УДК 519.7 + 512.624

А. А. Бурцев[1], *С. Б. Гашков*[2]

[1]Московский физико-технический институт (государственный университет)
[2]Московский государственный университет им. М. В. Ломоносова

О схемах для арифметики в конечных полях

В работе доказывается, что для любого $\varepsilon > 0$ при любом m, $n = m^s$ и $s \geqslant s_\varepsilon$ можно выбрать в поле $GF(2^n)$ базис, для которого схемная сложность умножения меньше $n^{1+\varepsilon/2}$, а сложность инвертирования меньше $n^{1+\varepsilon}$. При $n = 2 \cdot 3^k$ в некотором базисе получены оценки сложности умножения $n(\log_3 n)^{(\log_2 \log_3 n)/2+O(1)}$, и по порядку такие же оценки получены для инвертирования.

Ключевые слова: булевы схемы, сложность схем, арифметика, конечные поля.

1. Введение

Известно (см. [1], [2]), что при использовании стандартных базисов в полях $GF(2^n)$ сложность булевой схемы для умножения, построенной из двухвходовых элементов, равна $O(n \log n \log\log n)$. Для инвертирования (т.е. вычисления мультипликативного обратного в данном поле) известен быстрый алгоритм Евклида с оценкой сложности $O(n \log^2 n \log\log n)$ (см. [1], [3]). Однако мультипликативная константа в этой оценке велика (несколько сотен), и при реальных значениях n стандартный алгоритм Евклида работает быстрее. Кроме того, этот алгоритм затруднительно применить при построении булевой схемы для инвертирования. Методом [4] можно построить такую схему сложности: $I(n) = O(n^{(\omega+1)/2} \log_2 n)$, где ω — экспонента матричного умножения. Однако величина мультипликативной константы здесь с трудом поддается оценке, также трудно оценить глубину этой схемы. Используя [5], можно построить схему для инвертирования глубины $O(\log_2^2 n)$ и сложности $O(n^{\log_2 \sqrt{14}} (\log_2 n)^{\log_2 8/7})$, где мультипликативные константы сравнительно невелики, но и эта схема при реальных значениях n представляется неэффективной.

При использовании в поле $GF(2^n)$ нормального базиса можно построить схему для умножения сложности $O(n^2/\log n)$ (см. [6]). Если для инвертирования применить метод [7] (основанный на методе Шольца—Брауэра для вычисления $2^n - 1$ аддитивными цепочками [8]), то можно построить схему сложности $O(M_N(n) \log n) = O(n^2)$ с небольшой мультипликативной константой в оценке, где $M_N(n)$ — сложность умножения в данном базисе. Для некоторых специальных нормальных базисов (существующих не при всех n) можно построить более эффективные схемы для умножения, и, как следствие, для инвертирования. В [6] показано, что для оптимальных нормальных базисов первого типа можно построить мультиплер сложности $M(n) + O(n)$, где $M(n)$ — сложность умножения двоичных многочленов степени $n - 1$. Для оптимальных нормальных базисов второго типа в [6] указана оценка $3M(n)) + \frac{3n}{2} \log_2 n + O(n)$. В [6] также показано, что если $n = mk$, $m, k \geqslant n^C, C \leqslant 1/2$, $(m, k) = 1$, то для некоторого нормального базиса сложность умножения равна $O(n(m + k)/\log n) = O(n^{2-C}/\log n)$, откуда следует, что если n — достаточно гладкое число, то для некоторого нормального базиса сложность умножения равна $O(n^{2-C})$ при $C > 0$, характеризующем гладкость числа n. В [4] доказано, что для гауссовых нормальных базисов типа k в поле $GF(2^n)$ сложность умножения равна $O(M(nk))$, а в [9] подобный результат получен в более общем случае.

2. Схемы в поле $GF(2^n)$ при $n = m^s$

К упомянутым результатам можно добавить также следующие.

Теорема 1. *Для любого $\varepsilon > 0$ при любом m $n = m^s$ и $s \geqslant s_\varepsilon$ можно указать в поле $GF(2^n)$ базис (не стандартный и не нормальный), в котором можно построить схему умножения сложности $M(m^s) < n^{1+\varepsilon/2}$ и схему инвертирования сложности $I(m^s) < n^{1+\varepsilon}$.*

Доказательство. Пусть $k < s$ — параметр, значение которого укажем позднее. Выберем наименьшее r такое, что $2^{m^r} \geqslant 2m^k - 1$, и $r = s \bmod k$. Тогда $r = O(k)$. Поле

$$GF\left(2^{m^s}\right) = GF\left(q^{m^{s-r}}\right) = GF\left(q^{m^{kl}}\right), q = 2^{m^r},$$

представим в виде башни расширений

$$GF(q) \subset GF\left(q^{m^k}\right) \subset GF\left(\left(q^{m^k}\right)^{m^k}\right) = GF\left(q^{m^{2k}}\right) \subset \ldots \subset GF\left(q^{m^{kl}}\right).$$

Для каждого этажа башни

$$GF(q_i) = GF\left(q^{m^{ik}}\right) \subset GF\left(\left(q^{m^{ik}}\right)^{m^k}\right) = GF\left(q^{m^{(i+1)k}}\right) = GF(q_{i+1})$$

выберем стандартный базис $\{1, \alpha, \ldots, \alpha^{m^k-1}\}$, определяемый неприводимым над полем $GF(q_i)$ многочленом $p_i(x)$ степени m^k таким образом, чтобы элемент α порождал нормальный базис $\{\alpha, \alpha^Q \ldots, \alpha^{Q^{m^k-1}}\}$, где $Q = q_i$. Тогда произвольный элемент поля $GF(q_{i+1})$ можно представить в виде m^k-мерного вектора с компонентами из поля $GF(q_i)$ и в виде $m^{k(i+1)}$-мерного вектора с компонентами из поля $GF(q)$. Умножение в поле $GF(q_{i+1})$ можно свести к умножению по модулю многочлена p_i двух многочленов степени $t = m^k - 1$ над полем $GF(q_i)$. Известно [1], что умножение в поле $GF(q_{i+1})$ сводится к трем умножениям многочленов степени t над полем $GF(q_i)$ и t сложениям в этом поле. Для умножения двух многочленов f, g степени t над полем $GF(q_i)$ можно сначала вычислить значения $f(a_i), g(a_i)$ на произвольных $2t+1$ элементах его подполя $GF(q)$, выполнить $2t+1$ умножение в поле $GF(q_i)$ и потом, используя интерполяционную формулу, восстановить по значениям $h(a_i) = f(a_i)g(a_i)$ коэффициенты произведения $h(x) = f(x)g(x)$. Для выполнения всех этих операций с помощью схемы Горнера и формулы Лагранжа требуется $O(t^2)$ операций сложения и умножения на элементы подполя $GF(q)$ в поле $GF(q_i)$. Поэтому сложность умножения в поле $GF(q_{i+1})$ оценивается как

$$M(GF(q_{i+1})) \leqslant 3(2m^k - 1)M(GF(q_i)) + O(m^{2k})m^{ik}(\log_2 q)^{\log_2 3},$$

так как сложение в поле $GF(q_i)$ выполняется со сложностью $\log_2 q_i = m^{ik} \log_2 q$, а сложность умножения на элементы подполя $GF(q)$ равна $M(GF(q))m^{ik} = O(\log_2 q)^{\log_2 3}m^{ik}$, потому, что это умножение сводится к m^{ik} умножениям в поле $GF(q)$. Если обозначить $M(GF(q_i))$ через $M(i)$, а $3(2m^k - 1)$ через a, то полученное рекуррентное неравенство переписывается в виде $M(i+1) \leqslant aM(i) + bm^{(i+1)k}$, где $b = O(a)(m^k m^{r\log_2 3}) = O(a)m^{O(k)}$, $M(0) = M(GF(q)) = O(\log_2 q)^{\log_2 3}$. Применяя индукцию, имеем

$$M(l) \leqslant a^l M(0) + b\left(a^{l-1}m^k + a^{l-2}m^{2k} + \ldots + m^{lk}\right),$$

следовательно:

$$M(l) \leqslant a^l M(0) + a^l b\frac{1 - (m^k/a)^{l+1}}{1 - m^k/a} \leqslant a^l M(0) + \frac{a^l b}{1 - m^k/a} \leqslant$$

$$\leqslant a^l M(0) + 3a^l b/2 = O(a^{l+1})m^{O(k)} = O(a)m^{O(k)}2^{l\log_2 3(2m^k-1)}.$$

Учитывая, что $q_l = q^{m^{kl}}$, имеем $l = (\log_2 \log_q q_l)/\log_2 m^k$, $\log_2 q_l = n$,

$$M(GF(2^n)) = M(GF(q_l)) = O(m^{r\log_2 3})2^{l\log_2 3(2m^k-1)} = m^{O(k)}2^{\frac{\log_2 \log_q q_l \log_2 3(2m^k-1)}{\log_2 m^k}} =$$

$$= m^{O(k)}(\log_q q_l)^{\log_{m^k} 3(2m^k-1)} = m^{O(k)}(\log_2 q_l)^{\log_{m^k} 3(2m^k-1)} = m^{O(k)} n^{\log_{m^k} 3(2m^k-1)}.$$

Поскольку $\log_{m^k} 3(2m^k-1) \to 1$ при $m^k \to \infty$, то для любого $\varepsilon > 0$ при любом m, $n = m^s$ и $s \geqslant s_\varepsilon$, имеем $M\left(GF(2^n)\right) = M\left(GF(2^{m^s})\right) = n^{1+\varepsilon/2}$. Умножение на каждом этаже башни можно выполнять и в нормальном базисе, если выполнить переход к стандартному базису, произвести умножение в нем и вернуться опять в нормальный базис. Грубая оценка сложности переходов между базисами равна

$$m^{2k} M(GF(q_i)) + (m^{2k} - m^k) m^{ik+r},$$

ведь для выполнения как прямого, так и обратного преобразования координат требуется не более m^{2k} умножений и не более $m^{2k} - m^k$ сложений в поле $GF(q_i)$, имеющем размерность m^{ik+r}. С помощью циклических сдвигов вычислим в нормальном базисе систему степеней

$$x^Q, x^{Q^2}, \ldots, x^{Q^{m^k-1}},\ Q = q_i.$$

Возьмем кратчайшую линейную аддитивную цепочку (см. [8]) для числа $t = m^k - 1$, $a_0 = 1, a_1 = 2, a_2, \ldots, a_L = t$ длины $L = L(t)$, т.е. такую последовательность, что каждый ее член a_n при $n > 0$ равен $a_{n-1} + a_k$, $k < n$ (если $k = n-1$, то операция вычисления a_n называется *шагом удвоения*, а если $k < n-1$ — *линейным шагом*). Построим линейную аддитивную цепочку, содержащую подпоследовательность

$$\frac{Q^{a_1}-1}{Q-1}, \frac{Q^{a_2}-1}{Q-1}, \ldots, \frac{Q^t-1}{Q-1},$$

между соседними членами которой производятся несколько последовательных шагов удвоения и один линейный шаг, пользуясь формулами

$$\frac{Q^{a_i}-1}{Q-1} = \frac{Q^{a_j+a_h}-1}{Q-1} = Q^{a_h}\frac{Q^{a_j}-1}{Q-1} + \frac{Q^{a_h}-1}{Q-1}.$$

Так как возведение в степень Q^n в нормальном базисе делается бесплатно, а $x^{(Q^{a_0}-1)/(Q-1)} = x$, то для вычисления $K(x) = x^{(Q^{t+1}-Q)/(Q-1)}$ требуется только $L = L(m^k-1)$ операций умножения. Еще одно умножение требуется для вычисления $N(x) = xK(x)$. Поэтому сложность совместного вычисления $K(x), N(x)$ оценивается как

$$LM(GF(q_{i+1})) \leqslant L\left(3(m^{2k}+2m^k-1)M(GF(q_i)) + O(m^{2k})m^{ik}(m^r)^{\log_2 3}\right).$$

Используя формулу $x^{-1} = K(x)/N(x)$, получаем рекуррентную оценку сложности инвертирования:

$$I(\log_2 q_{i+1}) = I\left(m^{(i+1)k+r}\right) \leqslant I\left(m^{ik+r}\right) + m^k M(GF(q_i)) +$$

$$+ L(m^k-1)\left(3(m^{2k}+2m^k-1)M(GF(q_i)) + O(m^{2k})m^{ik}(m^r)^{\log_2 3}\right).$$

Очевидно, что $L(t) \leqslant \lambda_2(t) + \nu_2(t) - 1 \leqslant 2\log_2 t \leqslant 2k\log_2 m$, где $\lambda_2(t)$ — длина двоичной записи числа t, а $\nu_2(t)$ — число единиц в ней (см. [8], где приведены и более точные оценки). Из полученных выше оценок по индукции с помощью неравенства $aM(n) \leqslant M(an)$ выводим оценку

$$I(m^s) = I\left(m^{lk+r}\right) = I(\log_2 q_l) \leqslant I(m^r) + O(km^{2k}\log_2 m)M(\log_2 q_{l-1}) =$$

$$= I(m^r) + O(km^k \log_2 m)M(m^s) = O(km^k \log_2 m)M(m^s).$$

Теорема доказана.

Укажем конкретный пример применения данного метода. Пусть $m = 2, n = m^s$. Выберем $k = 8$, тогда $\log_{m^k} 3(2m^k-1) = \log_{256} 1533 < 1.33$ Получаем как следствие в некотором базисе поля $GF(2^{2^n})$ оценку сложности умножения $O(2^{n^{1.33}})$ и оценку сложности инвертирования $I(n) = O(M(n))$. Эти оценки асимптотически лучше оценок [10] (полученных для другого базиса).

3. Схемы в поле $\mathbf{GF}(2^n)$ при $\mathbf{n = 2 \cdot 3^k}$

При $m = 3$ можно уточнить доказанную теорему следующим образом.

Теорема 2. *При $n = 2 \cdot 3^k$ в поле $GF(2^n)$ можно указать некоторый (не стандартный и не нормальный) базис и построить в нем схемы умножения и инвертирования сложности:*

$$M(n) = n(\log_3 n)^{(\log_2 \log_3 n)/2+O(1)}, I(n) = O(M(n)).$$

Доказательство. Положим $q_i = 2^{a_i}, a_i = 2 \cdot 3^{b_i}, b_i = 2^i$ и рассмотрим башню полей

$$GF(q_0) \subset GF(q_1) \subset \ldots \subset GF(q_k).$$

Так как $q_i - 1 = 2^{a_i} - 1$ кратно $3^{b_i+1} = 3n_i$, то в поле $GF(q_i)$ найдется элемент порядка $3^{b_i+1} = 3n_i$, и, значит, определено дискретное преобразование Фурье порядка $3^{b_i+1} = 3n_i$ Как следует из [11], многочлены степени меньше $n_i = 3^{b_i} = a_i/2$ над полем $GF(q_i)$ могут быть перемножены с помощью $24n_i \log_3 n_i + O(n_i)$ умножений и $68n_i \log_3 n_i + O(n_i)$ сложений в этом поле. Если обозначить сложность умножения в поле $GF(q_i)$ через $M(GF(q_i))$, то сложность умножения многочленов степени меньше n_i над полем $GF(q_i)$ будет оцениваться как

$$(24n_i \log_3 n_i + O(n_i))M(GF(q_i)) + (68n_i \log_3 n_i + O(n_i))n_i.$$

Обозначим далее эту оценку через M_i. Выберем в этом поле примитивный элемент α_i, тогда двучлен $f_i = x^{n_i} - \alpha_i$ будет неприводимым согласно теореме 3.75 [12], так как $n_i = 3^{b_i}$ делит $q_i - 1$, а значит, и $q_{i+1} - 1 = 2^{a_{i+1}} - 1$. Выбирая в расширении $GF(q_{i+1})$ поля $GF(q_i)$ стандартный базис, соответствующий двучлену f_i, и замечая, что умножение в этом базисе сводится к умножению многочленов степени меньше n_i над полем $GF(q_i)$ и приведению результата по модулю f_i (которое выполняется школьным алгоритмом деления с помощью n_i операций умножения и n_i операций сложения в поле $GF((q_i))$), имеем

$$M(GF(q_{i+1})) \leqslant M_i + n_i M(GF(q_i)) + a_{i+1} \leqslant$$

$$\leqslant (24n_i \log_3 n_i + O(n_i))M(GF(q_i)) + (68n_i \log_3 n_i + O(n_i))n_i + a_{i+1} \leqslant$$

$$\leqslant (12a_i \log_3 a_i + O(a_i))M(GF(q_i)) + (17a_i^2 \log_3 a_i + O(a_i^2)) + a_{i+1} \leqslant$$

$$\leqslant (12a_i \log_3 a_i + O(a_i))M(GF(q_i)) + (17a_i^2 \log_3 a_i + O(a_i^2)) \leqslant$$

$$\leqslant (12a_i b_i + O(a_i))M(GF(q_i)).$$

Отсюда по индукции следует, что

$$\log_2 M(GF(q_n)) \leqslant \sum_{i=1}^{n-1} \log_2 12a_i b_i + O(1) = \sum_{i=1}^{n-1}((\log_2 3)2^i + i \log_2 24) + O(1) \leqslant$$

$$\leqslant (\log_2 3)2^n + n^2/2 + (2\frac{1}{2} + \log_2 3)n + O(1),$$

значит,

$$M(GF(q_n)) \leqslant O\left(3^{2^n+n} 2^{(n^2+5n)/2}\right), q_n = 2^{2 \cdot 3^{2^n}}.$$

Обозначая для краткости $a_n = 2 \cdot 3^{2^n}$ через N, имеем

$$M(GF(2^N)) \leqslant N(\log_3 N)^{n/2+O(1)} = N(\log_3 N)^{(\log_2 \log_3 N)/2+O(1)}.$$

Получим теперь оценку для сложности инвертирования. В расширении $GF(q_{i+1})$ поля $GF(q_i)$ выполняем инвертирование по формуле

$$x^{-1} = K(x)N(x)^{-1}, K(x) = x^{q_i} x^{q_i^2} \ldots x^{q_i^{n_i-1}}, N(x) = xK(x).$$

Так как

$$N(x)^{q_i} = x^{q_i}x^{q_i^2}\dots x^{q_i^{n_i}} = x^{q_i}x^{q_i^2}\dots x^{q_i^{n_i-1}}x = N(x),$$

то $N(x) \in GF(q_i)$, поэтому для инвертирования нужно вычислить $K(x), N(x)$, потом выполнить инвертирование в подполе $GF(q_i)$ и n_i раз выполнить умножение в поле $GF(q_i)$.

Для вычисления $N(x), K(x)$ сначала найдем $y = xx^{q_i^{n_i/3}}x^{q_i^{2n_i/3}}$, а потом

$$N(x) = yy^{q_i}\dots y^{q_i^{n_i/3-1}}, K(x) = y^{q_i}\dots y^{q_i^{n_i/3-1}}x^{q_i^{n_i/3}}x^{q_i^{2n_i/3}}.$$

Поскольку

$$y^{q_i^{n_i/3}} = x^{q_i^{n_i/3}}x^{q_i^{2n_i/3}}x^{q_i^{n_i}} = xx^{q_i^{n_i/3}}x^{q_i^{2n_i/3}} = y,$$

то $y \in GF(q_i^{n_i/3})$. Значит, для вычисления y можно сделать 2 умножения в поле $GF(q_{i+1})$ и 2 операции возведения в степени $q_i^{n_i/3}, q_i^{2n_i/3}$ в том же поле, потом вычислить

$$N(x) = yy^{q_i}\dots y^{q_i^{n_i/3-1}}$$

и для вычисления $K(x)$ сделать одно умножение в поле $GF(q_{i+1})$ на элемент подполя $GF(q_i^{n_i/3})$. Учитывая, что произвольный элемент поля $GF(q_{i+1})$ можно представить в виде

$$X_0 + X_1\gamma_i + X_2\gamma_i^2,$$

где $X_j = x_j + x_3\gamma_i^{3+j} + x_{3(n_i/3-1)+j}\alpha_i^{3(n_i/3-1)} \in GF(q_i^{n_i/3}), j = 0,1,2$, то умножение в поле $GF(q_{i+1})$ на элемент подполя $GF(q_i^{n_i/3})$ сводится к трем умножениям в этом подполе. Поле $GF(q_i^{n_i/3})$ является расширением степени $n_i/3 = 3^{b_i-1}$ подполя $GF(q_i)$ и в нем можно выбрать базис $\{1, \beta_i, \dots, \beta_i^{n_i/3-1}\}$, где $\beta_i^{n_i/3} = \alpha_i$. Умножение в этом базисе совпадает с умножением многочленов степени $n_i/3$ по модулю неприводимого над полем $GF(q_i)$ многочлена $x^{n_i/3}+\alpha_i$. В расширении $GF(q_i) \subset GF(q_{i+1})$ ранее был выбран базис $\{1, \gamma_i, \dots, \gamma_i^{n_i-1}\}$, где $\gamma_i^{n_i} = \alpha_i$. Положим $\beta_i = \gamma_i^3$. Тогда произвольный элемент подполя $GF(q_i^{n_i/3})$ имеет относительно базиса $\{1, \beta_i, \dots, \beta_i^{n_i/3-1}\}$ координаты, которые совпадают с $n_i/3$ координатами этого элемента относительно базиса $\{1, \alpha_i, \dots, \alpha_i^{n_i-1}\}$ (а остальные его координаты в указанном базисе равны нулю). Поэтому сложность умножения элементов данного подполя оценивается неравенством

$$M(GF(q_i^{n_i/3})) \leqslant M(a_{i+1}/3) + (n_i/3)M(GF(q_i)) + a_{i+1}/3 \leqslant$$

$$\leqslant (8n_i\log_3 n_i + O(n_i))M(GF(q_i)) + ((68/3)n_i\log_3 n_i + O(n_i))n_i + a_{i+1}/3 \leqslant$$

$$\leqslant (4a_ib_i + O(a_i))M(GF(q_i)).$$

Оценим сложность возведения в степени $q_i^{n_i/3}, q_i^{2n_i/3}$ в поле $GF(q_{i+1})$. Произвольный элемент x поля $GF(q_{i+1})$ можно представить в виде

$$X_0 + X_1\gamma_i + X_2\gamma_i^2,$$

где $X_j \in GF(q_i^{n_i/3}), j = 0,1,2$, то

$$x^{q_i^{n_i/3}} = X_0^{q_i^{n_i/3}} + X_1^{q_i^{n_i/3}}\gamma_i^{q_i^{n_i/3}} + X_2^{q_i^{n_i/3}}\gamma_i^{2\cdot q_i^{n_i/3}} = X_0 + X_1\gamma_i^{q_i^{n_i/3}} + X_2\gamma_i^{2\cdot q_i^{n_i/3}}.$$

Так как $q_i^{n_i/3} - 1$ делится на $q_i - 1$, а значит, кратно n_i, то

$$\gamma_i^{q_i^{n_i/3}} = \gamma_i(\alpha_i)^{(q_i^{n_i/3}-1)/n_i} = a_i\gamma_i, \gamma_i^{2\cdot q_{i-1}^3} = \gamma_i^2(\alpha_i)^{2(q_{i-1}^3-1)/9} = b_i\gamma_i^2, a_i, b_i \in GF(q_i),$$

поэтому $x^{q_i^{n_i/3}} = X_0 + X_1\gamma_i^{q_i^{n_i/3}} + X_2\gamma_i^{2\cdot q_i^{n_i/3}} = X_0 + X_1 a_i\gamma_i + X_2 b_i\gamma_i$, значит, возведение в степень $q_i^{n_i/3}$ в поле $GF(q_{i+1})$ сводится к двум умножениям в подполе $GF(q_i^{n_i/3})$ на элементы подполя $GF(q_i)$. Следовательно, его сложность оценивается как $(2n_i/3)M(GF(q_i))$. Точно так же оценивается сложность возведения в степень $q_i^{2n_i/3}$. Поэтому суммарная сложность всех выполненных операций равна

$$L_i = 2M(GF(q_{i+1})) + 3M(GF(q_i^{n_i/3})) + (4n_i/3)M(GF(q_i)) \leqslant$$

$$\leqslant (36a_ib_i + O(a_i))M(GF(q_i)).$$

Для вычисления

$$yy^{q_i}\dots y^{q_i^{n_i/3-1}},$$

где $y \in GF(q_i^{n_i/3})$, применяем тот же прием, вычисляя сначала

$$z = yy^{q_i^{n_i/9}}y^{q_i^{2n_i/9}}.$$

Так как $y^{q_i^{n_i/3}} = y$, то $z^{q_i^{n_i/9}} = z$, значит, $z \in GF(q_i^{n_i/9})$. Для вычисления z нужно выполнить два умножения в поле $GF(q_i^{n_i/3})$ и возведение в степени $q_i^{n_i/9}, q_i^{2n_i/9}$ в том же поле. Аналогично предыдущим рассуждениям, оцениваем их сложность как

$$2M(GF(q_i^{n_i/3})) + (4n_i/9)M(GF(q_i)) \leqslant (24a_{i-1}b_i + O(a_{i-1}))M(GF(q_i)).$$

Поскольку

$$yy^{q_i}\dots y^{q_i^{n_i/3-1}} = zz^{q_i}\dots z^{q_i^{n_i/9-1}},$$

то остается вычислить

$$zz^{q_i}\dots z^{q_i^{n_i/9-1}}, z \in GF(q_i^{n_i/9}).$$

Применяя тот же прием, сводим это вычисление со сложностью

$$2M(GF(q_i^{n_i/9})) + (4n_i/27)M(GF(q_i)) \leqslant (24a_{i-2}b_i + O(a_{i-2}))M(GF(q_i))$$

к вычислению

$$ww^{q_i}\dots w^{q_i^{n_i/27-1}}, w \in GF(q_i^{n_i/27})$$

и т.д. Так как $n_i = 3^{b_i}$, этот процесс закончится через b_i шагов. На каждом шаге требуемая сложность уменьшается асимптотически в три раза, поэтому сложность вычисления $N(x)$ оценивается как

$$\left(24\frac{3}{2}a_{i-1}b_i + O(a_i)\right)M(GF(q_i)),$$

значит, сложность вычисления $N(x), K(x)$ оценивается как

$$(44a_ib_i + O(a_i))M(GF(q_i)).$$

Отсюда следует рекуррентная оценка сложности инвертирования:

$$I(a_{i+1}) \leqslant I(a_i) + n_iM(GF(q_i)) + (44a_ib_i + O(a_i))M(GF(q_i)) \leqslant$$

$$\leqslant I(a_i) + (44a_ib_i + O(a_i))M(GF(q_i)).$$

Из нее по индукции получаем, что

$$I(a_n) \leqslant \sum_{i=1}^{n-1}(44a_ib_i + O(a_i))M(GF(q_i)) + I(a_0) =$$

$$= (44a_{n-1}b_{n-1} + O(a_{n-1}))M(GF(q_{n-1})).$$

Поскольку $M(GF(q_{i+1})) \leqslant (12a_ib_i + O(a_i))M(GF(q_i))$, то предполагая, что

$$M(GF(q_{i+1})) = (12a_ib_i + O(a_i))M(GF(q_i)),$$

получаем асимптотическую оценку:

$$I(a_n) \leqslant \left(\frac{11}{3} + o(1)\right) M(GF(q_n)).$$

Замечая, что $M(GF(q_n)) = O\left(3^{2^n+n}2^{(n^2+5n)/2}\right)$, во всех случаях имеем

$$I(a_n) = (44a_{n-1}b_{n-1} + O(a_{n-1}))M(GF(q_{n-1})) = O\left(3^{2^n+n}2^{(n^2+5n)/2}\right).$$

Поэтому при $N = a_n$ справедливо равенство $I(N) = O(M(GF(2^N)))$. Такие же оценки можно получить и для любого $N = 2 \cdot 3^n$. Для этого выберем k так, чтобы $2^{k-1} \leqslant n < 2^k$ и определим последовательность $a_k = N, a_{i-1} = 2 \cdot 3^{\lceil \log_3(a_i/2))/2 \rceil}$, положим $q_i = 2^{a_i}$ и рассмотрим башню полей $GF(q_0) \subset GF(q_1) \subset \ldots \subset GF(q_k)$. *Теорема доказана.*

Для практического построения схем для умножения и инвертирования в полях $GF(2^n)$ произвольной размерности можно разложить n на множители, равные степеням простых чисел, построить эти схемы для полей, размерности которых равны указанным множителям, сводя их построение к построению схем для полей простой размерности, а потом применить метод построения схем для полей составной размерности при условии взаимной простоты сомножителей. Для инвертирования в полях простой размерности применяется метод [7]. Вместо простых чисел, при возможности, можно применять размерности, для которых существуют оптимальные нормальные базисы, или гауссовы базисы малой сложности (см., например, [9]).

4. Вывод

Для любого $\varepsilon > 0$ при любом m, $n = m^s$ и $s \geqslant s_\varepsilon$ можно выбрать в поле $GF(2^n)$ базис, для которого схемная сложность умножения меньше $n^{1+\varepsilon/2}$, а сложность инвертирования меньше $n^{1+\varepsilon}$. При $n = 2 \cdot 3^k$ для некоторого базиса можно получить для умножения оценки сложности $n(\log_3 n)^{(\log_2 \log_3 n)/2+O(1)}$ и по порядку такие же оценки можно получить для инвертирования.

Литература

1. *Gathen J. von zur, Gerhard J.* Modern computer algebra. — Cambridge University Press, 1999.
2. *Schonhage A.* Schnelle Multiplication von Polynomen über Körpern der Charakteristik 2 // Acta Informatica. — 1977. — V. 7. — P. 395–398.
3. *Schonhage A.* Schnelle berechnung von kettenbruchentwicklungen // Acta Informatica 1. — 1971. — P. 139–144.
4. *Gao S., Gathen J. von zur, Panario D., Shoup V.* Algorithm for exponentiation in finite field // J. of Symbolic Computation. — 2000. — V. 29. — P. 879–889.
5. *Штрассен Ф.* Алгоритм Гаусса не оптимален // Кибернетический сборник. — Вып. 7. — М.: Мир, 1971.
6. *Болотов А.А., Гашков С.Б.* О быстром умножении в нормальных базисах конечных полей // Дискретная математика. — 2001. — Т. 13, № 3. — С. 3–31.

7. *Itoh T., Tsujii S.* A fast algorithm for computing multiplicative inverses in $GF(2^n)$ using normal bases // Inform. And Comp. — 1988. — V. 78. — P. 171–177.

8. *Кнут Д.* Искусство программирования. Т. 2. — 2-е изд. — М.: Вильямс, 2000.

9. *Gathen J. von zur, Nöcker M.* Fast arithmetic with general Gauss periods // Theor. Comp. Sci. — 2004. — V. 315. — P. 419–452.

10. *Paar C., Fan J.L.* Efficient inversion in tower fields of characteristic two. — ISIT, Ulm, Germany, 1997.

11. *Гашков С.Б.* Замечания о быстром умножении многочленов, преобразовании Фурье и Хартли // Дискретная математика. — 2000. — Т. 12, № 3. — С. 124–153.

12. *Лидл Р., Нидеррейтер Х.* Конечные поля. — М.: Мир, 1988.

Поступила в редакцию 19.02.2012.