На правах рукописи

Маевский Алексей Эдуардович

АЛГОРИТМЫ СПИСОЧНОГО ДЕКОДИРОВАНИЯ СПЕЦИАЛЬНОГО КЛАССА АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДОВ

Специальность 01.01.09 – дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата физико-математических наук

Ярославль – 2011

Работа выполнена на кафедре алгебры и дискретной математики факультета математики, механики и компьютерных наук Южного федерального университета

Научный руководитель:	кандидат физико-математических наук, доцент Деундяк Владимир Михайлович
Официальные оппоненты:	доктор физико-математических наук Кабатянский Григорий Анатольевич
	кандидат физико-математических наук, доцент Стукопин Владимир Алексеевич
Ведущая организация:	Институт систем информатики им. А.П.Ершова Сибирского отделения РАН

Защита диссертации состоится 25 февраля 2011 года в 14 ч. 00 мин. на заседании диссертационного совета Д.212.002.03 при Ярославском государственном университете им. П.Г. Демидова по адресу: 150008, г. Ярославль, ул. Союзная, 144, аудитория 426.

С диссертацией можно ознакомиться в библиотеке Ярославского государственного университета им. П.Г. Демидова

Автореферат разослан ____ января 2011 г.

Ученый секретарь диссертационного совета С.И. Яблокова

Общая характеристика работы

Актуальность темы

Широко известно, что при передаче информации как по пространственным, так и по временным каналам связи могут возникать ошибки. В конце 40-х годов прошлого века К. Шеннон показал, что для защиты передаваемых данных от случайных искажений и помех экономически эффективнее применять помехоустойчивые коды, чем строить дорогостоящие каналы высокого качества. С тех пор активное развитие получила теория помехоустойчивого кодирования, в процессе которого найдены различные классы помехоустойчивых кодов и определены границы их применимости. Из всего многообразия линейных кодов широкое практическое применение нашли коды Рида-Соломона (РС-коды); традиционно РС-коды используются, например, для защиты данных на носителях информации[1], в системах спутниковой связи[2], в системах исследования дальнего космоса[3].

В 1997 г. М.Судан[4] построил первый полиномиальный алгоритм, решающий задачу списочного декодирования РС-кодов, сформулированную для произвольных кодов Элайесом[5] и Возенкрафтом[6] еще в середине 1950-х годов. Алгоритм Судана оказался эффективным только для РС-кодов, имеющих скорость до $1/3$, поэтому несколько позже Гурусвами и Судан[7] модифицировали алгоритм Судана, сняв ограничение на скорость РС-кодов. Благодаря алгоритмам Судана и Гурусвами-Судана РС-коды нашли применение при решении многих прикладных задач, изначально далеких от

[1] *Immink K.A.S.* Coding techniques for digital recoders. N.-Y.: Prentice-Hall, 1991.

[2] *Wu W.W., Haccoun D., Peile R.E., Hirata Y.* Coding for satellite communication. // IEEE Journal on Selected Areas in Communications, 1987. Vol. 5. P. 724-785.

[3] *McEliece R.J., Swanson L.* Reed-Solomon codes and the exploration of the solar system. // Reed-Solomon codes and their applications (Editors Wicker S.B., Bhargava V.K.). N.-Y.: IEEE Press, 1994.

[4] *Sudan M.* Decoding of Reed Solomon codes beyond the error-correction bound. // Journal of Complexity, 1997. Vol. 13, No. 1. P. 180-193.

[5] *Elias P.* List decoding for noisy channel. Technical Report no. 335, Research Laboratory of Electronics, MIT, 1957.

[6] *Wozencraft J.M.* List decoding. // Quaterly Progress Report, Research Laboratory of Electronics, MIT, 1958. Vol. 48. P. 90-95.

[7] *Guruswami V., Sudan M.* Improved decoding of Reed-Solomon and algebraic-geometry codes. // IEEE Transactions on Information Theory, 1999, September. Vol. 45, P. 1757-1767.

теории кодирования, таких как предотвращение несанкционированного копирования компакт-дисков[8] [9], самообучение систем и распознавание образов[10], построение односторонних функций для криптографических целей[11], криптоанализ некоторых блочных шифров[12]. Отметим, что с каждым годом круг прикладных задач, решаемых с помощью списочного декодирования, интенсивно расширяется, вследствие чего возрастает и актуальность задачи улучшения характеристик существующих и построения новых алгоритмов списочного декодирования как РС-кодов, так и других помехоустойчивых кодов.

В 1981 г. В.Д.Гоппа, используя методы алгебраической геометрии, описал новый широкий класс помехоустойчивых кодов – алгебро-геометрические коды[13] (АГ-коды). Его работа завершила многолетние исследования в области построения наиболее общего класса кодов, включающего в себя классы РС-кодов, циклических кодов и некоторых других используемых на практике кодов. Для построения АГ-кодов он предложил использовать пространства рациональных дифференциальных 1-форм на гладких проективных кривых, такой способ построения позже получил название Ω-конструкции. Несколько позже В.Д.Гоппа описал другой способ построения АГ-кодов[14], основанный на использовании пространств Римана-Роха на гладкой проективной кривой, получивший название L-конструкции. Впоследствии были обнаружены другие конструкции АГ-кодов с привлечением более сложных объектов алгебраической геометрии. М.А.Цфасман,

---

[8] *Silverberg A., Staddon J., Walker J.L.* Efficient traitor traicing algorithms using list decoding // Advances in Cryptology – ASIACRYPT 2001, LNCS 2248, N.-Y.:Springer, 2001. P. 175-192.

[9] *Barg A., Kabatiansky G.A.* Class of i.p.p codes with effective tracing algorithm // Journal of Complexity, 2004. Vol. 20, No 2-3, P.137-147.

[10] *Ar S., Lipton R.J., Rubinfeld R., Sudan M.* Reconstructing algebraic functions from mixed data. // SIAM Journal of Computation, 1999. Vol. 28. No. 2. P. 488-511.

[11] *Sudan M.* List decoding: Algorithms and applications. // SIGACT News, 2000. Vol. 31, P. 16-27.

[12] *Jakobsen T.* Cryptoanalysis of block ciphers with probabilistic non-linear relation of low degree. // Proceedings of Advances in Cryptography – Crypto'98 (Editor Krawczyk H.). Lecture Notes in Computer Sciences No.1462, N.-Y.:Springer, 1998.

[13] *Гоппа В.Д.* Коды на алгебраических кривых. // Доклады АН СССР. 1981. Т. 259. № 6. С. 1289-1290.

[14] *Гоппа В.Д.* Алгебраико-геометрические коды. // Известия АН СССР, Серия математическая. 1982. Т. 46. № 4. С. 762-781.

С.Г.Влэдуц и Т.Цинк показали[15], что существуют АГ-коды, построенные с помощью весьма специальных кривых, значение минимального расстояния которых гарантированно превышает нижнюю границу Варшамова-Гилберта, существенно продвинувшись, таким образом, к решению одной из центральных в теории кодирования задач построения семейства кодов с асимптотически хорошими параметрами (кодов, у которых при стремлении параметров n, k, d к бесконечности отношения k/n и d/n одновременно отличны от нуля). Отметим, что практически все известные семейства кодов, отличные от алгебро-геометрических, либо асимптотически плохи, либо имеют параметры, лежащие на границе Гилберта-Варшамова, поэтому класс АГ-кодов представляет не только теоретический интерес, но и важен для практических приложений[16]. В связи с этим Шокройахи и Вассерман[17], используя идеи алгоритма Судана, построили алгоритм списочного декодирования некоторых подклассов АГ-кодов, эффективный только для кодов с низкими скоростями, а Гурусвами и Судан[18] его модифицировали, сняв ограничение на скорость кода. Однако высокая сложность математического аппарата и объектов теории алгебраических кривых, используемых при построении АГ-кодов и алгоритмов декодирования, затрудняет их применение к решению теоретических или практических задач.

В 1988 г. Юстесен и др.[19] упростили L-конструкцию Гоппы, используя вместо пространства Римана-Роха пространство всех однородных многочленов фиксированной полной степени из однородного координатного кольца гладкой плоской проективной кривой, построив при этом новый подкласс АГ-кодов, содержащий, в частности, РС-коды. Этот подкласс АГ-

[15] *Tsfasman M.A., Vlăduţ S.G., Zink T.* Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound // Mathematical Nachrichten, 1982. Vol. 109. P. 21-28.

[16] *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003. 504 с. С.88

[17] *Shokrollahi M., Wasserman H.* List decoding of algebraic-geometric codes. // IEEE Transactions on Information Theory, 1999. Vol. 45. P. 432-437.

[18] *Guruswami V., Sudan M.* Improved decoding of Reed-Solomon and algebraic-geometry codes. // IEEE Transactions on Information Theory, 1999, September. Vol. 45, P. 1757-1767.

[19] *Justesen J., Larsen K.J., Jensen H.E., Havemose A., Høholdt T.* Construction and decoding of a class of algebraic geometry codes. // IEEE Transactions on Information Theory, 1989. Vol. 35. N. 4. P. 811-821.

кодов будем далее называть алгебро-геометрическими кодами типа кодов Рида-Соломона (АГРС-кодами). Благодаря тому, что АГРС-коды по своей конструкции гораздо ближе к РС-кодам, чем другие АГ-коды, в той же статье авторы на основе классического алгоритма Питерсона декодирования кодов Боуза-Чоудхури-Хоквингема построили без использования дополнительных математических конструкций алгебраической геометрии практически реализуемый полиномиальный алгоритм декодирования кодов, двойственных АГРС-кодам. Отметим, что существующие алгоритмы декодирования РС-кодов и АГ-кодов непосредственно не могут быть перенесены на класс АГРС-кодов в силу различия базовых математических объектов.

В силу своей конструкции АГРС-коды, как и АГ-коды, обладают следующими характеристиками:

– максимальная длина АГРС-кода над полем $\mathbb{F}_q$ ограничена сверху достижимым числом $N_1 = q+1+2g\lfloor\sqrt{q}\rfloor$, определяемому максимальным количеством $\mathbb{F}_q$-рациональных точек на кривой рода g, в то время как максимальная длина РС-кода над полем $\mathbb{F}_q$ равна $q+1$;

– длина n, размерность k и конструктивное расстояние d^* АГРС-кода удовлетворяют двойному неравенству:

$$n - k - g + 1 \leq d^* \leq n - k + 1,$$

поэтому если отношение g/n мало, параметры АГРС-кода лежат близко к границе Синглтона.

Вследствие этого можно ожидать, что при условии существования практически реализуемых эффективных алгоритмов декодирования АГРС-коды наравне с РС-кодами найдут широкое применение в разнообразных прикладных задачах.

В связи с изложенным значимой и актуальной представляется задача построения алгоритмов списочного декодирования и декодирования с ограниченным расстоянием произвольного АГРС-кода с сохранением при этом основной направленности конструкции класса АГРС-кодов на минимальное использование математического аппарата теории алгебраических кривых и алгебраической геометрии.

Необходимо отметить, что одним из важных этапов всех алгоритмов списочного декодирования РС-кодов и АГ-кодов, начиная с алгоритма Судана, является вычисление корней многочлена одной переменной с коэффициентами из кольца $\mathbb{F}_q[x]$ многочленов одной переменной над конечным полем в случае РС-кодов или вычисление корней многочлена одной переменной с коэффициентами из пространств Римана-Роха $L(D)$ на плоской проективной кривой над конечным полем в случае АГ-кодов. Задача факторизации многочленов одной или нескольких переменных с коэффициентами из различных алгебраических структур является классической в алгоритмической алгебре, существует множество общих подходов ее решения, например, методы Кронекера, Гензеля, Берлекэмпа, Цассенхауза. Однако использование общих подходов в алгоритмах списочного декодирования неэффективно в силу того, что факторизуемые многочлены могут иметь неприводимые делители высоких степеней, на вычисление или избавление от которых тратится значительная часть вычислительного времени. В силу этого для существующих алгоритмов списочного декодирования разработаны специальные алгоритмы вычисления корней многочленов, ориентированные на использование тонких свойств алгебраических структур, над которыми рассматриваются многочлены. Так, для алгоритмов списочного декодирования РС-кодов первый эффективный полиномиальный алгоритм разработали Рот и Рукенштейн[20]; Ву и Зигель[21] перенесли этот алгоритм на случай списочного декодирования АГ-кодов. Отметим также алгоритмы Ого и Пека[22], Гао и Шокройахи[23], существующие в двух вариантах

[20] *Roth R.M., Ruckenstein G.* Efficient decoding of Reed-Solomon codes beyond half the minimum distance. // IEEE Transactions on Information Theory, 2000. Vol. 46. P. 246-257.

[21] *Wu X.-W., Siegel P.H.* Efficient root-finding algorithm with application to list decoding of algebraic-geometric codes. // IEEE Transactions on Information Theory, 2001. Vol. 47. No.6. P. 2579-2587.

[22] *Augot D., Pecquet L.* A Hansel lifting to replace factorization in list-decoding of algebraic-geometry and Reed-Solomon codes. // IEEE Transactions on Information Theory, 2000. Vol. 46. No. 7. P. 2605-2614.

[23] *Gao S.-H., Shokrollahi M.* Computing roots of polynomials over function fields of curves. // Coding theory and cryptography: from Enigma and Geheimschreiber to quantum theory (Editor Joyner D.), N.Y.:

– для РС-кодов и для АГ-кодов. Тем не менее, все построенные алгоритмы в случае АГРС-кодов не применимы в силу специфичности структуры используемого в их конструкции однородного координатного кольца. В связи с этим представляется актуальным дальнейшее развитие теории и практики вычисления корней многочленов с коэффициентами из различных алгебраических структур, в частности, используемых в конструкциях помехоустойчивых кодов. Например, конструкция АГРС-кодов использует однородное координатное кольцо гладкой плоской проективной кривой над конечным полем, конструкция проективных кодов Рида-Маллера[24] использует кольцо многочленов нескольких переменных над конечным полем. Такие алгоритмы могут найти применение как в существующих, так и разрабатываемых алгоритмах декодирования.

Цель работы

Цель работы – разработка алгоритмов списочного декодирования и декодирования с ограниченным расстоянием произвольного АГРС-кода, а также разработка новых алгоритмов вычисления корней многочленов одной переменной с коэффициентами из однородного координатного кольца гладкой плоской проективной кривой и кольца многочленов нескольких переменных над произвольной областью целостности.

Основные методы исследования

В работе используются методы и результаты теории помехоустойчивого кодирования, в частности, подходы Берлекэмпа-Велча, Судана, Гурусвами-Судана к построению алгоритмов декодирования; алгоритмической алгебры, в частности, подходы Рота-Рукенштейн, Гао-Шокройахи к построению алгоритмов вычисления корней многочленов; линейной и общей алгебры; алгебраической геометрии и коммутативной алгебры в части, касающейся теории проективных алгебраических кривых над конечными полями; теории сложности алгоритмов.

Springer, 2000. P. 214-228.

[24] *Duursma I.M.* Algebraic geometry codes: general theory // Advances in algebraic geometry codes (editors E.Martinez-Moro, C.Munuera, D.Ruano), Singapore: World Scientific Publishing Co. Pte. Ltd., 2008. P. 1-48.

Основные результаты работы

Основные результаты работы, выносимые на защиту, состоят в следующем:

1. Построен полиномиальный алгоритм декодирования с ограниченным расстоянием произвольного АГРС-кода, полностью обоснована его корректность, вычислены максимальное количество исправляемых ошибок и асимптотические верхние границы временной и емкостной сложности в наихудшем случае.

2. Построены базовый и модифицированный полиномиальные алгоритмы списочного декодирования произвольного АГРС-кода. Для каждого алгоритма полностью обоснована корректность, вычислены оценки максимального значения радиуса сферы Хэмминга, внутри которой алгоритм способен вычислить все элементы выходного списка, а также оценки асимптотических верхних границ временной и емкостной сложности в наихудшем случае.

3. Для многочленов одной переменной с коэффициентами из однородного координатного кольца гладкой проективной кривой построены два алгоритма вычисления всех корней, принадлежащих заданной градуировочной компоненте: в случае многочлена первой степени – на основе метода неопределенных коэффициентов, в случае многочленов произвольной степени – на основе подхода Гао-Шокройахи. Для каждого алгоритма полностью обоснована корректность и вычислены асимптотические верхние границы временной и емкостной сложности в наихудшем случае.

4. Построен алгоритм вычисления корней многочленов одной переменной с коэффициентами из кольца многочленов нескольких переменных над произвольной областью целостности, полностью обоснована его корректность и вычислена асимптотическая верхняя граница его временной сложности в наихудшем случае.

Научная новизна

Все основные результаты работы являются новыми.

Теоретическая и практическая ценность

Работа носит теоретический характер. Результаты диссертации могут быть использованы специалистами, работающими в области теории и практики помехоустойчивого кодирования, криптографии, теории обучения, теории распознавания образов.

Апробация результатов

Основные результаты диссертации представлены в виде докладов на следующих конференциях: Международная школа-семинар по анализу и геометрии памяти Н.В. Ефимова (п.Абрау-Дюрсо, 2004 и 2006 гг.), Межрегиональная научно-практическая конференция "Теория и практика создания радиотехнических и мехатронных систем (теория, проектирование, экономика)" (Ростов-на-Дону, 2007 г.), Международная алгебраическая конференция, посвященная 100-летию со дня рождения Д.К.Фаддеева (СПб., 2007 г.), Международная научно-практическая конференция "Информационная безопасность" (Таганрог, 2008 и 2010 гг.), а также неоднократно обсуждались на семинаре "Математические методы в защите информации" кафедры алгебры и дискретной математики мехмата ЮФУ (руководитель – к.ф.-м.н., доцент Деундяк В.М.).

Публикации [25]

Основные результаты опубликованы в 11 работах [1–11].

В работе [3] автору принадлежит разработка структуры алгебро-геометрического кодека, в работе [11] автору принадлежит определение понятия поверхности помехоустойчивости, а также способы выбора параметров алгоритма списочного декодирования для решения задачи декодирования по максимуму правдоподобия.

[25]Работа поддержана ФЦП "Научные и научно-педагогические кадры инновационной России", Государственный контракт №02.740.11.0208 от 7 июля 2009 г.

Структура и объем диссертации

Диссертация состоит из введения, четырех глав, заключения и списка литературы, содержащего 72 наименования, включая работы автора. Полный объем диссертации составляет 141 страницу машинописного текста.

Краткое содержание работы

Во введении обоснована актуальность темы диссертационной работы, сформулирована цель и поставлены задачи проводимых исследований, определены научная новизна и значимость выполненных изысканий, приведены сведения о публикациях и апробации полученных результатов, структуре диссертации, раскрыто краткое содержание глав работы.

Первая глава содержит предварительные сведения из теории линейных помехоустойчивых кодов, теории градуированных колец, теории проективных алгебраических кривых. В частности, приводятся определения однородного координатного кольца $\mathbb{F}_q[\mathcal{P}_F]$ гладкой плоской проективной кривой $\mathcal{P}_F$ над конечным полем $\mathbb{F}_q$ как градуированного кольца $\bigoplus_{s\geq 0}(\mathbb{F}_q[\mathcal{P}_F])_s$, функции Гильберта $\mathcal{H}$ кольца $\mathbb{F}_q[\mathcal{P}_F]$, локального кольца $\mathcal{O}_{F,P}$ точки P кривой $\mathcal{P}_F$, кратности пересечения плоских проективных кривых в терминах локальных колец. В конце главы вводится конструкция класса АГРС-кодов, рассматриваются формулы вычисления их параметров, обсуждается связь с РС-кодами и АГ-кодами, выбирается модель вычислений для оценки сложности построенных в работе алгоритмов.

Определение. *Пусть $\mathcal{P}_F$ – гладкая плоская проективная кривая рода g, порожденная абсолютно неприводимым однородным многочленом $F \in \mathbb{F}_q[x_1, x_2, x_3]$ степени m, $\mathcal{A}$ – подмножество всех $\mathbb{F}_q$-рациональных точек $\mathcal{P}_F$ с зафиксированными значениями однородных координат, $n = |\mathcal{A}|$. Для произвольного $j \in [1, \lfloor (n-1)/m \rfloor]$ определим АГРС-код $C_{F,\mathcal{A}}(j)$ как образ отображения вычисления*

$$ev_{\mathcal{A}}^{(j)} : (\mathbb{F}_q[\mathcal{P}_F])_j \to \mathbb{F}_q^n, \quad f \mapsto (f(P_1), f(P_2), \ldots, f(P_n)).$$

Доказывается, что АГРС-код $C_{F,\mathcal{A}}(j)$ имеет длину n, размерность $k(j) = \mathcal{H}(j)$, минимальное кодовое расстояние $d(j) \geq n - mj$.

Вторая глава посвящена построению алгоритмов декодирования произвольного АГРС-кода. В пункте 2.1 рассматриваются центральные в современной теории кодирования задачи декодирования по максимуму правдоподобия и списочного декодирования. Показывается, что задача декодирования по максимуму правдоподобия может быть сведена к задачам декодирования с ограниченным расстоянием и списочного декодирования. Пусть C – линейный код в метрическом векторном пространстве $\mathbb{F}_q^n$ с метрикой Хемминга $d(x, y)$. Для произвольных $v \in \mathbb{F}_q^n$ и целого $R \in [1, n]$ рассмотрим множество

$$C^{(R)}(v) = \{c \in C \mid d(v, c) \leq R\}.$$

Задача списочного декодирования заключается в вычислении множества $C^{(R)}(v)$, *задача декодирования с ограниченным расстоянием* является практически важным частным случаем задачи списочного декодирования и заключается в вычислении множества $C^{(R)}(v)$ при $R \in [1, \lfloor (d-1)/2 \rfloor]$, где d – минимальное расстояние кода C. Пункт 2.1 заканчивается аналитическим обзором существующих алгоритмов списочного декодирования РС-кодов и АГ-кодов, рассмотрением возможности их практической реализации.

В пункте 2.2 на основе идей подхода Берлекэмпа-Велча к декодированию РС-кодов строится и полностью обосновывается алгоритм UniqDecoding декодирования произвольного АГРС-кода $C_{F,\mathcal{A}}(j)$ с ограниченным расстоянием до $d^*(j) - 1 - m\lceil (d^*(j) - 1)/2m + g/m \rceil$, где $d^*(j) = n - mj$ – конструктивное расстояние кода $C_{F,\mathcal{A}}(j)$. Центральной частью алгоритма UniqDecoding является вычисление многочлена вида $Q_a(T) = N + DT$, где $D \in (\mathbb{F}_q[\mathcal{P}_F])_a$, $N \in (\mathbb{F}_q[\mathcal{P}_F])_{a+j}$, $a = \lceil (d^*(j) - 1)/2m + g/m \rceil$, удовлетворяющего условиям

$$\forall i \in [1, n], \forall P_i \in \mathcal{A} : \ N(P_i) + v_i D(P_i) = 0, \tag{1}$$

и последующее нахождение его T-корня из $(\mathbb{F}_q[\mathcal{P}_F])_j$. В этом же пункте вычисляются асимптотические оценки временной и емкостной сложности построенного алгоритма в наихудшем случае, равные $T_{UD}(n,j)+O(n^3)$, $A_{UD}(n,j)+O(n^2)$ соответственно, где $T_{UD}(n,j)$, $A_{UD}(n,j)$ – временная и емкостная сложности алгоритма вычисления корня многочлена $Q_a(T)$.

В пункте 2.3 на основе идей подхода Судана к списочному декодированию РС-кодов строится и полностью обосновывается базовый алгоритм ListDecoding списочного декодирования произвольного АГРС-кода $C_{F,\mathcal{A}}(j)$, основанный на вычислении многочлена вида $Q_{a,b}(T)=\sum_{s=0}^{b} D_sT^s$, где для всех $s\in[0,b]$: $D_s\in(\mathbb{F}_q[\mathcal{P}_F])_{a+(b-s)j}$, с последующим вычислением множества всех T-корней $Q_{a,b}(T)$ из $(\mathbb{F}_q[\mathcal{P}_F])_j$. В процессе обоснования алгоритма доказывается, что если параметры алгоритма a, b и целое число $R\in[1,n]$ удовлетворяют системе неравенств

$$\begin{cases} \sum_{s=0}^{b}\mathcal{H}(a+(b-s)j)>n, \\ n-R>m(a+bj), \end{cases}$$

то алгоритм ListDecoding для произвольного $v\in\mathbb{F}_q^n$ вычисляет все элементы множества $C^{(R)}(v)$, при этом $|C^{(R)}(v)|\le b$. После обоснования корректности алгоритма вычисляются асимптотические оценки временной и емкостной сложности построенного алгоритма в наихудшем случае, равные $T(a,b,j)+O(bn^3)$, $A(a,b,j)+O(bn^2)$ соответственно, где $T(a,b,j)$, $A(a,b,j)$ – временная и емкостная сложности алгоритма вычисления всех корней многочлена $Q_{a,b}(T)$. В конце пункта 2.3 рассматриваются вопросы выбора значений параметров a, b, R алгоритма и оценивается верхняя граница $\rho_{\max}(\lambda)$, $\lambda=mj/n\approx k(j)/n$, максимального значения отношения R/n в зависимости от параметров кода $C_{F,\mathcal{A}}(j)$. В частности, доказывается, что $\rho_{\max}(\lambda)>\rho_1(\lambda)$, где $\rho_1(\lambda)$ – максимальное значение отношения R/n при $b=1$, только в случае $\lambda\le 0,3(3)$.

В пункте 2.4 на основе идей подхода Гурусвами-Судана к модификации алгоритма Судана списочного декодирования РС-кодов строится и полностью обосновывается модифицированный алгоритм MListDecoding списочного декодирования произвольного АГРС-кода $C_{F,\mathcal{A}}(j)$. В начале пункта вводится критерий того, что пара $(P,v)\in\mathcal{A}\times\mathbb{F}_q$ является нулем кратности не менее $r(>0)$ заданного многочлена $Q_{a,b}(T)=\sum_{s=0}^{b} D_sT^s$,

$\forall s \in [0,b]$: $D_s \in (\mathbb{F}_q[\mathcal{P}_F])_{a+(b-s)j}$, по отношению к некоторой проективной прямой $L \in \mathbb{F}_q[\mathcal{P}_F]$, показывается, что в каждой градуировочной компоненте кольца $\mathbb{F}_q[\mathcal{P}_F]$ существует базис специального вида, удобный для вычисления кратности, и доказывается следующая

Теорема 1. *Для произвольного целого $j \in \left[1, \left\lfloor \frac{n-1}{m} \right\rfloor\right]$ зафиксируем АГРС-код $C_{F,\mathcal{A}}(j)$ длины n, размерности $k(j)$, с конструктивным расстоянием $d^*(j) = n - mj$. Если существуют целые числа $r \in \mathbb{N}$, $a \in \left[0, \frac{r(d^*(j)-1)-1}{m}\right]$, $b \in \mathbb{N}$, $R \in [1,n]$, удовлетворяющие неравенствам*

$$\begin{cases} \sum_{s=0}^{b} \mathcal{H}(a+(b-s)j) > n\binom{r+1}{2}, \\ r(n-R) > m(a+bj), \end{cases}$$

то для любого вектора $v = (v_1, \ldots, v_n) \in \mathbb{F}_q^n$ справедливы утверждения:

(i) в кольце многочленов $\mathbb{F}_q[\mathcal{P}_F][T]$ одной переменной T существует такой ненулевой многочлен

$$Q_{a,b}(T) = D_0 + D_1 T + D_2 T^2 + \ldots + D_b T^b,$$

что

(a) $\forall i \in [0,b] :\ D_i \in (\mathbb{F}_q[\mathcal{P}_F])_{a+(b-i)j}$, $D_b \neq 0$,

(b) для всех $i \in [1,n]$ элемент (P_i, v_i) является нулем $Q_{a,b}(T)$ кратности не менее r по отношению к некоторой прямой L_i;

(ii) многочлен $Q_{a,b}(T)$ может быть найден за время $O(bn^3r^5)$;

(iii) любой элемент множества

$$B^{(R)}(v) = \left\{ G \in (\mathbb{F}_q[\mathcal{P}_F])_j \mid d(ev_{\mathcal{A}}^{(j)}(G), v) \le R \right\}$$

является T-корнем многочлена $Q_{a,b}(T)$: $\forall G \in B^{(R)}(v) :\ Q_{a,b}(G) = 0$.

На основании теоремы 1 выписывается алгоритм списочного декодирования, получающий на вход вектор v, значения параметров a, b, R, r, и вычисляющий множество $C^{(R)}(v)$. Далее определяются асимптотические оценки временной и емкостной сложности алгоритма MListDecoding в наихудшем случае, равные $T(a,b,j)+O(bn^3r^5)$, $A(a,b,j)+O(bn^2r^3)$ соответственно, где $T(a,b,j)$, $A(a,b,j)$ – временная и емкостная сложности алгоритма вычисления всех корней многочлена $Q_{a,b}(T)$. Завершается пункт рассмотрением вопроса оптимального выбора значений параметров a, b, R, r алгоритма и оценивается верхняя граница $\rho_{\max}^{(r_0)}(\lambda)$, $\lambda = mj/n \approx k(j)/n$, максимального значения отношения R/n в зависимости от параметров кода $C_{F,\mathcal{A}}(j)$ и фиксированного значения r_0 параметра r. В частности, доказывается, что

$$\forall r_0 \in \mathbb{N},\, \forall \lambda \in (0,1):\; 1/2 - \lambda/2 \le \rho_{\max}^{(r_0)}(\lambda) \le 1 - \sqrt{\lambda}.$$

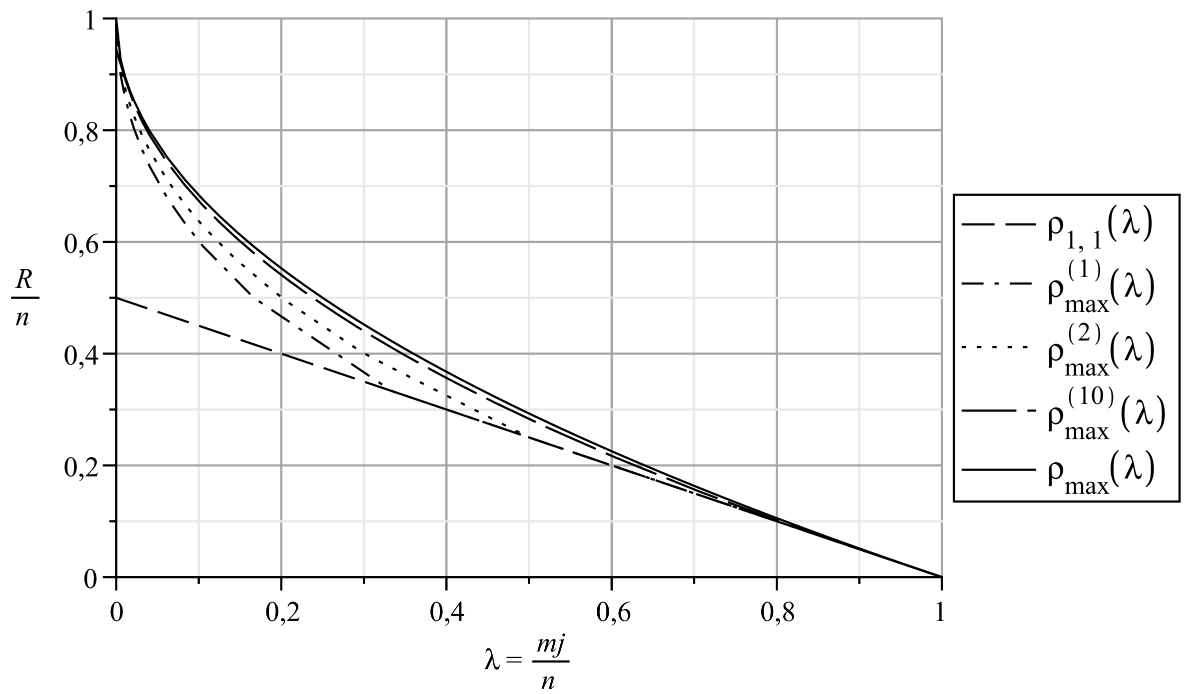

Рисунок 1. Зависимость $\rho_{1,1}(\lambda)$, $\rho_{\max}^{(1)}(\lambda)$, $\rho_{\max}^{(2)}(\lambda)$, $\rho_{\max}^{(10)}(\lambda)$, $\rho_{\max}(\lambda)$ от λ

На рис. 1 для наглядности представлены графики функций $\rho_{1,1}(\lambda)$, $\rho_{\max}^{(1)}(\lambda)$, $\rho_{\max}^{(2)}(\lambda)$, $\rho_{\max}^{(10)}(\lambda)$, соответствующих случаям декодирования с ограниченным расстоянием, списочного декодирования с помощью алгоритма ListDecoding, списочного декодирования с помощью алгоритма MListDecoding с кратностями $r = 2$ и $r = 10$ соответственно, а также график функции $\rho_{\max}(\lambda) = 1-\sqrt{\lambda}$. Из их сравнения можно сделать вывод о том, что алгоритм MListDecoding по сравнению с алгоритмом ListDecoding потенциально позволяет вычислять список мощности 2 и выше для АГРС-кодов, параметры которых удовлетворяют условию $k(j)/n \approx \lambda \geq 0,3(3)$.

Несмотря на то, что алгоритм UniqDecoding является частным случаем алгоритма ListDecoding, который, в свою очередь, является частным случаем алгоритма MListDecoding, каждый из алгоритмов имеет самостоятельное практическое значение. Так, алгоритм UniqDecoding решает классическую задачу декодирования с ограниченным расстоянием, а алгоритм ListDecoding значительно проще алгоритма MListDecoding за счет отсутствия требований к кратности нулей вида (P, v), что исключает рассмотрение в нем дополнительных математических объектов и во многом упрощает структуру системы уравнений, возникающей при вычислении $Q_{a,b}(T)$.

Третья глава посвящена построению алгоритмов вычисления корней многочленов с коэффициентами из кольца $\mathbb{F}_q[\mathcal{P}_F]$, возникающих в алгоритмах декодирования АГРС-кодов из главы 2.

В пункте 3.1 рассматривается задача вычисления корня многочлена $Q_a(T) = N + DT \in \mathbb{F}_q[\mathcal{P}_F]$, возникающая в алгоритме UniqDecoding, и на основе метода неопределенных коэффициентов строится алгоритм FindRootUD. Основная идея алгоритма заключается в том, что произвольный элемент G пространства $(\mathbb{F}_q[\mathcal{P}_F])_j$ может быть записан в виде $G = \sum_{s=0}^{\mathcal{H}(j)} G_s \phi_s^{(j)}$, где $\phi_1^{(j)}, \ldots, \phi_{\mathcal{H}(j)}^{(j)}$ – базис $(\mathbb{F}_q[\mathcal{P}_F])_j$, $\forall s \in [1, \mathcal{H}(j)] : G_s \in \mathbb{F}_q$. Тогда система равенств (1) может быть рассмотрена как неоднородная система линейных уравнений относительно неизвестных коэффициентов G_s элемента G. Решая эту систему, например, методом Гаусса, можно либо вычислить коэффициенты искомого корня G, либо выявить отсутствие корня многочлена $Q_a(T)$ в пространстве $(\mathbb{F}_q[\mathcal{P}_F])_j$. Асимптотические оценки временной и емкостной сложностей алгоритма FindRootUD равны $O(k(j)n^2)$ и $O(d^*(j)k(j)n)$ соответственно, итоговые асимптотические оценки временной и емкостной сложностей алгоритма UniqDecoding с использованием алгоритма FindRootUD равны $O(n^3)$ и $O(n^2)$.

В пункте 3.2 рассматривается задача вычисления множества всех корней многочлена $Q_{a,b}(T) = \sum_{s=0}^{b} D_s T^s \in \mathbb{F}_q[\mathcal{P}_F]$, возникающего в алгоритмах ListDecoding, MListDecoding, и, на основе идеи проекционного подхода Гао-Шокройахи, строится алгоритм FindRootsLD. Центральным шагом алгоритма FindRootsLD является построение такого гомоморфизма Pr кольца $\mathbb{F}_q[\mathcal{P}_F]$ и некоторого расширения $\mathbb{F}_{q^e}$ поля $\mathbb{F}_q$, что сужение Pr на градуировочную компоненту $(\mathbb{F}_q[\mathcal{P}_F])_j$ является мономорфизмом. После этого задачу вычисления всех корней многочлена $Q_{a,b}(T)$ можно свести к задаче вычисления всех корней многочлена $Pr(Q_{a,b}(T)) \stackrel{\text{def}}{=} \sum_{s=0}^{b} Pr(D_s)T^s$ в поле $\mathbb{F}_{q^e}$ с последующим восстановлением их прообразов относительно Pr. В пункте доказывается, что в качестве гомоморфизма Pr можно взять гомоморфизм вычисления значения элементов $\mathbb{F}_q[\mathcal{P}_F]$ в $\mathbb{F}_{q^e}$-рациональной точке $\mathbf{P}$ степени e кривой $\mathcal{P}_F$ с фиксированными однородными координатами при условии, что величина e удовлетворяет неравенству $e > \max\{mj, ma\}$. Кроме того отмечено, что если величина e удовлетворяет неравенству

$$q^e - 2gq^{e/2} > \sum_{r|e, r<e} (q^r + 2gq^{r/2}),$$

то на кривой $\mathcal{P}_F$ существует не менее e $\mathbb{F}_{q^e}$-рациональных точек степени e. Алгоритм FindRootsLD заключается в вычислении многочлена $Pr(Q_{a,b}(T)) \in \mathbb{F}_{q^e}[T]$, нахождении всех его корней в поле $\mathbb{F}_{q^e}$ с помощью какого-либо известного метода и для каждого найденного корня β вычислении решения уравнения $Pr(G) = \beta$, рассматриваемого как системы из e линейных уравнений относительно неизвестных коэффициентов разложения G по базису $(\mathbb{F}_q[\mathcal{P}_F])_j$. В конце пункта вычисляются асимптотические оценки временной и емкостной сложностей алгоритма FindRootsLD, равные $T_F(b, e, q) + O(be(e + (a + bj)^2))$ и $A_F(b, e, q) + O(be(a + bj)^2 + mj(b + e))$, где $T_F(b, e, q)$, $A_F(b, e, q)$ – временная и емкостная сложности алгоритма вычисления всех корней многочлена степени b из $\mathbb{F}_{q^e}[T]$. Кроме того, вычисляются итоговые асимптотические оценки алгоритмов UniqDecoding, ListDecoding, MListDecoding при условии использования в них на шаге факторизации алгоритма FindRootsLD, равные, соответственно, $O(n^3)$, $O(n^2)$, $T_F(b, e, q) + O(bn^3)$, $A_F(b, e, q) + O(bn^2)$, $T_F(b, e, q) + O(bn^3r^5)$, $A_F(b, e, q) + O(bn^2r^3)$.

Четвертая глава посвящена задаче построения алгоритма FindRoots вычисления всех корней полной степени не выше d многочлена одной переменной $Q(T)$ с коэффициентами из кольца многочленов $n(\geq 1)$ переменных над произвольной областью $\mathbb{D}$.

В пункте 4.1 вводятся необходимые обозначения, рассматривается связь поставленной задачи с классическими алгоритмами факторизации многочленов нескольких переменных, прогнозируются области возможного применения алгоритма.

В пункте 4.2 вводится проекционный гомоморфизм

$$\psi_n^T : \mathbb{D}[x_1, \ldots, x_n][T] \to \mathbb{D}[x_1, \ldots, x_{n-1}][T],$$

сопоставляющий произвольному многочлену результат подстановки вместо переменной x_n нулевого элемента области $\mathbb{D}$, и для произвольного ненулевого многочлена $Q(T) \in \mathbb{D}[x_1, \ldots, x_n][T]$ и его корня $f \in \mathbb{D}[x_1, \ldots, x_n]$ степени не выше d определяются вспомогательные последовательности многочленов $\{Q_i(T)\}_{i=0}^d$, $\{M_i(T)\}_{i=0}^d$ и $\{f_i\}_{i=0}^d$ из колец $\mathbb{D}[x_1, \ldots, x_n][T]$, $\mathbb{D}[x_1, \ldots, x_{n-1}][T]$ и $\mathbb{D}[x_1, \ldots, x_{n-1}]$ соответственно, вычисляемые рекурсивно следующим образом: $f_0 = f$, $Q_0(T) = Q_0^{(x)}(T) = Q^{(x)}(T)$, $M_0(T) = \psi_n^T(Q_0(T))$, $\forall i \in [1, d]$

$$f_i = (f_{i-1} - \psi_n^T(f_{i-1}))/x_n,$$
$$Q_i(T) = Q_{i-1}^{(x)}(x_n T + \psi_n^T(f_{i-1})), \quad M_i(T) = \psi_n^T(Q_i^{(x)}(T)),$$

где $Q_i^{(x)}(T) = Q_i(T)/x_n^{r_i}$, r_i – такое неотрицательное целое число, что $x_n^{r_i}$ делит $Q_i(T)$, но $x_n^{r_i}$ не делит $Q_i(T)$. Далее исследуются различные свойства этих последовательностей многочленов, с помощью которых доказываются следующие важные утверждения:

1) $f = \sum_{i=0}^d x_n^i \psi_n^T(f_i)$.

2) *Если $(T - f)$ делит $Q(T)$, то для всех целых $i \in [0, d]$ многочлен $(T - \psi_n^T(f_i))$ делит многочлен M_i.*

3) *$(T - f)$ делит $Q(T)$ тогда и только тогда, когда T делит $Q_{d+1}(T) \stackrel{\text{def}}{=} Q_d^{(x)}(x_n T + \psi_n^T(f_d))$.*

В конце пункта 4.2 описывается идея рекурсивного алгоритма FindRoots, заключающаяся в следующем. Если для каждого $i \in [0, d]$ выполнить следующие действия: вычислить множество $\Omega_{M_i,n-1}(d-i)$ всех корней степени не выше $d-i$ многочлена $M_i(T) \in \mathbb{D}[x_1, \ldots, x_{n-1}][T]$ и для каждого элемента множества $\Omega_{M_i,n-1}(d-i)$, являющегося кандидатом на составляющую $\psi_n^T(f_i)$ некоторого корня f многочлена $Q(T)$, вычислить многочлен $M_{i+1}(T)$, то, при $i = d$, мы получим множество последовательностей вида $\{\psi_n^T(f_i)\}_{i=0}^d$ и соответствующих им последовательностей $\{Q_i(T)\}_{i=0}^d$, $\{M_i\}_{i=0}^d$. Те последовательности $\{\psi_n^T(f_i)\}_{i=0}^d$, для которых T делит $Q_{d+1}(T)$, согласно утверждению 3 соответствуют корням исходного многочлена $Q(T)$ и по ним можно восстановить искомые корни в соответствии с утверждением 1.

В пункте 4.3 на основе результатов из пункта 4.2 строится рекурсивный алгоритм FindRoots вычисления всех корней степени не выше d многочлена $Q(T)$. Особенностью алгоритма является наличие двойной рекурсии – по количеству переменных в коэффициентах текущего многочлена и по номеру вычисляемого многочлена в текущей вспомогательной последовательности многочленов. В конце пункта 4.3 обосновывается корректность алгоритма и доказывается, что алгоритм закончит свою работу за конечное число шагов. Отметим, что при $n = 1$ и $\mathbb{D} = \mathbb{F}_q$ алгоритм FindRoots на уровне идей совпадает с алгоритмом Рота-Рукенштейн.

Пункт 4.4 посвящен анализу вычислительной сложности алгоритма FindRoots. Для этого процесс работы алгоритма представляется как ориентированный лес, в котором каждому дереву соответствует рекурсивный вызов алгоритма с уменьшением количества переменных в коэффициентах многочленов, а каждой вершине дерева соответствует рекурсивный вызов алгоритма с переходом к следующему многочлену из вспомогательной последовательности. В пункте оценивается максимальная полная степень многочленов, вычисляемых в процессе работы алгоритма, максимальные ширина и количество вершин каждого дерева леса вызовов, общее количество деревьев леса, суммарное количество вершин деревьев леса и на основе этих оценок доказывается, что асимптотическая оценка временной сложности алгоритма в наихудшем случае равна

$$O(bd^n(F(b) + (s + bd^2)^{2n} + b^2d^{n-1}(s + bd^2)^n))$$

арифметических операций в области $\mathbb{D}$, где b – максимальная степень переменной T в многочлене $Q(T)$, s – максимальная полная степень коэффициентов $Q(T)$, $F(b)$ – временная сложность алгоритма вычисления всех корней многочлена из кольца $\mathbb{D}[T]$ степени b. Отметим, что в случае $\mathbb{D} = \mathbb{F}_q$ оценка временной сложности алгоритма FindRoots может быть упрощена:

$$O(bd^n(F(b) + (s + bd^2)^{2n} + b^2(s + bd^2)^{(n-1)\log_2 3+1})).$$

Одновременно с анализом сложности алгоритма во второй части пункта 4.4 рассматриваются вопросы оптимального представления многочленов и реализации арифметических операций с ними с точки зрения уменьшения вычислительных затрат.

Завершается работа **заключением**, в котором сформулированы основные результаты и кратко обозначены возможные направления дальнейших исследований.

Публикации автора по теме диссертации

Статьи в ведущих рецензируемых научных журналах и изданиях, включенных в перечень ВАК РФ

1. *Маевский А.Э.* Алгоритм вычисления корней многочленов с коэффициентами из кольца многочленов над произвольной областью целостности. // Математические заметки, 2009. Т.85. Вып.1. С. 73-88.

2. *Маевский А.Э.* Алгоритм поиска корней многочленов с коэффициентами из кольца $k[x, y]$. // Вестник Донского государственного технического университета, 2007. Т.7. №3(34). С. 263-269.

3. *Маевский А.Э. Пеленицын А.М.* Реализация программного алгебро-геометрического кодека с применением алгоритма Сакаты. // Известия Южного федерального университета. Технические науки. Тематический выпуск "Информационная безопасность", 2008. №8(85). С. 196-198.

Другие публикации

4. *Маевский А.Э.* Алгоритм списочного декодирования одного класса алгебро-геометрических кодов на проективных кривых. // Интегральные и дифференциальные уравнения. Сб. статей. Вып. 6. Ростов-на-Дону: ДГТУ, 2007. С. 73-78.

5. *Маевский А.Э.* Аналог алгоритма Гурусвами-Судана для списочного декодирования специального класса алгебро-геометрических кодов. // Материалы XI Международной научно-практической конференции "Информационная безопасность". В 3 ч. Ч.1. Таганрог: Издательство ТТИ ЮФУ, 2010. С. 226-231.

6. *Маевский А.Э.* Некоторые алгебро-геометрические кодеки и их программная реализация. // Труды участников международной школы-семинара по геометрии и анализу памяти Н.В.Ефимова. Ростов-на-Дону: Издательство ООО "ЦВВР", 2004. С. 208-209.

7. *Маевский А.Э.* О распространении алгоритма Берлекэмпа-Велча на один класс алгебро-геометрических кодов на проективных кривых. // Тезисы докладов международной алгебраической конференции, посвященной 100-летию со дня рождения Д.К.Фаддеева. СПб., 2007. С. 52-54.

8. *Маевский А.Э.* О списочном декодировании одного класса алгебро-геометрических кодов на проективных кривых // Труды участников международной школы-семинара по геометрии и анализу памяти Н.В. Ефимова. Ростов-на-Дону: Изд-во ООО "ЦВВР", 2006. С. 55-56.

9. *Маевский А.Э.* Полиномиальный алгоритм списочного декодирования специального класса алгебро-геометрических кодов // Труды научной школы И.Б.Симоненко. Ростов-на-Дону: Издательство ЮФУ, 2010. С. 145-168.

10. *Маевский А.Э.* Разработка и исследование помехоустойчивых свойств алгебро-геометрического списочного кодека // Теория и практика создания радиотехнических и мехатронных систем (теория, проектирование, экономика): Материалы межрегиональной научно-практической конференции, ФГУП "ВНИИ "Градиент". Ростов-на-Дону, 2007. С. 12-13.

11. *Маевский А.Э., Мкртичян В.В.* О некоторых стратегиях детерминизации списочных декодеров // Интегральные и дифференциальные уравнения. Сб. статей. Вып. 6. Ростов-на-Дону: ДГТУ, 2007. С. 79-87.