На правах рукописи

Лапиков Игорь Игоревич

ПОСТРОЕНИЕ И РЕАЛИЗАЦИЯ АЛГОРИТМОВ РЕШЕНИЯ СИСТЕМ ЦЕЛОЧИСЛЕННЫХ НЕРАВЕНСТВ В МЕТОДЕ РАЗДЕЛЯЮЩИХ ПЛОСКОСТЕЙ

05.13.19 – «Методы и системы защиты информации, информационная безопасность»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2019

Работа выполнена в Федеральном государственном учреждении «Федеральный исследовательский центр «Информатика и управление» Российской академии наук»

Научный руководитель: **Никонов Владимир Глебович**
доктор технических наук, профессор, член-корреспондент ФГКНУ «Академия криптографии Российской Федерации»

Официальные оппоненты: **Еремеев Михаил Алексеевич**
доктор технических наук, профессор, профессор кафедры «Прикладные и информационные технологии» Института комплексной безопасности и специального приборостроения ФГБУ ВО «МИРЭА – Российский технологический университет»

Алексеев Евгений Константинович
кандидат физико-математических наук, начальник отдела криптографических исследований ООО «КРИПТО-ПРО»

Ведущая организация: Федеральное государственное унитарное предприятие «Научно-исследовательский институт «КВАНТ»

Защита диссертации состоится 19 июня 2019 г. в 13 ч. 30 мин. на заседании диссертационного совета Д 002.073.02 при Федеральном исследовательском центре «Информатика и управление» Российской академии наук по адресу: 119333, г. Москва, ул. Вавилова, д.44, кор.2.

С диссертацией можно ознакомиться в библиотеке Федерального исследовательского центра «Информатика и управление» Российской академии наук по адресу: г. Москва, ул. Вавилова, д.44, кор. 2 и на сайте www.frccsc.ru.

Автореферат разослан «___» _____ 2019 г.

Ученый секретарь
диссертационного совета Р.В. Разумчик

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Расширение арсенала методов анализа и синтеза современных узлов защиты информации за счет использования достижений физики и математики, в том числе в действительной области, является актуальным направлением развития современных систем связи.

Повышение быстродействия систем передачи и обработки информации предполагает обращение к новым физическим принципам, например, с привлечением оптических методов. Оптическая среда обладает целым рядом особенностей в сравнении с традиционной, в частности, в оптике относительно легко могут быть выполнены операции вычисления скалярного произведения и сравнения. Сочетание этих двух операций приводит к реализации пороговой функции и делает пороговый базис перспективным для переработки информации в этой вычислительной среде, включая построение систем защиты информации.

В диссертации рассмотрена модель угрозы несанкционированного доступа к защищаемой информации путем программно-математического воздействия на информационную систему с использованием уязвимостей генераторов псевдослучайных последовательностей (ПСП), реализованных в аппаратных или программных средствах защиты. Техническая проблема построения скоростных и просто реализуемых генераторов ПСП для решения задач информационной безопасности базируется на противоречии между характеристиками самого генератора с одной стороны и обеспечением приемлемого уровня его устойчивости к компрометации с учетом существующих методов анализа с другой. Базовая задача информационной безопасности, на решение которой направлены проведенные исследования, состоит в разработке методов компрометации генераторов ПСП. Для ее решения в диссертации используются пороговые методы, при использовании которых исходная задача анализа генератора интерпретируется как задача решения систем неравенств в действительной области с булевыми или k-значными неизвестными. Такой прием известен как метод разделяющих плоскостей и направлен на решение произвольных систем дискретных уравнений. Его исходные положения, обоснование и развитие приведены в работах Балакина Г.В., Анашкиной Н.В., Никонова В.Г., Никонова Н.В., Рыбникова К.К., Шурупова А.Н., Ivanescu P.L., Rudeanu S. и других.

В трудах этих авторов основное внимание уделялось проблеме сведения исходных нелинейных систем уравнений, описывающих работу узлов защиты информации, к равносильным системам неравенств в булевой или k-значной области. В то же время менее подробно рассматривались вопросы анализа и решения самих систем линейных неравенств, поскольку для этого

предполагалось использовать известные алгоритмы линейного программирования и дискретной оптимизации, которые адаптировались к конкретной специфике задачи.

Последующие исследования показали актуальность построения новых методов решения систем линейных неравенств, поскольку именно алгоритмическая часть метода разделяющих плоскостей в конечном итоге и определяет его вычислительную сложность. Алгоритмические вопросы приобрели еще большую актуальность после появления полиномиального алгоритма Хачияна решения систем линейных неравенств с целочисленными коэффициентами относительно действительных неизвестных. Не предполагая нахождения непосредственно целочисленных решений, алгоритм Хачияна, тем не менее, для ряда практических приложений показал свою эффективность, позволяя по найденным действительным решениям определять целочисленные путем простого округления. Особый интерес алгоритм Хачияна представляет при рассмотрении систем неравенств с k-значными неизвестными в силу того, что при увеличении k множество решений, образующих n-мерную k-звенную решетку, приближается по своим математическим свойствам к множеству действительных значений n-мерного куба со стороной равной $k-1$.

Таким образом, исследование алгоритмов решения систем линейных неравенств, в частности алгоритма Хачияна, является важным направлением для информационной безопасности и дискретной математики в целом, что свидетельствует об актуальности темы диссертации.

Объектом исследования являются системы целочисленных неравенств, возникающие в задачах информационной безопасности, сводящихся к решению систем такого вида.

Предметом исследования являются методы решения систем линейных неравенств в действительной и дискретной областях.

Основной целью исследования является построение и реализация алгоритмов решения линейных неравенств, возникающих в прикладных задачах информационной безопасности и дискретной математики.

Научная новизна. В работе построен новый алгоритм решения систем линейных неравенств с дискретными неизвестными, основанный на методе эллипсоидов. Для отдельных классов таких систем показано, что он имеет полиномиальную оценку сложности. Разработанный алгоритм впервые применен для решения всех рассмотренных в диссертации прикладных задач анализа узлов защиты информации. Новым положением следует признать применение полиномиального алгоритма, основанного на методе эллипсоидов, для решения задачи характеризации k-значной пороговой функции.

Теоретическая значимость диссертационного исследования состоит в развитии метода разделяющих плоскостей для решения систем дискретных уравнений и сводящихся к ним системам защиты информации в *k*-значной логике. С теоретической точки зрения представляет интерес полученная оценка расстояния единственности задачи нахождения начального заполнения линейного регистра сдвига с трехчленным законом обратной связи по отрезку подряд идущих знаков старшего разряда.

Практическая значимость заключается в обосновании применения метода эллипсоидов для широкого круга прикладных задач анализа узлов защиты информации, сводящихся к решению систем неравенств с дискретными неизвестными. Важное практическое значение имеет выполненная в процессе диссертационного исследования разработка программного комплекса.

Методология и методы исследования. В работе использованы алгебраические, комбинаторные, геометрические, алгоритмические методы исследования, методы дискретной оптимизации и параллельные вычисления.

Реализация и внедрение результатов работы. Результаты диссертационного исследования внедрены в образовательный процесс Балтийского Федерального университета им. И. Канта в форме раздела курса лекционных занятий при подготовке специалистов по направлению 10.05.01 «Компьютерная безопасность» и в практическую деятельность ООО «Ю-КОРП» и ООО «Лингвистические и информационные технологии». В ходе работы над диссертационным исследованием получены свидетельства о регистрации программ для ЭВМ:

1. «Программа, реализующая адаптивный алгоритм эллипсоидов решения систем линейных неравенств с *k*-значными неизвестными» №2018617222 [11].

2. Программный комплекс «Практические приложения адаптивного алгоритма эллипсоидов в задачах информационной безопасности, сводящихся к решению систем неравенств с *k*-значными неизвестными» №2018616595 [12].

Личный вклад. Выносимые на защиту результаты получены соискателем лично. В опубликованных совместных работах постановка и исследование задач осуществлялись совместными усилиями авторов при непосредственном участии соискателя.

Апробация работы. Основные результаты работы докладывались и обсуждались на XLIII Международной конференции, XIII Международной конференции молодых ученых «Информационные технологии в науке, образовании, телекоммуникации и бизнесе ‘IT+SE15’» (2015 г.), Всероссийской конференции «Сибирская научная школа-семинар с международным участием 'Компьютерная безопасность и криптография' SIBECRYPT'17» (2017 г.), XI Всероссийской научной конференции ученых, специалистов и профессорско-преподавательского состава «Территориальные распределенные системы

охраны» (2018 г.) и семинарах в Балтийском Федеральном университете им. И. Канта и Федеральном исследовательском центре «Информатика и управление» Российской академии наук.

Результаты диссертационного исследования полностью отражены в 10 печатных работах. Из них 7 статей в рецензируемых журналах [1-7], рекомендованных ВАК для публикации основных научных результатов диссертаций на соискание ученой степени кандидата наук, и 3 публикации в материалах международных и всероссийских конференций [8, 9, 10].

Степень достоверности полученных результатов подтверждена проработкой литературных источников по теме диссертации, реализацией необходимого количества численных расчётов, а также современной методикой исследования, которая соответствует поставленным в работе целям и задачам. Научные положения, выводы и рекомендации, сформулированные в диссертации, подкреплены убедительными фактическими данными, наглядно представленными в приведенных таблицах и рисунках. Достоверность всех полученных теоретических результатов обоснована их строгими математическими доказательствами. Проверка корректности результатов также осуществлялась с использованием вычислительных экспериментов.

На защиту выносятся следующие основные положения:

1. Адаптивный алгоритм решения систем линейных неравенств с *k*-значными неизвестными, развивающий метод эллипсоидов Хачияна.
2. Пространственно-декомпозиционный алгоритм, основанный на геометрическом распараллеливании адаптивного алгоритма эллипсоидов.
3. Экспериментальное доказательство возможности применения разработанных алгоритмов для решения широкого класса прикладных задач, включая анализ узлов защиты информации, сводящихся к решению систем линейных неравенств с *k*-значными неизвестными.
4. Способ применения адаптивного алгоритма эллипсоидов для восстановления линейной рекурренты над кольцом $\mathbb{Z}_{2^m}$, реализованной линейным регистром сдвига с трехчленным законом обратной связи, по подряд идущим знакам ее старшей координатной последовательности, который позволил дать оценку расстоянию единственности задачи.
5. Применение модифицированного метода эллипсоидов Хачияна для характеризации *k*-значной пороговой функции.

Объем и структура диссертации. Диссертация состоит из введения, 3-х глав, заключения, списка использованной литературы и 7 приложений. Каждая глава завершается выводами. Общий объем диссертации – 164 страницы машинописного текста (с приложениями). Основная часть работы изложена на 143 страницах и содержит 19 рисунков и 16 таблиц. Список литературы включает 125 наименований.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность диссертационной работы, сформулированы цели, научная новизна исследования, перечислены используемые методы исследования, показана теоретическая и практическая значимость полученных результатов, приведены сведения о результатах внедрения, представлены выносимые на защиту положения.

В **первой главе** рассмотрена проблематика псевдобулева направления в дискретной математике, проведен анализ метода разделяющих плоскостей в булевом случае, изучены основные проблемы его переноса в *k*-значную область. В ***параграфе 1.1*** рассмотрены пороговые функции, задаваемые линейными неравенствами в действительной области. Непосредственно в самом представлении пороговые функции сочетают области действительной и дискретной математики, что нашло свое отражение и в задачах синтеза пороговых элементов, реализующих пороговых функции, и в использовании аппарата линейных неравенств при анализе дискретных схем. С точки зрения синтеза арифметические операции подсчета скалярного произведения и сравнения могут быть реализованы в аналоговой среде, что согласуется с различными удобными вычислительными платформами. Использование пороговых функций при анализе позволяет перевести исходные дискретные задачи в действительную область с привлечением хорошо разработанных методов непрерывной математики. В то же время, несмотря на простоту и логическую лаконичность задания, пороговые функции оказались весьма сложным объектом исследования, так как в общем случае не оказалось какого-либо легко проверяемого критерия принадлежности функций к классу пороговых. Особое внимание в параграфе уделено свойствам монотонности пороговых булевых и *k*-значных функций, а также вопросу сложности реализации пороговых функций в традиционных базисах.

В ***параграфе 1.2*** проведен обзор направлений развития методов анализа и решения произвольных систем булевых уравнений

$$\left\{ f_i\left(x_1,\ldots,x_n\right)=a_i, \text{ где } x_j, a_i \in \{0,1\},\ j=\overline{1,n},\ \ i=\overline{1,m},\ m,n\in\mathbb{N}, \right. \qquad (1)$$

связанных с идеей замены булевых задач на равносильные относительно булевых решений задачи в действительной области. Достоинством этого направления является возможность использования для анализа и решения булевых задач относительно хорошо разработанного математического аппарата в поле действительных чисел $\mathbb{R}$.

Указанное направление включает в себя широкую группу методов[1]. В настоящее время известны и изучаются методы, основанные на сведении булевых задач к задачам определения решений линейных и некоторых классов нелинейных систем уравнений и неравенств в поле действительных чисел, а также к задачам минимизации действительных функционалов. Наибольшее продвижение связано с использованием различных видов пороговых представлений булевых функций.

В ***параграфе 1.3*** проведен анализ и обобщение фундаментальных результатов Никонова В.Г.[2,3] в разработке метода разделяющих плоскостей и метода разделяющих поверхностей. В *пунктах 1.3.1, 1.3.2* доказана взаимосвязь метода разделяющих плоскостей с задачами пороговой логики и задачей покрытия графа, а таже показано, что в общем случае нахождение систем линейных неравенств, равносильных булевым равенствам, представляет сложную задачу пороговой логики, сводящуюся к исследованию геометрических свойств булевой функции в *n*-мерном пространстве. Для снижения реальной размерности решаемой задачи предложен метод фиксации части переменных, изложенный в *пункте 1.3.3. В пункте 1.3.4* проанализированы теоретические положения метода разделяющих поверхностей при его переносе в *k*-значную область.

Таким образом, в первой главе проведен анализ положений метода разделяющих плоскостей, направленного на сведение трудноформализуемых задач дискретной математики к решению равносильных систем линейных неравенств. Этот метод, детально разработанный для булевых задач, в определенных условиях, а именно для так называемых выпуклых функций и уравнений, применим в *k*-значной области. В центре внимания метода разделяющих плоскостей оказался класс пороговых функций, формально легко реализуемых, но обладающих целым рядом достаточно сложных свойств.

Вторая глава посвящена изучению и анализу метода эллипсоидов в алгоритме Хачияна и построению на его основе алгоритмов решения систем линейных неравенств с *k*-значными неизвестными. В ***параграфе 2.1*** проведен анализ концепции построения полиномиального алгоритма Хачияна. Хачияном Л.Г. рассматривалась задача решения системы из $m \geq 2$ линейных неравенств относительно $n \geq 2$ действительных неизвестных $x_1, x_2, ..., x_n$:

---

[1] Балакин Г.В, Никонов В.Г. Псевдобулево направление в дискретной математике // Обозрение прикл. промышл. матем. 2012. Т. 19. Вып. 6.

[2] Балакин Г.В., Никонов В.Г. Методы сведения булевых уравнений к системам пороговых соотношений // Обозрение прикл. промышл. матем. 1994. Т. 1. Вып. 3. С. 389–401.

[3] Никонов, В.Г. Пороговые представления булевых функций // Обозрение прикл. и промышл. Матем. 1994. Вып. 1. №3. С. 402-457.

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n \le b_1, \\ \quad ... \\ a_{m1}x_1 + ... + a_{mn}x_n \le b_m. \end{cases} \qquad (2)$$

с целыми коэффициентами a_{ij}, b_i, $i = \overline{1,m}$, $j = \overline{1,n}$.

Для системы (2) введено понятие длины входа системы

$$L = \left[\sum_{i,j=1}^{m,n} \log_2 (|a_{ij}| + 1) + \sum_{i=1}^{m} \log_2 (|b_i| + 1) + \log_2 mn \right] + 1. \qquad (3)$$

Величина L соответствует числу битов, необходимых для записи коэффициентов системы (2). Хачияном Л.Г. доказано, что если система линейных неравенств (2) совместна, то она имеет решения в гипершаре радиуса $R_{нач} = 2^L$, который в алгоритме Хачияна определен как начальная локализация области поиска решений[4]. Далее в алгоритме строится последовательность эллипсоидов, описанных вокруг полушаров в *n*-мерном пространстве. В процессе работы алгоритма на каждой итерации происходит движение центра эллипсоида к области решений, если она существует. Доказано, что через не более чем $w = 6n^2L$ итераций очередной центр эллипсоида либо оказывается решением системы (2), если система совместна, либо в случае несовместности системы (2), введенная автором невязка в центре текущего эллипсоида будет больше определенного порогового значения. Предложенный Хачияном Л.Г. алгоритм требует для своей работы память порядка $O(nm + n^2)$ чисел, каждое из которых имеет в двоичной записи с фиксированной запятой $O(L)$ разрядов. Над этими числами производится порядка $O(n^3(n+m)L)$ элементарных операций. Таким образом, Хачияном Л.Г. впервые доказано, что задача определения совместности систем линейных неравенств в $\mathbb{R}^n$ принадлежит к классу полиномиально разрешимых на детерминированных машинах Тьюринга задач.

В ***параграфе 2.2*** обобщены положения метода эллипсоидов, выделены необходимые процедуры для адаптации его применения в *k*-значной области. На базе проведенного анализа в ***параграфе 2.3*** построен адаптивный алгоритм эллипсоидов решения систем линейных неравенств с *k*-значными неизвестными, обоснована его сходимость и определены условия его применения.

Исследования показали, что значение $R_{нач}$ и величина w в исходном алгоритме Хачияна характеризуют его исключительно высокую сложность, а ожидаемое действительное (нецелочисленное) решение не позволяет

[4] Хачиян Л.Г. Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1979. Т. 244. №5. С. 1093-1096.

непосредственно применить этот алгоритм для решения систем линейных неравенств с дискретными неизвестными.

Устранение указанных недостатков в диссертации достигнуто путем построения нового алгоритма, основанного на идеях метода эллипсоидов Хачияна, в котором уточнена исходная локализация области решений и введены дополнительные критерии выхода.

В адаптивный алгоритм эллипсоидов в качестве модификации в сравнении с полиномиальным алгоритмом Хачияна введен дополнительный критерий выхода из алгоритма по пороговому значению невязки системы $\theta(x'_\nu) \le 0$. Значение x'_ν получается путем округления координат центра эллипсоида x_ν, полученного на ν-ой итерации работы алгоритма. Этот критерий является корректным, поскольку $\theta(x'_\nu) = \max_{i=1...m}\left\{A_i^T x'_\nu - b_i\right\}$ и, если $\theta(x'_\nu) \le 0,$ то очевидно, что все неравенства системы вида (2) выполняются и приближение центра очередного эллипсоида x'_ν попадает в многогранник решений системы (2). Если исходная система (2) несовместна, то выход по введенному критерию невозможен, поскольку коэффициент невязки будет положительным на всех w итерациях. Следовательно, данная модификация никак не повлияет на корректность работы всего алгоритма в целом и все леммы из ***параграфов 2.1, 2.2*** также будут верны. Целью адаптивного алгоритма является попадание в некоторую δ- окрестность точки, т.е. в область, где решение может быть локализовано за счет используемой в алгоритме методики перехода из действительной в *k*-значную область.

В адаптивном алгоритме эллипсоидов уточнена исходная локализация области поиска решений системы (2). Поскольку неизвестные x_j, $j = \overline{1,n}$ в системе (2) *k*-значные, т.е. $x_j \in \{0,1,...,k-1\}$, то в качестве исходного в алгоритме выбран гипершар радиуса $R'_0 = \dfrac{(k-1)\sqrt{n}}{2}$. Значение R'_0 определяется спецификой исходной задачи, когда все потенциальные решения системы (2) лежат в *n*-мерной *k*-звенной решетке V_k^n, которая вкладывается в гипершар указанного радиуса с центром в точке $x_0\left(\dfrac{k-1}{2},...,\dfrac{k-1}{2}\right)$. Исследование систем линейных неравенств с *k*-значными неизвестными, проведенное, в частности, в задаче восстановления линейной рекурренты по ее старшей координатной последовательности показало возможность потери решения си-

стемы в ходе работы алгоритма, если оно лежит на границе гиперсферы радиуса R_0'. Для случая $k=5$, $n=2$ в решетке V_5^2 граничные решения обозначены ◆ (см. Рисунок 1).

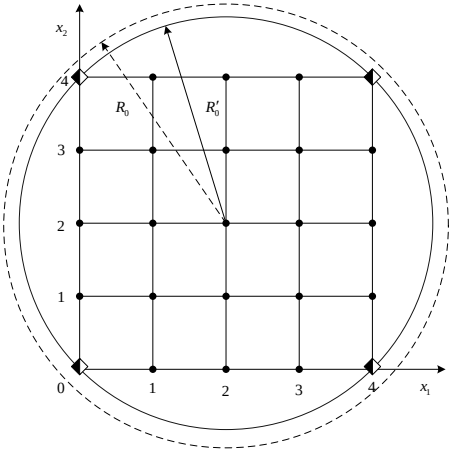

Рисунок 1 – Граничные решения в решетке V_5^2.

Для устранения этого недостатка в диссертации предложено на начальной итерации в качестве исходного радиуса вместо $R_0' = \frac{(k-1)\sqrt{n}}{2}$ использовать значение

$$R_0 = \left(\frac{(k-1)\sqrt{n}}{2}\right) \bullet \left(1 + \frac{1}{16n^2}\right), \qquad (4)$$

где значение коэффициента растяжения $\left(1 + \frac{1}{16n^2}\right)$ обоснованно взято из работы Хачияна Л.Г.[5]

Очевидно, что данное уточнение существенно не влияет на скорость сходимости адаптивного алгоритма эллипсоидов, но сводит к минимуму возможность потери граничных решений.

Далее факт попадания в область решений устанавливается при вычислении на текущей итерации ν невязок системы $\theta(x_\nu) \le 0$ и $\theta(x_\nu') \le 0$, и, наконец, система (2) будет иметь единственное целочисленное решение,

[5] Хачиян Л.Г. Полиномиальные алгоритмы в линейном программировании // ЖВМиМФ. 1980. Т.20. №1. С. 51-68

если вокруг области решений возможно описать гипершар радиуса $R < 0,5$. Целочисленный ответ получается непосредственным округлением координат центра текущего эллипсоида. Для адаптивного алгоритма эллипсоидов справедлива теорема.

Теорема 1. Если многогранник решений системы неравенств (2) с *k*-значными неизвестными целиком лежит внутри гипершара S радиуса $R < 0,5,$ то адаптивный алгоритм за полиномиальное время определит факт совместности либо несовместности системы и, в случае совместности, найдет единственное целочисленное решение.

Другие отличия адаптивного алгоритма от исходного алгоритма Хачияна, такие как уменьшение радиуса исходной локализации и дополнительные критерии выхода, приводят только к снижению оценки w и не влияют на сам факт ее полиномиального характера.

Дополнительные исследования в области применения метода эллипсоидов в задаче решения систем линейных неравенств с *k*-значными неизвестными позволили уточнить оценки величины максимального количества итераций на основе анализа структуры системы (2), а также сходимости алгоритма. Хачияном Л.Г. показано, что определитель матрицы B_ν характеризует объем задаваемого ей эллипсоида $\left|detB_\nu\right| \sim mes(E_\nu)$ [5]. Из логики алгоритма Хачияна вытекает, что если

$$\left|detB_\nu\right| \le d \qquad (5)$$

для некоторого d и невязка $\theta(x_\nu) \ge 2^{-L+1}$, то система несовместна. Специфика рассматриваемой задачи, когда ведется поиск *k*-значного решения, делает критерий несовместности системы на основании (5) предпочтительным в сравнении с предложенным Хачияном критерием несовместности по невязке системы. Таким образом, при выполнении условия (5) можно утверждать, что в ходе своей работы адаптивный алгоритм локализовал область возможных решений в гипершаре радиуса $R < 0,5$ и, следовательно, выполнены условия Теоремы 1 и, если решение системы (2) существует, то оно будет найдено путем округления, иначе можно утверждать о несовместности системы (2). В процессе проведения экспериментальных исследований при значениях $k \le 64$ параметр d был оценен как $d = 10^{-9}$ и при выполнении условия (5) наблюдалось практическое отсутствие движения центра эллипсоида x_ν на $\nu+1$ и последующих итерациях.

Еще одним дополнительным критерием выхода, ведущим к уточнению величины w в зависимости от области начальной локализации, может быть

использование оценки, полученной Хачияном Л.Г.[6] для алгоритма решения задачи выпуклого программирования:

$$w' = \frac{3}{2} n^2 L\left(\frac{8\tilde{d}^2 hNR^{\tilde{d}}}{\varepsilon} \right), \tag{6}$$

где n – количество неизвестных системы (6), $L(a) = \lfloor \log_2 a \rfloor + 1$ – число битов в двоичной записи числа a, $\tilde{d}$ – степень нелинейности полинома, задающего неравенства системы, h – максимальный по модулю коэффициент системы линейных неравенств, M_i – количество ненулевых коэффициентов i-го неравенства системы, $N = \max\{M_i\}$, $i = \overline{1,m}$, R – натуральная граница решений, а $\varepsilon \in (0,1)$ – требуемая точность задачи (для систем вида (2) достаточна точность $\varepsilon = 10^{-9}$). Очевидно, что для систем вида (2) с k-значными неизвестными оценка w' имеет вид:

$$w' = \frac{3}{2} n^2 \left(\left\lfloor \log_2 \left(\frac{10^9 8hN(k-1)}{l} \right) \right\rfloor + 1 \right), \tag{7}$$

поскольку для линейных неравенств степень нелинейности полинома $\tilde{d}$ равна 1, а натуральная граница решений R определяется логикой задачи k, где l – коэффициент пространственной декомпозиции, который для адаптивного алгоритма равен 1.

При определении несовместности (2) также выявлен признак несоблюдения леммы, доказательство которой приведено в докторской диссертации Хачияна Л.Г.[6], в которой утверждается, что

$$\frac{V^{\mathbb{R}^n}(E^{\nu+1})}{V^{\mathbb{R}^n}(E^{\nu})} = \left|\det B^{\nu+1}\right| / \left|\det B^{\nu}\right| \le 2^{-1/2n}. \tag{8}$$

Для некоторых типов систем линейных неравенств, в частности несовместных, наблюдается сначала убывание $\left|\det B^{\nu}\right|$, а затем его рост, что свидетельствует о необходимости остановки алгоритма. В дальнейшем завершение работы адаптивного алгоритма по невыполнению условия (8) будем называть критерием выхода по соотношению объемов. Невыполнение условия (8) не всегда свидетельствует о несовместности системы линейных неравенств. В частности, в ряде практических задач получены системы линейных неравенств, многогранник решений которых в действительной и k-значной области не пуст и совпадает, и, следовательно, единственное их

[6] Хачиян Л.Г. Сложность выпуклых задач вещественного и целочисленного полиномиального программирования: дисс. ... доктора физ.-мат. наук: 05.13.02. М., 1983. 252 с.

решение может быть найдено только при округлении. По этой причине полученное в результате работы адаптивного алгоритма эллипсоидов решение необходимо проверить на принадлежность к многограннику решений и только тогда можно утверждать о несовместности рассматриваемой системы неравенств. На практике установлено, что данный критерий дает значительный временной выигрыш при использовании как в адаптивном алгоритме, так и в построенном на его базе пространственно-декомпозиционном алгоритме (ПД-алгоритме), описанном в ***параграфе 2.4***. В основе ПД-алгоритма лежит геометрическое распараллеливание на базе пространственной декомпозиции области поиска решений, которая осуществляется за счет разбиения исходной *n*-мерной *k*-звенной решетки V_k^n на t областей $V_k^n(1), V_k^n(2), ..., V_k^n(t)$:

$$\bigcup_{q=1}^{t} V_n^k(q) = V_n^k, \tag{9}$$

где t – некоторый параметр, характеризующий количество потоков обработки, зависящее от вычислительной мощности ЭВМ. Каждый элемент пространственной декомпозиции $V_k^n(q)$ выбирается так, что он целиком вкладывается в некий гиперкуб с ребром b или целиком составляет этот гиперкуб, а затем погружается в соответствующий гипершар радиуса $R_0^{(q)}$:

$$V_n^k(q) \subset S_0^{(q)}, R_0^{(q)} < R_0. \tag{10}$$

Гипершары $S_0^{(1)}, S_0^{(2)}, ..., S_0^{(t)}$ рассматриваются как исходные области локализации для t ветвей метода эллипсоидов, а их радиусы $R_0^{(q)}$ равны между собой, поэтому в дальнейшем будем использовать обозначение $R_0^{(l)}$. Предлагаемая методика распараллеливания основана на разбиении (9) и локализации каждой из t областей внутри *n*-мерного шара радиуса $R_0^{(l)}$ с центром в точке $X_0(S_0^{(q)})$:

$$R_0^{(l)} = \frac{b\sqrt{n}}{2} \bullet \left(1 + \frac{1}{16n^2}\right), \tag{11}$$

где b – ребро гиперкуба, в который вкладывается элемент разбиения $V_n^k(q)$. Выбор параметров b и $R_0^{(l)}$ определяется видом разбиения (9), а увеличение $R_0^{(l)}$ в $\left(1 + \frac{1}{16n^2}\right)$ раз объясняется теми же причинами, что и для исходного адаптивного алгоритма эллипсоидов.

Рассмотрим естественное мозаичное разбиение V_k^n путем дробления каждого ребра на l частей, тогда

$$b = \frac{a}{l} \Rightarrow R_0'^{(l)} = \frac{a\sqrt{n}}{2l} \Rightarrow l = \frac{a\sqrt{n}}{2R_0'^{(l)}}. \qquad (12)$$

Отсюда получим, что общее количество элементов разбиения, а следовательно потоков, равно $t = l^n$. В дальнейшем коэффициент l будем называть коэффициентом пространственной декомпозиции. Каждый гипершар, содержащий элемент такого разбиения, имеет радиус $R_0^{(l)} = R_0'^{(l)} \bullet \left(1 + \frac{1}{16n^2}\right)$, и соответствующая стартовая задача метода эллипсоидов характеризуется матрицей $B_0 = diag(R_0^{(l)}, ..., R_0^{(l)})$ размерности $n \times n$. При этом отличаются центры гипершаров, каждый из которых совпадает с центром гиперкуба с ребром b разбиения $V_k^n(q)$. Очевидно, если каждое ребро длины a исходного гиперкуба, в который вкладывается *n*-мерная *k*-звенная решетка V_k^n, разбивается на l частей длины b, то координаты центров гиперкубов, в которые вкладывается элемент $V_k^n(q)$, имеют вид

$$X_0(S_0^{(q)}) = \left(\frac{b}{2} + h_1 b, ..., \frac{b}{2} + h_n b\right), \text{ где } h_j \in \{0, ..., h_{\max}\},\ j = \overline{1,n}. \qquad (13)$$

Значение $h_{\max}$, при котором центр гипершара не выходит за рамки решетки V_n^k, вычисляется из неравенства $\frac{b}{2} + h_{\max} b < a$, следовательно $h_{\max} = [l - 0{,}5]$, где $[]$ –взятие целой части.

После того как вычислены параметры инициализации работы, адаптивный алгоритм запускается в каждом из потоков до первого успешного завершения. Успешным считается завершение потока, при котором найдено решение системы (2), а неудачным – при котором решение системы (2) не найдено.

Приведем формальное описание ПД-алгоритма решения систем линейных неравенств с *k*-значными неизвестными.

1 Этап. Инициализация.

1.1. Инициализация коэффициента пространственной декомпозиции l и начальных параметров адаптивного алгоритма: матрицы коэффициентов A, вектора свободных членов b, k – значности логики, начального

радиуса $R_0^{(l)} = \frac{b\sqrt{n}}{2} \bullet \left(1 + \frac{1}{16n^2}\right)$, длины входа L, оценок максимального количества итераций работы алгоритма $w = 6n^2 L$,

$w' = \frac{3}{2} n^2 \left(\left\lfloor \log_2 \left(\frac{10^9 8hN(k-1)}{l} \right) \right\rfloor + 1 \right)$ и критериев выхода из алгоритма.

1.2. Инициализация n-мерных гипершаров $S_0^{(q)}$, $q = \overline{1,t}$, начальной итерации с параметрами $X_0(S_0^{(q)}) = \left(\frac{b}{2} + h_1 b, ..., \frac{b}{2} + h_n b \right)$, где $h_j \in \{0, ..., h_{\max}\}$, $j = \overline{1,n}$, $h_{\max} = [l - 0,5]$ и $B_0 = diag\left(R_0^{(l)}, \ldots, R_0^{(l)}\right)$.

2 Этап. Поиск решения или доказательство несовместности системы $A\bar{X} \le b$ *в каждой из областей пространственной декомпозиции* $V_k^n(q)$.

2.1. В каждом из t потоков (в зависимости от мощности ЭВМ одновременно или группами по $\beta \ge 2$ штук) запускаем копию адаптивного алгоритма эллипсоидов.

2.2. При $q \le t$ инициализируем новую копию адаптивного алгоритма, иначе 2.7.

2.3. Работа адаптивного алгоритма в q-ом потоке.

2.3.1. Вычисление невязок системы линейных неравенств и невязки алгоритма на ν-ой итерации по формулам $\theta(T) = \max_{i=1...m} \left\{ A_i T - b_i \right\}$, где $T \in \left\{ X_\nu^{(q)}, X_\nu'^{(q)} \right\}$, и $\theta_\nu = \min\left(\theta_{\nu-1}, \theta\left(X_{\nu-1}^{(q)}\right)\right)$.

2.3.2. Проверка выполнения критериев выхода.

2.3.2.1. Критерий выхода по отрицательной невязке системы линейных неравенств в центре эллипсоида $\theta\left(X_\nu'^{(q)}\right)$.

2.3.2.2. Нулевое значение вектора $\eta_\nu = B_\nu^T A_{i_\nu}^T$, что означает вырожденность матрицы эллипсоида B_ν.

2.3.2.3. Проверка условия $\left|\det B_\nu\right| \le 10^{-9}$.

2.3.2.4. Проверка условия $\left|\det B^\nu\right| / \left|\det B^{\nu-1}\right| > 2^{-1/2n}$.

2.3.2.5. Выполнение $\nu \ge w'$ итераций.

2.3.2.6. Выполнение $\nu > w$ итераций.

Если критерий сработал, перейти на шаг 2.4, иначе – 2.3.3.

2.3.3. Инициализация параметров нового эллипсоида

$\eta_\nu = B_\nu^T A_{i_\nu}^T$, где $i_\nu = \arg\max_{i=1...m} \left\{ A_i X_\nu^{(q)} - b_i \right\}$, матрицы

$$\tilde{\eta}_\nu = \begin{pmatrix} \eta_1\eta_1 & \dots & \eta_1\eta_n \\ \dots & \dots & \dots \\ \eta_n\eta_1 & \dots & \eta_n\eta_n \end{pmatrix}.$$

Вычисление параметров нового эллипсоида

$$X_\nu^{(q)} \approx X_{\nu-1}^{(q)} - \frac{B_{\nu-1}\eta_{\nu-1}}{(n+1)\|\eta_{\nu-1}\|}$$ и

$$B_\nu \approx \left(1+\frac{1}{16n^2}\right)\frac{n}{\sqrt{(n^2-1)}}\left\{ B_{\nu-1}\left[\sqrt{\left(\frac{n-1}{n+1}\right)}-1\right]\frac{B_{\nu-1}\tilde{\eta}_{\nu-1}}{\|\eta_\nu\|^2}\right\}.$$

Перейти к шагу 2.3.1.

2.4. Выход из алгоритма: вектор решений $X_{вых}^{(q)} = (x_1, x_2, \dots, x_n)$, полученный в результате перехода от действительного к локализованному в эллипсоиде последней итерации *k*-значному решению.

2.5. Проверка полученного решения $X_{вых}^{(q)} = (x_1, x_2, \dots, x_n)$. Если $X_{вых}^{(q)}$ – решение системы $A\bar{X} \le b$, то перейти на шаг 2.6, иначе перейти к – 2.2 и инициализировать новый поток.

2.6. Прерывание работы всех копий адаптивного алгоритма, вывод полученного решение $X_{вых}^{(q)}$ на экран. Перейти к шагу 2.8.

2.7. Вывести сообщение о том, что система $A\bar{X} \le b$ – несовместна. Перейти к шагу 2.8.

2.8. Завершение работы.

Помимо распараллеливания показана возможность применения ПД-алгоритма для исследования систем линейных неравенств с многогранниками решений сложной формы. В этом случае результаты работы каждого из потоков могут быть использованы как реперные точки для локализации области решений с последующим переходом к направленному перебору.

В ***параграфе 2.5*** проведено сравнение параметров работы построенных алгоритмов с альтернативными методами решения систем линейных неравенств с *k*-значными неизвестными. Особое внимание уделено сравнению с эвристическими алгоритмами, которое осуществлено на модели случайных систем. Для решения построенных в результате моделирования случайных систем линейных неравенств с *k*-значными неизвестными применены разработанные алгоритмы. На основании проведенных исследований сделан вывод об их надежности. Адаптивный алгоритм эллипсоидов решил все сгенерированные в ходе эксперимента системы неравенств при количестве

неизвестных $n \le 10^2$ и числе неравенств $m \le 10^3$, что значительно превосходит результаты эвристических алгоритмов, полученные в работах Анашкиной Н.В. и Шурупова А.Н.[7,8] Сравнение для *k*-значного случая осуществлялось с градиентным алгоритмом, предложенным Никоновым В.Г.[9], который является развитием алгоритма Балаша для частного случая структурных систем. Проведенные экспериментальные исследования позволили утверждать о высокой надежности адаптивного алгоритма эллипсоидов в задаче решения случайных систем линейных неравенств с *k*-значными неизвестными. Для всех рассмотренных примеров адаптивный алгоритм эллипсоидов в 100% случаев нашел решение, но из-за конкретного строения многогранника решений оно в отдельных случаях не совпадало с эталонным. Данный фактор не является слабой стороной алгоритма, поскольку в большинстве практических задач информационной безопасности получаемая в результате анализа узлов защиты информации система неравенств имеет единственное дискретное решение.

В целом **вторая глава** посвящена проблеме решения систем линейных неравенств в действительной и дискретной областях. Основным результатом главы является разработанный на базе метода эллипсоидов Хачияна адаптивный алгоритм решения систем линейных неравенств, позволяющий находить дискретные решения. К числу новых результатов также относится предложенный в главе пространственно-декомпозиционный алгоритм, основанный на геометрическом распараллеливании, который направлен на сокращение временной сложности адаптивного алгоритма. С теоретической точки зрения важно отметить строго доказанную теорему о строении систем неравенств, для которых задача поиска дискретных решений имеет полиномиальную сложность.

В **третьей главе** рассмотрено применение разработанных алгоритмов в прикладных задачах анализа узлов защиты информации и дискретной математики. ***В параграфе 3.1*** проведен обзор основных направлений применения генераторов ПСП в современных системах обеспечения информационной безопасности, показана их определяющая роль в задачах:

— формирования паролей пользователей в системах разграничения доступа;

— генерации ПСП в узлах с защитными преобразованиями на базе бинарного сумматора;

---

[7] Анашкина Н.В., Шурупов А.Н. Экспериментальное сравнение алгоритмов Балаша и имитации отжига в задаче решения систем линейных неравенств // ПДМ. Приложения. 2014. вып. 7. С. 151-153.

[8] Анашкина Н.В., Шурупов А.Н. Применение алгоритмов локального поиска к решению систем псевдобулевых неравенств // ПДМ. Приложения. 2015. вып. 8. С. 136-138.

[9] Никонов В.Г., Ситников П.Н. Градиентный алгоритм решения систем линейных неравенств с k-значными неизвестными // Вестник МГУЛ «Лесной вестник». 2008. №2. С. 115-120.

– формирования прекурсоров и затемняющих множителей в протоколах слепой электронной подписи;

– внесения неопределенности в работу средств и объектов защиты;

– построения полностью автоматического публичного теста Тьюринга.

В ***параграфе 3.2*** рассмотрена задача изучения запретов и полузапретов булевых и *k*-значных функций. Разработанные алгоритмы применены для доказательства принадлежности комбинации знаков выходной последовательности, вырабатываемых фильтрующим генератором, к одному из обозначенных классов. В завершении параграфа отмечено, что сведение систем уравнений сдвигового типа к системам линейных неравенств позволило с новых позиций оценить проблему изучения запретов и полузапретов дискретных функций. Возможность такого сведения повышает актуальность применения известных и разработки новых алгоритмов проверки совместности и нахождения дискретных решений систем линейных неравенств, в частности, адаптивного алгоритма эллипсоидов, предложенного в данной работе. Если для нахождения дискретных решений систем линейных неравенств могут быть использованы различные эвристические методы, то доказательство несовместности с помощью адаптивного алгоритма представляется, по-видимому, единственным возможным с заведомо определенной оценкой сложности.

В ***параграфе 3.3*** разработанные алгоритмы использованы в задачах анализа биективных отображений с помощью систем линейных неравенств в *k*-значной области. В этом случае адаптивный алгоритм может быть применен для решения следующих задач:

1. Нахождение входного вектора $\overline{X}$ по известному выходному вектору $\overline{Y}$ и известной системе линейных неравенств, задающей биекцию.
2. Определение параметров подстановки Π по набору знаков входа-выхода $(\overline{x_1}, \overline{y_1}), ..., (\overline{x_t}, \overline{y_t})$.
3. Доказательство того, что заданное отображение – биекция.

Показано, что все приведенные задачи сводятся к решению систем линейных неравенств с *k*-значными неизвестными, для которых решение определялось с помощью адаптивного алгоритма эллипсоидов.

В ***параграфе 3.4*** адаптивный алгоритм эллипсоидов применен при анализе ряда типовых узлов защиты информации. В *пункте 3.4.1* рассмотрена задача восстановления начального состояния комбинирующего генератора с каскадом кольцевых регистров на входе (см. Рисунок 2).

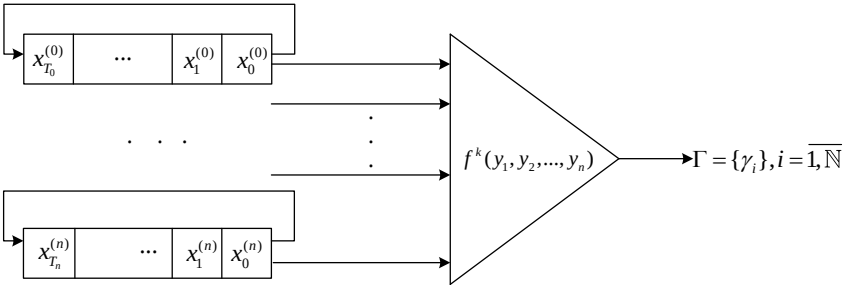

Рисунок 2 – Комбинирующий генератор с пороговой функцией усложнения и каскадом кольцевых регистров на входе.

В *пункте 3.4.2* исследована задача нахождения начального состояния стационарного регистра без обратной связи (см. Рисунок 3) с заданным правилом подачи переменных данных на функцию усложнения.

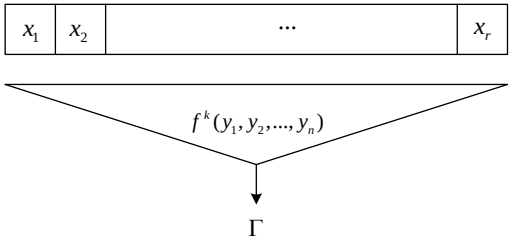

Рисунок 3 – Общая схема узла защиты информации на базе стационарного регистра с пороговой функцией усложнения.

В параграфе показана возможность сведения данных задач к системам линейных неравенств с *k*-значными неизвестными, для решения которых применены разработанные алгоритмы.

В ***параграфе 3.5*** на базе разработанных алгоритмов и результатов Никонова В.Г. и других авторов построен полиэдральный метод решения задачи восстановления линейной рекурренты, реализованной линейным регистром сдвига с трехчленным законом обратной связи, по подряд идущим знакам ее старшей координатной последовательности (см. Рисунок 4).

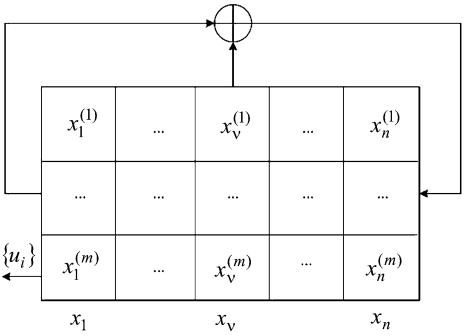

Рисунок 4 – Обобщенная схема ЛРС с трехчленным законом обратной связи, реализующего ЛРП над кольцом $\mathbb{Z}_{2^m}$.

Специфика решаемой задачи позволяет применить адаптивный алгоритм эллипсоидов в прямом исполнении. Рассмотрим этапы применения полиэдрального метода.

1 Этап. Формирование системы линейных неравенств с k-значными неизвестными.

1.1.Построение на основе старшей координатной последовательности $\{u_l\}$ последовательности знаков переноса $\{c_l\}$, исходя из соотношения

$$\begin{cases} c_i = 0, \text{если } u_i = u_{i-n} \oplus u_{i-n+v}, \\ c_i = 1, \text{если } u_i \neq u_{i-n} \oplus u_{i-n+v}, \end{cases} \quad i = \overline{n+1, I},$$

где I – длина последовательности знаков старшего разряда.

1.2. Формирование неравенств из уточненных оценок за счет знаков переноса в старший разряд c_i при известных ограничениях для порождающих элементов.

1.3. Приведение полученных на шаге 1.2 неравенств к виду $A\bar{X} \le b$, где $\bar{X}$ – вектор неизвестных, A – матрица коэффициентов системы, b – вектор свободных членов.

2 Этап. Решение системы линейных неравенств с k-значными неизвестными вида $A\bar{X} \le b$.

2.1. Инициализация начальных параметров адаптивного алгоритма: матрицы коэффициентов A, вектора свободных членов b, начального гипершара области локализации решений радиуса $R_0 = \dfrac{(k-1)\sqrt{n}}{2} \bullet \left(1 + \dfrac{1}{16n^2}\right)$,

длины входа L, оценок максимального количества итераций работы алгоритма $w = 6n^2L$, $w' = \frac{3}{2}n^2\left(\left\lfloor \log_2\left(10^9 8hN(k-1)\right)\right\rfloor + 1\right)$ и критериев выхода из алгоритма.

2.2. Инициализация гипершара начальной итерации с параметрами $x_0\left(\frac{k-1}{2},...,\frac{k-1}{2}\right)$ и $B_0 = diag\left(R_0,\ldots,R_0\right)$.

2.3. Вычисление невязок системы линейных неравенств и невязки алгоритма на ν-ой итерации по формулам $\theta(T) = \max_{i=1...m^*}\left\{A_i T - b_i\right\}$, где $T \in \left\{x_\nu, x'_\nu\right\}$, $\theta_\nu = \min(\theta_{\nu-1}, \theta(x_{\nu-1}))$, m^* – количество неравенств системы.

2.4. Проверка выполнения критериев выхода.

Опишем основные критерии выхода из алгоритма.

2.4.1. Критерий выхода по отрицательной невязке системы линейных неравенств в центре эллипсоида $\theta\left(x'_\nu\right)$.

2.4.2. Нулевое значение вектора $\eta_\nu = B_\nu^T A_{i_\nu}^T$, что означает вырожденность матрицы эллипсоида B_ν.

2.4.3. Проверка условия $\left|\det B_\nu\right| \le 10^{-9}$.

2.4.4. Проверка условия $\left|\det B^\nu\right| / \left|\det B^{\nu-1}\right| > 2^{-1/2n}$.

2.4.5. Выполнение $\nu \ge w'$ итераций.

2.4.6. Выполнение $\nu > w$ итераций.

Если критерий, сработал перейти на шаг 2.6, иначе – 2.5.

2.5. Инициализация параметров нового эллипсоида

$\eta_\nu = B_\nu^T A_{i_\nu}^T$, где $i_\nu = \arg\max_{i=1...m^*}\left\{A_i x_\nu - b_i\right\}$, матрицы

$$\tilde{\eta}_\nu = \begin{pmatrix} \eta_1\eta_1 & \ldots & \eta_1\eta_n \\ \ldots & \ldots & \ldots \\ \eta_n\eta_1 & \ldots & \eta_n\eta_n \end{pmatrix}.$$

Вычисление параметров нового эллипсоида

$$x_\nu \approx x_{\nu-1} - \frac{B_{\nu-1}\eta_{\nu-1}}{(n+1)\|\eta_{\nu-1}\|} \quad \text{и}$$

$$B_\nu \approx \left(1+\frac{1}{16n^2}\right)\frac{n}{\sqrt{(n^2-1)}}\left\{B_{\nu-1}\left[\sqrt{\left(\frac{n-1}{n+1}\right)}-1\right]\frac{B_{\nu-1}\tilde{\eta}_{\nu-1}}{\|\eta_\nu\|^2}\right\}.$$

Перейти к шагу 2.3.

2.6. Выход из алгоритма: вектор решений $(x_1, x_2, \ldots, x_n)$, полученный в результате перехода от действительного к локализованному в эллипсоиде последней итерации *k*-значному решению.

2.7. Завершение работы.

Для данной задачи приведены эмпирические результаты, на основании которых получена аппроксимирующая функция, характеризующая верхнюю оценку расстояния единственности задачи

$$l = 1,7(m-1)n(\ln(0,46(m-1)n)), \qquad (14)$$

которая экспериментально подтверждена при росте n и m ($n \in \{5,8,16,32\}$, $m \in \{3,4,5,6\}$).

В ***параграфе 3.6*** проведено исследование возможности применения метода эллипсоидов для распознавания и нахождения аналитического задания пороговой *k*-значной функции, на основе которого показан способ сведения задачи характеризации к решению систем неравенств с действительными неизвестными, и построен алгоритм характеризации пороговых функций на базе модифицированного метода эллипсоидов Хачияна, что позволило доказать в общем случае полиномиальную сложность этой задачи. В конце параграфа осуществлено сравнение параметров разработанного алгоритма и геометрического метода Бурделева А.В.[10] Проведенные эксперименты показали, что каждый из рассмотренных алгоритмов обладает своей сферой предпочтительного применения. Установлено, что значительно отличается характер роста сложности геометрического алгоритма и модифицированного метода эллипсоидов в зависимости от *n* и *k*, причем при увеличении k сложность геометрического алгоритма растет значительно быстрее, чем сложность метода эллипсоидов. К числу преимуществ метода эллипсоидов также относится его общая полиномиальная сложность с заведомо известной оценкой сложности как алгоритма в целом, так и одной итерации в частности.

[10] Бурделев А.В., Никонов В.Г. О новом алгоритме характеризации k-значных пороговых функций // Comp. nanotechnol. 2017. Вып. 1. С. 7–14.

В то же время преимущества геометрического метода связаны с заведомо целочисленными значениями коэффициентов, доказанной сходимостью и возможностью нахождения для некоторых классов функций порогового представления за одну итерацию.

Очевидным недостатком геометрического алгоритма является отсутствие общей оценки сложности, обнаруженная тенденция к росту модулей коэффициентов с увеличением числа итераций и отсутствие детерминированного доказательства непороговости функции.

На основе проведенного анализа двух алгоритмов построен комбинированный алгоритм характеризации *k*-значных пороговых функций, сочетающий положительные стороны каждого из двух рассмотренных. Способность геометрического алгоритма быстро находить приближение параметров пороговой функции предложено использовать в методе эллипсоидов, рассматривая вектор, состоящий из этих параметров в качестве стартовой точки.

Практические эксперименты показали, что использование первых приближений геометрического алгоритма в качестве стартовой точки для метода эллипсоидов в случае, если функция имеет пороговое представление, значительно сокращает количество итераций в методе эллипсоидов, а в случае, если функция не имеет порогового представления, модифицированный метод эллипсоидов за известное число итераций покажет отсутствие такого представления.

В **приложениях** приведены акты о внедрении результатов исследования, свидетельства о регистрации программ для ЭВМ, описание состава и функциональных возможностей программных продуктов, созданных в процессе работы над диссертацией.

В **заключении** подведены итоги исследования, сформулированы основные теоретические и прикладные результаты, предложены направления дальнейших исследований по данной тематике.

СПИСОК ОСНОВЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

[1]. Лапиков, И.И. Адаптивный алгоритм решения систем линейных неравенств с k-значными неизвестными / И.И. Лапиков, В.Г. Никонов // Труды Военно-космической академии им. А.Ф. Можайского. – 2016. – №650. – С. 88-94.

[2]. Лапиков, И.И. О возможности геометрического распараллеливания адаптивного алгоритма решения систем неравенств с k-значными неизвестными на базе метода эллипсоидов Хачияна // Системы управления и информационные технологии. – 2016. – №2. – С. 14-19.

[3]. Лапиков, И.И. Распознавание параметров узла защиты информации, реализованного пороговой k-значной функцией / А.В. Бурделев, В.Г. Никонов, И.И. Лапиков // Труды СПИИРАН. – 2016. – №3 (46). – С. 108-127.

[4]. Лапиков, И.И. Сравнительный анализ геометрического метода и модифицированного метода эллипсоидов в задаче распознавания параметров k-значной пороговой функции / И.И. Лапиков, А.В. Бурделев // Интернет-журнал «НАУКОВЕДЕНИЕ». – 2017. – Т. 9, №6. Режим доступа: https://naukovedenie.ru/PDF/53TVN617.pdf

[5]. Лапиков, И.И. Применение адаптивного алгоритма эллипсоидов для изучения запретов булевых и k-значных функций / И.И. Лапиков, В.Г. Никонов, Н.В. Никонов // XXI век: итоги прошлого и проблемы настоящего плюс. – 2018. – №7(41). – С. 11-17.

[6]. Лапиков, И.И. О возможности построения пространственно-декомпозиционного алгоритма на базе геометрического распараллеливания адаптивного алгоритма эллипсоидов // Computational nanotechnology. – 2018. – Вып. 1. – С. 140-145.

[7]. Лапиков, И.И. Полиэдральный метод восстановления линейной рекурренты по ее старшей координатной последовательности / И.И. Лапиков // Вестник компьютерных и информационных технологий. – 2018. – №8. – С. 46-56.

[8]. Лапиков, И.И. О возможности применения метода эллипсоидов для распознавания пороговых функций / И.И. Лапиков // ПДМ. Приложения. – 2017. – №10. – С. 163-165.

[9]. Лапиков, И.И. О построении алгоритма, основанного на методе эллипсоидов Хачияна Л.Г., для решения систем неравенств с k-значными неизвестными / И.И. Лапиков, В.Г. Никонов // Информационные технологии в науке, образовании и управлении: труды международной конференции IT+S&E' 15 под ред. проф. Е.Л. Глориозова. – М.: ИНИТ. – 2015. – С. 262-264.

[10]. Лапиков, И.И. О возможности применения адаптивного алгоритма эллипсоидов для нахождения начального состояния комбинирующего генератора с каскадом кольцевых регистров на входе // Материалы XI Всероссийской научной конференции ученых, специалистов и профессорско-преподавательского состава «Территориальные распределенные системы охраны». – 2018. – С.361-367.

[11]. Свидетельство о государственной регистрации программы для ЭВМ №2018617222. Российская Федерация. Программа, реализующая адаптивный алгоритм эллипсоидов решения систем линейных неравенств с k-значными неизвестными и его модификации / И.И. Лапиков; заявитель и правообладатель Лапиков Игорь Игоревич. – №2018614127; заявка 18.04.2018; зарегистр. 21.06.2018; опубл. 21.06.2018, Бюл. № 7. – 1 с.

[12]. Свидетельство о государственной регистрации программы для ЭВМ №2018616595. Российская Федерация. Практические приложения адаптивного алгоритма эллипсоидов в задачах информационной безопасности, сводящихся к решению систем неравенств с k-значными неизвестными / И.И. Лапиков; заявитель и правообладатель Лапиков Игорь Игоревич. – №2018614143; заявка 18.04.2018; зарегистр. 04.06.2018; опубл. 04.06.2018, Бюл. № 6. – 1 с.