МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М. В. ЛОМОНОСОВА

МЕХАНИКО–МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи
УДК 519.7

Сергеев Игорь Сергеевич

О РЕАЛИЗАЦИИ НЕКОТОРЫХ ОПЕРАЦИЙ В КОНЕЧНЫХ ПОЛЯХ СХЕМАМИ ЛОГАРИФМИЧЕСКОЙ ГЛУБИНЫ

01.01.09 — дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание учёной степени
кандидата физико-математических наук

МОСКВА — 2007

Работа выполнена на кафедре дискретной математики Механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, профессор С. Б. Гашков.
Официальные оппоненты:	доктор физико-математических наук, профессор В. Б. Алексеев;
	кандидат физико-математических наук, доцент А. Е. Жуков.
Ведущая организация:	Московский педагогический государственный университет

Защита диссертации состоится 12 октября 2007 г. в 16 ч. 15 мин. на заседании диссертационного совета Д.501.001.84 в Московском государственном университете имени М. В. Ломоносова по адресу: 119991, Российская Федерация, Москва, ГСП-1, Ленинские горы, МГУ имени М. В. Ломоносова, Механико-математический факультет, ауд. 1408.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 12 сентября 2007 г.

Учёный секретарь
диссертационного совета
Д.501.001.84 в МГУ
доктор физико-математических наук,
профессор В. Н. Чубариков

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Теория конечных полей была построена в работах Ферма, Эйлера, Лежандра, Гаусса, Галуа, Диксона и других выдающих ученых, и до последней четверти 20-го века развивалась как область чистой математики, но в связи с потребностями кодирования и криптографии в настоящее время активно развиваются прикладные аспекты теории. Вопросам эффективной реализации арифметики в конечных полях посвящено много работ и несколько специальных книг, в основном зарубежных авторов.

Особенность вычислений в конечном поле состоит в необходимости выбора представления элементов — от него существенно зависит способ реализации (и, как следствие, сложность и глубина логической схемы). Потенциально возможны (и описаны в теоретических работах) разные представления, но практически используются в основном два, а именно представления в стандартных и нормальных базисах, а также производные от них.

Наиболее широко используемым является представление в стандартном базисе — элементы поля в нем представляются многочленами, арифметические операции с которыми выполняются по модулю неприводимого многочлена, определяющего этот базис.

Умножение многочленов выполняется аналогами числовых методов, наиболее известные из которых были разработаны А. А. Карацубой[1], А. Л. Тоомом[2], А. Шёнхаге и Ф. Штрассеном[3, 4] в 60–70-е годы. На последнем методе достигаются одновременно наилучшие по порядку известные оценки схемной глубины $O(\log n)$ и сложности $O(n \log n \log\log n)$, где n — разрядность сомножителей (или их степень, в случае если это многочлены).

Иначе дело обстоит с делением (или инвертированием, т.к. деление сводится к инвертированию и умножению). Асимптотически быстрые ал-

[1] Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. // Доклады АН СССР. — 1962. — Т. 145(2). — С. 293–294.

[2] Тоом А. Л. О сложности схемы из функциональных элементов, реализующей умножение целых чисел. // Доклады АН СССР. — 1963. — Т. 150(3). — С. 496–498.

[3] Schönhage A., Strassen V. Schnelle multiplikation großer zahlen. // Computing. — 1971. — V. 7. — P. 271–282. [Русский перевод: Шёнхаге А., Штрассен Ф. Быстрое умножение больших чисел. // Кибернетический сборник. Вып. 10. М.: Мир, 1973. С. 87–98.]

[4] Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2. // Acta Inf. — 1977. — V. 7. — P. 395–398.

горитмы деления чисел основаны на методе С. Кука[5] и имеют такую же по порядку сложность, как и умножение. Однако логарифмический порядок схемной глубины на этих методах не достигается — наилучшая известная оценка глубины $O(\log n \log\log n)$ для таких схем получена Дж. Рейфом и С. Тейтом[6]. Для сложности схем с глубиной $O(\log n)$ известна оценка $O(n^{1+\epsilon})$, полученная Й. Хаастадом и Т. Лейтоном[7].

Упомянутые методы деления переносятся на степенные ряды, но не приложимы прямо к делению в конечном поле. Один из способов деления (инвертирования) в конечном поле состоит в применении расширенного алгоритма Евклида — наилучшая известная для него оценка сложности $O(n \log^2 n \log\log n)$ достигается в методе, предложенном для чисел А. Шёнхаге[8], а для многочленов Ф. Штрассеном[9]. Для глубины соответствующих схем можно указать оценку $O(n)$. Схема сложности $O(n^w \log n)$, где $w < 1,667$ — экспонента умножения матриц размера $\sqrt{n} \times \sqrt{n}$ и $\sqrt{n} \times n$, может быть построена методом, основанным на использовании аддитивных цепочек А. Брауэра[10]. Глубина этой схемы оценивается как $O(\log^2 n)$.

Схемы логарифмической глубины (и полиномиальной сложности) для инвертирования в конечном поле впервые были построены Б. Литоу и Дж. Давида[11], а также Х. фон цур Гатеном[12] в конце 80-х годов. Сложность этих схем оценивалась авторами как $n^{O(1)}$, а глубина — как $O(\log n)$. Анализ показывает, что для сложности и глубины предложенных схем нельзя привести лучшие оценки, чем $O(n^5)$ и $15 \log_2 n$ соответственно. Улучшение этого результата являлось стимулом для настоящей работы.

В представлении конечного поля с помощью нормальных базисов можно быстро выполнять возведение в степени определенного вида, од-

[5]Cook S. On the minimum computation time of functions. Ph. D. Thesis. Harvard Univ., 1966.

[6]Reif J., Tate S. Optimal size integer division circuits. // SIAM J. Comput. — 1990. — V. 19, №5. — P. 912–925.

[7]Hastad J., Leighton T. Division in $O(\log n)$ depth using $O(n^{1+\epsilon})$ processors. 1986. *http://www.nada.kth.se/~yohanh/paraldivision.ps.*

[8]Schönhage A. Schnelle berechnung von kettenbruchentwicklungen. // Acta Inf. — 1971. — V. 1. — P. 139–144.

[9]Strassen V. The computational complexity of continued fractions. // SIAM J. Comput. — 1983. — V. 12, №1. —P.1–27.

[10]Brauer A. On addition chains. // Bull. AMS. — 1939. — V. 45. — P. 736–739.

[11]Litow B., Davida G. $O(\log n)$ parallel time finite field inversion. // Proc. Aegean Workshop on Computing. Lecture Notes in Comp. Sci. — 1988. — V. 319. — P. 74–80.

[12]von zur Gathen J. Inversion in finite fields using logarithmic depth. // J. Symb. Comput. — 1990. — V. 9. — P. 175–183.

нако другие операции (в частности, умножение) выполняются существенно сложнее, чем в стандартных базисах (речь идет об общем случае, поскольку на практике используются конкретные базисы, в которых необходимые операции реализуются эффективно). В самое последнее время ряд исследователей (Э. Калтофен, В. Шауп[13], А. А. Болотов, С. Б. Гашков[14] и др.) высказали идею о том, что для ускорения реализации многих операций в нормальном представлении, и возможно некоторых операций в стандартном представлении, целесообразно (как с практической точки зрения, так и для получения теоретических оценок) использовать быстрые переходы между нормальными и стандартными базисами. Оценки вида $O(n^\alpha)$, $\alpha < 2$, для сложности перехода в общем случае, по-видимому, до сих пор не были известны. Получение таких оценок также являлось стимулом для данной работы.

Цель работы

Целью работы является разработка конструктивных методов и получение новых верхних оценок сложности реализации некоторых арифметических операций (инвертирования, умножения, координатных преобразований и т.д.) в конечных полях схемами логарифмической глубины из функциональных элементов.

Методы исследования

В работе используются методы теории синтеза управляющих систем, теории конечных полей и теории чисел.

Научная новизна

Основные результаты диссертации являются новыми и заключаются в следующем:

1. Получена новая верхняя оценка сложности инвертирования в стандартном базисе конечного поля при реализации схемами логарифмической глубины из функциональных элементов.

[13]Kaltofen E., Shoup V. Subquadratic-time factoring of polynomials over finite fields. // Math. Comput. — 1998. — V. 67, №223. — P. 1179–1197.

[14]Болотов А. А., Гашков С. Б. О быстром умножении в нормальных базисах конечных полей. // Дискретная математика. — 2001. — Вып. 13, №3. — С. 3–31.

2. Получена новая верхняя оценка схемной глубины инвертирования в конечном поле характеристики два.

3. Получены новые верхние оценки сложности перехода между стандартными и нормальными базисами конечных полей в общем случае, в том числе, для реализации схемами логарифмической глубины.

Как следствие, получены новые верхние оценки сложности умножения в нормальном базисе, проверки базисности нормальной системы в стандартном базисе и некоторых других операций в конечных полях.

Теоретическая и практическая ценность

Работа носит теоретический характер. Результаты работы могут найти применение в прикладных разработках по теории кодирования и компьютерной алгебре.

Апробация результатов

Результаты диссертации докладывались на семинаре «Синтез управляющих систем» под руководством академика РАН О.Б. Лупанова в 2005 г., на семинаре «Многозначная логика и ее приложения» под руководством С.Б. Гашкова и А.Б. Угольникова в 2005 г., на научном семинаре отдела теоретической кибернетики Института прикладной математики имени М.В. Келдыша РАН в 2006 г., на XIV Международной конференции «Проблемы теоретической кибернетики» (Пенза, 23–28 мая 2005 г.), на XVI Международной школе-семинаре «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.), на Ломоносовских чтениях в 2006 г. в МГУ.

Публикации

Основные результаты диссертации опубликованы в трех работах автора, перечисленных в конце автореферата [1–3].

Структура и объем работы

Диссертация состоит из пяти глав, разбитых на параграфы (первая глава является вводной). Текст диссертации изложен на 96 страницах. Список литературы включает 93 наименования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во вводной **главе 1** приводится постановка задачи, краткая историческая справка о предшествующих работах в данной области и формулируются основные результаты диссертации.

В **главе 2** даются основные определения и сведения вспомогательного характера.

Полем называется кольцо с единицей, ненулевые элементы которого образуют абелеву группу относительно операции умножения. Эта группа называется мультипликативной группой поля. *Конечным полем* называется поле, содержащее конечное число элементов — это число называется *порядком* поля. Порядок конечного поля может быть только степенью простого числа (которое является характеристикой поля), и при этом все поля одного порядка изоморфны. Мультипликативная группа конечного поля — циклическая. Единственное с точностью до изоморфизма конечное поле порядка q обозначается $GF(q)$.

Конечное поле $GF(q^n)$ можно рассматривать как расширение поля $GF(q)$ (или векторное пространство над $GF(q)$) степени n — все элементы $GF(q^n)$ порождаются линейными комбинациями над $GF(q)$ базисных элементов. С различным выбором базиса связаны различные представления элементов поля (под представлением понимается способ кодирования).

При реализации операций в конечном поле $GF(q^n)$ используется два основных представления: *стандартное* (или *полиномиальное*), в котором элементы поля рассматриваются как многочлены степени не выше $n-1$, а операции производятся по модулю некоторого неприводимого над $GF(q)$ многочлена $m_n(t)$ степени n, и *нормальное*, когда элементы поля рассматриваются как линейные комбинации над $GF(q)$ с базисными элементами

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

где α — порождающий элемент (или *генератор*) базиса. В обоих случаях элементы поля кодируются набором коэффициентов в разложении по соответствующему базису.

В качестве модели для реализации операций в конечном поле $GF(q^n)$ рассматриваются *схемы над* $GF(q)$, которые определяются аналогично схемам из функциональных элементов, т.е. как ориентированные графы без ориентированных циклов с вершинами-входами, которым приписаны символы переменных или константы, и функциональными элементами в других вершинах; некоторые вершины являются выходами. Входы и выходы элементов схемы принимают значения в $GF(q)$, а сами функци-

ональные элементы реализуют функции над $GF(q)$. Понятие схемы над $GF(2)$ тождественно понятию булевой схемы.

В качестве основного схемного базиса выбирается (функционально полный) базис бинарных арифметических операций: сложения, вычитания, умножения и деления, а также констант. Дополнительно при простом q используется функция минимума или максимума двух элементов поля (как чисел от 0 до $q-1$), а в общем случае — бинарные арифметические операции в $\mathbb{Z}_q$ (при наличии соответствия между элементами $GF(q)$ и $\mathbb{Z}_q$ можно считать, что соответствующие элементы реализуют некоторые функции над $GF(q)$).

Как обычно, сложность и глубина схемы S обозначаются через $L(S)$ и $D(S)$ соответственно.

В **главе 3** рассматриваются различные подходы к построению схем m-кратного умножения по модулю многочлена степени n над конечным полем с глубиной $O(\log(mn))$. Целью является минимизация порядка сложности таких схем относительно n. Основной результат главы формулируется следующим образом.

Теорема 3.4 *Пусть $j, l, r \in \mathbb{N}$, $j \le \lceil \log_2 \log_2 m \rceil$. Тогда m-кратное умножение многочленов над $GF(q)$ по модулю многочлена степени n выполняется схемой $M_{m,n}$ сложности и глубины*

$$L(M_{m,n}) = O\left(la^j m^{1+\frac{1}{r}\left(3-\frac{1}{2^j}+\frac{2,5}{l2^j}\right)} n^{1+\frac{1}{l4^j}} \left(2^{-j}\log(mn)\log\log(mn) + l^2\right)\right),$$

$$D(M_{m,n}) = O\left((l+j)\log m + r(1+l/2^j)\log n\right),$$

где $a = 81$, если q четно, и $a = 8$, иначе.

Оценки теоремы 3.4 используются при выводе основных результатов о схемной реализации инвертирования.

В **главе 4** изучается вопрос о построении схем для инвертирования в конечном поле $GF(q^n)$ с глубиной $O(\log n)$.

В конечном поле $GF(q^n)$ инвертирование эквивалентно возведению в степень $q^n - 2$. Методом аддитивных цепочек строится схема сложности $O(n^w \log n)$ и глубины $O(\log^2 n)$, где $w < 1,667$ — экспонента умножения матриц размера $\sqrt{n} \times \sqrt{n}$ и $\sqrt{n} \times n$. Такая схема состоит из $O(\log n)$ подсхем, реализующих умножения и операции Фробениуса (возведения в степень вида q^k) в поле $GF(q^n)$. В предложенном параллельном алгоритме инвертирования также используются многократные умножения. Доказана

Теорема 4.3 *Пусть $r \in \mathbb{N}$. Тогда инвертирование в стандартном базисе поля $GF(q^n)$ реализуется схемой I_n сложности и глубины*

$$L(I_n) = O(rn^{1/r}(n^w + n^{1,5}\log n \log\log n)), \qquad D(I_n) = O(r\log n).$$

Из теоремы 4.3 вытекает, что можно построить схему для инвертирования сложности $O(n^{1,667})$ и глубины $O(\log n)$. В частном случае $r \sim \log n$ получаются оценки из метода аддитивных цепочек.

Для стандартного базиса, допускающего сравнительно несложный переход к нормальному базису и обратно (под переходом подразумевается соответствующее преобразование координат), т. е. имеющего низкую транзитивную сложность, оценка теоремы 4.3 может быть улучшена.

Теорема 4.4 *Пусть $R \in \mathbb{N}$, $R = o(\log n / \log\log n)$. Пусть схемы T' и T'' реализуют соответственно прямой и обратный переходы между нормальным и стандартным базисами поля $GF(q^n)$. Тогда для инвертирования в любом из указанных базисов можно построить схему I_n сложности и глубины*

$$L(I_n) = O(R^b n^{1+2/R}) + O(R\sqrt[R]{n})(L(T') + L(T'));$$

$$D(I_n) = O(R(\log n + D(T') + D(T''))),$$

где $b = (4/3)\log_2 3$, если q четно, и $b = 1$, если q нечетно.

Из теоремы 4.4 следует, что в базисах с почти линейной транзитивной сложностью инвертирование также выполняется с почти линейной сложностью. При этом, если соответствующие переходы между базисами выполняются с глубиной $O(\log n)$, то строящаяся схема инвертирования также имеет глубину $O(\log n)$. В качестве примера можно рассмотреть гауссовы нормальные базисы (ГНБ).

ГНБ k-го типа существует в поле $GF(q^n)$, если число $kn + 1$ — простое, и порождается элементом

$$\alpha = \zeta + \zeta^{\gamma} + \ldots + \zeta^{\gamma^{k-1}},$$

где ζ — примитивный корень степени $kn + 1$ в поле $GF(q^{kn})$, а γ — примитивный корень степени k в поле вычетов $\mathbb{Z}_{kn+1}$, который вместе с q порождает всю мультипликативную группу $\mathbb{Z}_{kn+1} \setminus \{0\}$.

Утверждение 4.2 *Пусть $k = o(\log n)$ и $\epsilon > 0$, $\epsilon = \Omega(\log\log n / \log n)$. Тогда можно построить схему инвертирования в ГНБ k-го типа поля $GF(q^n)$ сложности $O(\epsilon^{-b} n^{1+\epsilon})$ и глубины $O(\epsilon^{-1}\log n)$, где b — из теоремы* 4.4.

Далее в работе выясняется вопрос о минимизации глубины схемы инвертирования в полях характеристики два. Показано, что инвертирование в произвольном базисе поля $GF(2^n)$ можно реализовать схемой глубины асимптотически $(3 + \sigma)\log_2 n$, где σ — константа глубины многократного сложения, которая определяется как наименьшее число, такое, что существует схема сложения n одноразрядных чисел, имеющая

глубину $(\sigma + o(1))\log_2 n$ (известно, что $\sigma < 3,44$). Сложность построенной схемы инвертирования равна $O(n^4)$. Данный результат вытекает из следующей теоремы о сложности и глубине реализации возведения в произвольную степень в конечном поле.

Теорема 4.5 *Пусть m — количество ненулевых разрядов в двоичной записи числа E. Тогда можно построить схему $E_{m,n}$, реализующую операцию возведения в степень E в поле $GF(2^n)$, со сложностью и глубиной (при $\epsilon > 0$)*

$$L(E_{n,m}) \le (1 + o(1))\frac{\log_2(mn) + C_0(\epsilon)}{\log_2(m^2 n)} \cdot m^2 n^2 + C_1(\epsilon) m^{2+\epsilon} n^{1+\epsilon};$$

$$D(E_{n,m}) \le (2 + \epsilon)\log_2 n + 4,44 \log_2 m + O(\log^2 \log n) + C_2(\epsilon),$$

где C_i — некоторые ограниченные на любом отрезке интервала $(0, 1]$ функции.

В **главе 5** описывается построение схем для реализации переходов между нормальными и стандартными базисами и рассматриваются некоторые приложения.

Основным результатом главы является следующая

Теорема 5.2 *Переход между двумя любыми нормальными или стандартными базисами поля $GF(q^n)$ может быть выполнен схемой сложности $O(n^\nu)$ и глубины $O(\log n)$, где*

$$\nu > \min_{\sigma \in [0,\,1]} \max\{\omega(\sigma, 1-\sigma, 1),\ \omega((1+\sigma)/2, (1+\sigma)/2, 1)\},$$

а $\omega(\alpha, \beta, \gamma)$ — экспонента умножения матриц размера $n^\alpha \times n^\beta$ и $n^\beta \times n^\gamma$.

Из данной теоремы следует (при подстановке известных оценок для матричных экспонент), что для сложности построенных схем справедлива оценка $O(n^{1,806})$. Как следствие, умножение или инвертирование в произвольном нормальном базисе поля $GF(q^n)$ может быть реализовано схемой сложности $O(n^{1,806})$ и глубины $O(\log n)$. Это примеры операций, которые выполняются асимптотически быстрее посредством перехода к стандартному базису, чем специально разработанными для нормальных базисов алгоритмами.

В качестве примера операции в стандартном базисе, которая может быть выполнена быстрее за счет перехода к нормальному представлению, приводится тест на базисность нормальной системы, т. е. задача проверки, порождает ли заданный элемент β нормальный базис в поле $GF(q^n)$, иначе говоря, является ли нормальная система $\{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}$ линейно независимой над $GF(q)$. Показано, что эта операция также реализуется схемой сложности $O(n^{1,806})$ и глубины $O(\log n)$.

При дополнительных ограничениях оценки сложности теоремы 5.2 можно улучшить. Например, нормальные базисы, в которых быстро выполняется умножение стандартным алгоритмом (Месси—Омура), допускают быстрый переход к стандартным базисам и обратно.

Стандартный метод умножения в нормальном базисе B поля $GF(q^n)$ имеет сложность $O(C_B n)$, где C_B — сложность базиса B — понятие, вытекающее из структуры этого алгоритма. *Сложность нормального базиса* с генератором α определяется как суммарное количество ненулевых коэффициентов в разложении элементов

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

в этом базисе. Для любого базиса B выполнено $2n-1 \le C_B < n^2$. Справедлива

Теорема 5.3 *Переход от стандартного базиса к нормальному базису B в поле $GF(q^n)$ может быть реализован схемой сложности $O(\sqrt{n}C_B) + O(n^{1,667})$, а обратный переход можно выполнить схемой сложности $O(n^{1,667}) + O(n^{1,5}\log q \log n \log\log n)$.*

Метод умножения в нормальных базисах, вытекающий из теоремы 5.3, предназначен для полей с малым основанием q.

В заключение автор выражает глубокую благодарность научному руководителю С. Б. Гашкову за постановку задач, а также коллективам кафедры дискретной математики механико-математического факультета Московского государственного университета имени М. В. Ломоносова и отдела теоретической кибернетики Института прикладной математики имени М. В. Келдыша РАН за всесторонние помощь и поддержку.

Публикации автора по теме диссертации

1. Сергеев И. С. Об инвертировании в конечных полях характеристики 2 с логарифмической глубиной. // Вестник МГУ. Серия 1. Математика. Механика. — 2007. — №1. — С. 28–33.

2. Сергеев И. С. О схемах логарифмической глубины для инвертирования в конечных полях характеристики два. // Математические вопросы кибернетики. Вып. 15. — М.: Физматлит, 2006. — С. 35–64.

3. Сергеев И. С. О реализации некоторых операций конечных полей характеристики 2 схемами логарифмической глубины. // Материалы XVI Международной школы-семинара «Синтез и сложность управляющих систем» (Санкт-Петербург, 26–30 июня 2006 г.). — М.: Изд-во мех.-матем. факультета МГУ, 2006. — С. 101–103.