(1)	7230(2)	7236(1)	7242(1)
7252(1)	7259(2)	7266(2)	7268(2)	7271(3)	7274(2)	7275(3)
7278(2)	7282(1)	7306(1)	7310(2)	7313(2)	7314(2)	7319(2)
7326(2)	7328(2)	7330(1)	7334(2)	7348(1)	7349(2)	7358(2)
7361(2)	7368(2)	7370(2)	7373(2)	7379(2)	7385(2)	7389(2)
7398(2)	7406(2)	7410(1)	7413(2)	7415(2)	7421(2)	7425(2)
7433(2)	7434(2)	7439(2)	7443(3)	7445(2)	7450(1)	7458(1)
7461(2)	7464(2)	7469(2)	7473(2)	7476(1)	7478(2)	7484(2)
7491(2)	7498(1)	7506(1)	7515(2)	7516(1)	7522(1)	7526(2)
7530(2)	7538(2)	7540(1)	7541(2)	7545(2)	7546(1)	7548(1)
7550(2)	7553(2)	7565(2)	7569(2)	7572(1)	7574(2)	7580(2)
7586(2)	7588(1)	7593(2)	7602(1)	7613(2)	7620(1)	7629(2)
7631(2)	7634(2)	7642(1)	7643(2)	7649(2)	7656(2)	7659(3)
7665(2)	7668(1)	7674(2)	7686(2)	7688(2)	7690(1)	7691(2)
7695(3)	7706(2)	7713(2)	7716(1)	7719(2)	7721(2)	7730(2)
7746(2)	7748(2)	7755(3)	7756(1)	7763(2)	7784(2)	7788(1)
7790(2)	7803(2)	7814(2)	7820(2)	7821(2)	7823(2)	7824(2)
7828(1)	7830(2)	7833(2)	7835(2)	7841(2)	7852(1)	7863(2)
7865(2)	7868(2)	7869(2)	7874(2)	7876(1)	7880(2)	7882(1)
7883(3)	7886(2)	7893(2)	7895(2)	7898(2)	7900(1)	7901(2)
7904(2)	7906(1)	7911(2)	7929(2)	7932(1)	7940(2)	7943(3)
7948(1)	7950(2)	7953(2)	7959(2)	7961(2)	7979(3)	7985(2)
7995(2)	8000(2)	8003(3)	8016(2)	8031(2)	8033(2)	8034(2)
8043(3)	8051(2)	8052(1)	8063(2)	8068(1)	8069(2)	8092(1)
8093(2)	8094(2)	8096(2)	8108(2)	8111(2)	8114(2)	8115(3)
8116(1)	8122(1)	8126(2)	8133(2)	8136(2)	8146(1)	8150(2)
8159(2)	8166(2)	8169(2)	8170(1)	8174(2)	8178(1)	8181(2)
8190(2)	8205(2)	8210(2)	8213(2)	8218(1)	8220(1)	8223(3)
8226(2)	8236(1)	8238(2)	8240(2)	8242(1)	8243(3)	8246(2)
8259(2)	8264(2)	8268(1)	8273(2)	8280(2)	8283(3)	8286(2)
8290(1)	8292(1)	8301(2)	8303(3)	8309(2)	8310(1)	8325(2)
8336(2)	8346(2)	8349(2)	8351(2)	8362(1)	8373(2)	8381(2)
8386(1)	8393(2)	8411(2)	8414(2)	8421(2)	8422(1)	8428(1)
8441(2)	8442(1)	8446(1)	8450(2)	8451(3)	8465(2)	8466(1)
8471(3)	8481(2)	8489(2)	8490(2)	8493(2)	8505(2)	8510(2)
8512(1)	8513(2)	8523(2)	8526(2)	8538(1)	8546(2)	8549(2)
8553(2)	8561(2)	8562(1)	8568(2)	8572(1)	8579(3)	8583(2)

8591(3) 8594(2) 8596(1) 8598(1) 8601(2) 8603(2) 8604(2)
8608(1) 8619(2) 8626(1) 8628(2) 8649(2) 8658(2) 8663(3)
8666(2) 8668(1) 8675(3) 8676(1) 8679(2) 8692(1) 8693(2)
8694(2) 8698(1) 8709(2) 8715(2) 8721(2) 8730(1) 8735(2)
8738(2) 8740(1) 8741(2) 8746(1) 8754(2) 8759(3) 8786(2)
8789(2) 8798(2) 8799(3) 8802(1) 8806(1) 8811(2) 8813(2)
8818(1) 8820(1) 8834(2) 8836(1) 8841(2) 8853(2) 8856(2)
8866(1) 8873(2) 8874(2) 8886(1) 8891(2) 8894(2) 8903(3)
8913(2) 8918(2) 8919(3) 8922(1) 8925(2) 8931(3) 8932(1)
8945(2) 8951(3) 8954(2) 8955(3) 8961(2) 8962(1) 8968(1)
8969(2) 8970(1) 8978(2) 8979(3) 8988(2) 8990(2) 8994(2)
8998(1) 9006(2) 9010(1) 9021(2) 9023(2) 9028(1) 9029(2)
9038(2) 9044(2) 9048(1) 9058(1) 9059(2) 9066(2) 9071(3)
9074(2) 9084(2) 9090(2) 9095(3) 9105(2) 9114(2) 9125(2)
9126(2) 9134(2) 9144(2) 9150(1) 9155(2) 9160(1) 9164(2)
9172(1) 9180(1) 9183(3) 9189(2) 9202(1) 9206(2) 9213(2)
9216(2) 9220(1) 9221(2) 9226(1) 9230(2) 9240(1) 9246(2)
9256(1) 9260(2) 9270(2) 9276(2) 9282(1) 9292(1) 9293(2)
9296(2) 9318(2) 9322(1) 9330(2) 9335(3) 9336(1) 9340(1)
9342(1) 9348(1) 9350(2) 9356(2) 9359(3) 9365(2) 9370(1)
9371(3) 9374(2) 9378(2) 9386(2) 9393(2) 9396(1) 9418(1)
9419(3) 9420(1) 9429(2) 9432(1) 9434(2) 9436(1) 9449(2)
9455(3) 9458(2) 9459(3) 9466(1) 9473(2) 9478(1) 9479(3)
9486(2) 9489(2) 9490(1) 9504(2) 9506(2) 9518(2) 9525(2)
9532(1) 9534(2) 9538(1) 9539(2) 9543(2) 9546(1) 9569(2)
9570(2) 9578(2) 9581(2) 9586(1) 9590(2) 9600(1) 9603(3)
9606(2) 9609(2) 9612(1) 9615(2) 9618(1) 9624(2) 9628(1)
9629(2) 9642(1) 9650(2) 9659(3) 9660(1) 9666(2) 9676(1)
9686(2) 9689(2) 9693(2) 9695(2) 9696(1) 9701(2) 9711(2)
9713(2) 9716(2) 9720(2) 9731(2) 9732(1) 9734(2) 9741(2)
9748(1) 9750(2) 9753(2) 9765(2) 9766(1) 9770(2) 9771(2)
9776(2) 9785(2) 9791(2) 9798(2) 9801(2) 9802(1) 9830(2)
9832(1) 9848(2) 9849(2) 9850(1) 9854(2) 9858(1) 9863(2)
9869(2) 9875(3) 9881(2) 9882(1) 9900(1) 9906(1) 9909(2)
9922(1) 9926(2) 9930(2) 9933(2) 9940(1) 9944(2) 9945(2)
9948(1) 9959(2) 9963(2) 9968(2) 9974(2) 9981(2) 9986(2)
9989(2) 9995(3) 9998(2)

Список литературы

[1] Берлекемп Е. Алгебраическая теория кодирования. М.: Мир, 1971.

[2] Лидл Р., Нидеррейтер Х. Конечные поля. М.: Мир, 1988.

[3] Jungnickel D. Finite fields: Structure and arifmetics. Wissenschaftsverlag, 1995.

[4] Mullin R. C., Onyszchuk I. M., Vanstone S. A., Wilson R. M. Optimal normal bases in $GF(p^n)$ // Discrete Applied Mathematics. 22. 1988/89. P. 149–161.

[5] Gao, Lenstra. Optimal normal bases // Design, Codes and Cryptography. 2. 1992. P. 315–323.

[6] Ash, Blake, Vanstone S. A. Low complexity normal bases // Discrete Applied Mathematics. 25. 1988/89. P. 191–210.

[7] Gao, Vanstone S. A. On orders of optimal normal basis generators. 64. N 211. 1995. P. 1227–1233.

[8] Gao, von zur Gathen J., Panario. Gauss periods: orders and cryptografical applications // Mathematics of Computation. V. 67. N 221. 1998. P. 343–352.

[9] Schonhage A. Schnelle Multiplication von Polynomen über Körpern der Charakteristik 2 // Acta Informatica. 7. 1977. P. 395–398.

[10] von zur Gathen. J, Gerhard J. Computer algebra. Cambridge University Press, 1999.

[11] Кнут Д. Искусство программирования на ЭВМ. Т. 2. М.: Мир, 1977.