Московский Государственный Университет
имени М. В. Ломоносова
Механико-математический факультет

На правах рукописи
УДК 519.722

Ярыкина Мария Сергеевна

О НЕСУЩЕСТВОВАНИИ ДВОИЧНЫХ КОДОВ ПРИ РАЗЛИЧНЫХ УСЛОВИЯХ РАВНОМЕРНОЙ РАСПРЕДЕЛЕННОСТИ

(01.01.09 — дискретная математика и математическая кибернетика)

А В Т О Р Е Ф Е Р А Т
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва 2008

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

Научный руководитель: кандидат физико-математических наук, доцент Ю. В. Таранников

Официальные оппоненты: доктор физико-математических наук В. М. Блиновский, Институт проблем передачи информации имени А. А. Харкевича РАН

доктор физико-математических наук, профессор А. А. Сапоженко, Московский государственный университет имени М. В. Ломоносова

Ведущая организация: Институт математики имени С. Л. Соболева СО РАН.

Защита диссертации состоится 17 октября 2008г. в 16 часов 40 минут на заседании диссертационного совета Д.501.001.84 при Московском государственном университете имени М. В. Ломоносова по адресу: Российская федерация, 119991, Москва, ГСП-1, Ленинские горы, д. 1, Московский государственный университет имени М. В. Ломоносова, Механико-математический факультет, аудитория 14–08.

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

Автореферат разослан 17 сентября 2008 г.

Ученый секретарь диссертационного совета Д.501.001.84 при МГУ, доктор физико-математических наук, профессор — А. О. Иванов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы

Диссертация является исследованием в области теории кодирования.

Одной из важных задач теории кодирования является задача построения кодов для шифрования данных с целью сохранения секретности информации. С ростом производительности компьютеров и появлением новых алгоритмов декодирования требуются новые алгоритмы с лучшими параметрами. Для построения эффективных алгоритмов шифрования нужны булевы функции с определенными свойствами: уравновешенность, корреляционная иммунность, нелинейность, алгебраическая степень и т. д.

Рассмотрим кодирование с помощью поточного шифратора, использующего регистр сдвига с линейной обратной связью (LFSR). Шифрование с использованием одно лишь LFSR не обеспечивает достаточной секретности шифрования. Одним из более надёжных является алгоритм, в котором на вход некоторой булевой функции f от t переменных подаются выходы t различных LFSR — нелинейный комбинатор. Используемая булева функция f должна быть уравновешенной (т. е. число единичных значений должно быть равно числу нулевых значений), а также иметь максимальную алгебраическую степень и нелинейность.

Зигенталер[1] предложил алгоритм дешифрования указанной выше комбинации LFSR, используя корреляцию выхода функции f и некоторого подмножества ее входных переменных, и ввел понятие *корреляционно-иммунной функции*. Булева функция f называется корреляционно-иммунной порядка m, где $1 \leqslant m \leqslant n$, если выход функции f и любое множество из m входных переменных статистически независимы. Другими словами, если вес любой подфункции f' функции f от $n-m$ переменных удовлетворяет условию: $wt(f') = wt(f)/2^m$. Уравновешенная корреляционно-иммунная порядка m функция называется *m-устойчивой*. Для использования функции f в качестве нелинейного комбинатора нескольких LFSR нужно, чтобы она была m-устойчивой с максимально возможным m.

Как видно из определения, корреляционно-иммунные функции являются равномерно распределенными по подкубам, т.е. веса всех подкубов

[1] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Transactions on Information theory, V. IT-30, № 5, 1984, pp. 776–780.

определенной размерности одинаковы и вес любого подкуба размерности t равен $\frac{wt(f)}{2^n} \cdot 2^t$ при $n - m \leqslant t \leqslant n$. Корреляционно-иммунная функция порядка $n-1$ является равномерно распределенной по всем подкубам размерности от 1 до n. Более общий случай равномерного распределения по подкубам — это *l-уравновешенные* функции, т. е. функции, у которых для любых подфункций f_1 и f_2 от одинакового числа переменных выполнено неравенство $|wt(f_1) - wt(f_2)| \leqslant l$. В отличие от корреляционно-иммунных функций, которые равномерно распределены по подкубам размерности от $n-m$ до n, l-уравновешенные функции должны быть равномерно распределены по подкубам всех размерностей одновременно. Таранниковым Ю. В. исследованы 1-уравновешенные[2] и l-уравновешенные[3] булевы функции.

Также интерес представляет и исследование булевых функций, равномерно распределенных по шарам. Функции, двоичные наборы которых равномерно распределены по шарам, могут иметь некоторые полезные приложения. Например, такие функции можно использовать для построения хеширующей функции. Также такие коды полезны когда нам нужно, чтобы все слова на выходе связи имели примерно одинаковую вероятность декодирования. В частности, при декодировании списком некоторой длины l. Кроме того, неравномерность распределения по шарам может быть использована в атаках на шифраторы.

Булева функция f называется *равномерно распределенной со степенью 1 по шарам*[4] (1-РРШ), если для каждого радиуса r максимальный вес шара радиуса r и минимальный вес шара радиуса r (из всех 2^n шаров радиуса r в булевом кубе размерности n) отличаются не более, чем на единицу. Весом шара мы называем количество единичных значений функции в шаре, в качестве расстояния используем расстояние Хемминга. В работе[4] полностью описаны все 1-РРШ функции и получено, что при $n \geqslant 7$ вес любой 1-РРШ функции либо не превосходит 2, либо не менее $2^n - 2$. В диссертации рассматривается вопрос существования кодов, равномерно распределённых по шарам со степенью l, где l — произвольное натуральное число.

---

[2]Тарапников Ю. В. Класс 1-уравновешенных функций и сложность его реализации // Вестник Московского Университета. Серия 1. Математика. Механика. 1991. № 2, с. 83–85.

[3]Тарапников Ю. В. О некоторых оценках для веса l-уравновешенных булевых функций. // Дискретный анализ и исследование операций, 1995, Т. 2, № 4, с. 80–96.

[4]Тарапников Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1. // Вестник Московского Университета. Серия 1. Математика. Механика. 1997, вып. 52, №5, стр. 18–22.

В теории кодирования при решении задач списочного декодирования используются коды, являющиеся l-упаковками. Двоичный код C является *l-упаковкой* радиуса R, если в любой шар радиуса R попадает не более чем l кодовых слов. Точная асимптотическая оценка мощности l-упаковки в зависимости от ее радиуса $R = \tau n$ получена Блиновским В. М.[5]. В теории списочного декодирования принято оценивать не саму мощность кода m, а величину $A(m) = (\log_2 m)/n$. В работе[5] при больших τ величина $A(m)$ равна $o(1)$, а в диссертации автором получена явная оценка $m(\tau)$, которая согласуется с этим результатом и уточняет его.

Корреляционно-иммунные функции очень полезны в теории кодирования. Большой интерес представляет построение корреляционно-иммунных функций с максимальной нелинейностью, и, желательно, с максимальной алгебраической степенью.

Корреляционная иммунность функции и ее алгебраическая степень являются противоречащими друг другу свойствами: в силу *неравенства Зигенталера* алгебраическая степень корреляционно-иммунной порядка m функции f от n переменных удовлетворяет неравенству $deg(f) \leqslant n - m - 1$. Нелинейность булевой функции и ее корреляционная иммунность также являются противоречащими друг другу свойствами. Нелинейность произвольной булевой функции не превосходит[6] $2^{n-1} - 2^{n/2-1}$. В 2000 году было независимо доказано[7, 8, 9], что нелинейность m-устойчивой функции от n переменных не превосходит $2^{n-1} - 2^{m+1}$ при $m \leqslant n-1$. Причем если эта граница достигается, то $m > 0.5n - 2$.

Таранниковым Ю. В. предложен[10, 11, 12] метод построения таких функ-

---

[5]Блиновский В. М. Границы для кодов при декодировании списком конечного объема. Проблемы передачи информации. 1986. Том 22, № 1, стр. 11–25.

[6]Мак-Вильямс Ф. Дж. Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

[7]Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions // In Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science, V. 1880, 2000, pp. 515–532.

[8]Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity, // Proceedings of Indocrypt 2000, Lecture Notes in Computer Science,V. 1977, pp. 19–30, Springer-Verlag, 2000.

[9]Zheng Y. , Zhang X. M. Improved upper bound on the nonlinearity of high order correlation immune functions.// Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science, Springer-Verlag, 2001, V. 2012, pp. 264–274.

[10]Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях. Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 91–148

[11]Tarannikov Yu. New constructions of resilient Boolean functions with maximal nonlinearity // Fast Software Encryption. 8th International Workshop, FSE 2001 Yokohama, Japan, April 2–4, 2001. Revised Papers, Lecture Notes in Computer Science, V. 2355, 2002, pp. 66–77.

[12]Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Springer-Verlag, 2001, V. 2247, pp. 254–266.

ций с помощью подходящих матриц. Понятие *подходящей* (k_0, k, p, t)-матрицы вводится Таранниковым Ю. В.[11] Требуется построить такую подходящую матрицу, чтобы соотношение $\frac{t}{t+k}$ было минимально. В данной работе доказывается нижняя оценка для этого соотношения параметров.

Цель работы

Целью работы является изучение вопросов существования двоичных кодов, равномерно распределенных по шарам и оценка одного важного параметра матриц специального вида.

Научная новизна работы

Результаты работы являются новыми. В диссертации получены следующие основные результаты:

1. Доказано несуществование кодов, равномерно распределенных со степенью l по шарам для почти всех значений их мощности в булевых кубах достаточно большой размерности n.

2. Для одного поддиапазона мощности кода получена явная оценка значения размерности n, начиная с которой не существует кодов, равномерно распределенных со степенью l по шарам.

3. Получена явная верхняя оценка мощности l-упаковки большого радиуса ($R > n/4$) в зависимости от параметра $\tau = R/n$.

4. Получена явная точная оценка параметра матриц специального вида. С помощью таких матриц построены[12] корреляционно-иммунные функции порядка $m > 0.5902... \cdot n + O(\log_2 n)$ с максимальной нелинейностью.

Методы исследования

В работе используются методы теории кодирования, теории булевых функций, комбинаторного анализа и математического анализа.

Теоретическая и практическая ценность

Диссертация носит теоретический характер. Результаты диссертации могут найти применение в теории кодирования и теории булевых функций.

Апробация работы

Результаты диссертации докладывались на следующих научно-исследовательских семинарах и конференциях:

- Семинар «Синтез и сложность управляющих систем» под руководством О. Б. Лупанова (2003)
- Семинар «Булевы функции в криптологии» под руководством О. А. Логачева и Ю. В. Таранникова на мех-мат факультете МГУ (март 2007).
- Семинар под руководством Л. А. Бассалыго в ИППИ РАН (май 2008).
- Семинар под руководством А. А. Сапоженко на ВМиК факультете МГУ (май 2008).
- Международная конференция «NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security» (Звенигород, сентябрь 2007)
- IX международный семинар «Дискретная математика и ее приложения», посвященный 75-летию со дня рождения ак. О.Б. Лупанова (Москва, июнь 2007)
- VI молодежная научная школа по дискретной математике и ее приложениям (Москва, апрель 2007)
- V международная конференция «Дискретные модели в теории управляющих систем» (Москва, Ратмино, май 2003)
- V международная конференция «Algebraic and Combinatorial Coding Theory» (Царское Село, сентябрь 2002)
- Международная конференция «IEEE International Symposium on Information Theory ISIT2002» (Швейцария, июль 2002)
- Международная конференция «Indocrypt 2001» (Индия, Ченнай (Мадрас), декабрь 2001)
- Пятая научная молодежная школа по дискретной математике и ее приложениям (Москва, ноябрь 2001)
- Международная школа-семинар «Дискретная математика и математическая кибернетика» (Москва, Ратмино, май 2001)
- Конференция молодых ученых механико-математического факультета МГУ (апрель, 2001г)

Публикации

Результаты диссертации опубликованы в 13 работах автора, список которых приведен в конце автореферата [1–13].

Структура и объем работы

Диссертация состоит из введения, пяти глав и списка литературы из 27 наименований. Общий объем диссертации — 77 страниц, в работе содержится 2 рисунка.

КРАТКОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** содержится обзор результатов, связанных с темой диссертации, приводится постановка задач, дается краткое изложение основных результатов диссертации.

В **главах 1–3** рассматривается задача существования двоичных кодов, равномерно распределенных со степенью l по шарам.

В **главе 1** вводится определение кода, равномерно распределённого со степенью l по шарам

Определение 1 *Пусть l — натуральное число. Код $C \subseteq V^n$ называется* равномерно распределенным по шарам *со степенью l (l-РРШ кодом), если*

$$\max_x\{wt((S_r(x), C)\} - \min_x\{wt((S_r(x), C)\} \leqslant l$$

для каждого r, $0 \leqslant r \leqslant n$,

где $S_r(x)$ — шар радиуса r в центром в точке x, $wt((S_r(x), C)$ — вес шара $S_r(x)$, равный мощности множества $S_r(x) \cap C$. В качестве расстояния используем расстояние Хемминга.

Основным результатом глав 1–3 является

Теорема 1 *Пусть l — фиксированное натуральное число, n — размерность булевого куба и $2l + 1 \leqslant m \leqslant 2^{n-1}$. Тогда в булевом кубе размерности n не существует l-*РРШ *кодов мощности m для достаточно больших n.*

Эта теорема следует непосредственно из теорем 3–6.

Напротив, при $m \leqslant 2l$ существуют l-РРШ коды при сколь угодно больших n:

Теорема 2 *Пусть l — фиксированное натуральное число, n — размерность булевого куба. Тогда для любого n существует l-*РРШ *код мощности m при $m \leqslant 2l$.*

Если рассматривать шары не всех радиусов сразу, а лишь одного или нескольких — равномерное распределение кодовых слов по шарам возможно при любом n, например, код Хемминга является равномерно распределенным со степенью 1 по шарам радиуса $r = 1$, а любая l-упаковка радиуса R является равномерно распределенной со степенью l по шарам по шарам радиуса $r \leqslant R$.

В **главе 1** рассматриваются коды *малой* мощности.

Рассмотрим произвольную функцию $M(n) = o\left(\sqrt{n}e^{\frac{n}{4^{l+1}}}\right)$. Тогда под кодами *малой мощности* понимаем коды, мощность которых удовлетворяет условию $2l + 1 \leqslant m \leqslant M(n) = o\left(\sqrt{n}e^{\frac{n}{4^{l+1}}}\right)$. В случае кодов малой мощности неравномерность распределения по шарам устанавливается на шарах, радиус которых близок к $n/2$. При доказательстве теоремы используются неравенства для сумм биномиальных коэффициентов.

Теорема 3 *Пусть $l \in \mathbb{N}$ и $m = m(n) \geqslant 2l + 1$. Тогда, для достаточно больших n не существует l-*РРШ *кодов мощности m в следующих случаях:*
1) l — константа и $\frac{m}{\sqrt{n}e^{\frac{n}{4^{l+1}}}} \underset{n\to\infty}{\longrightarrow} 0$,
2) $l = k\log_2 m + O(1)$ и $\lim\limits_{n\to\infty} \frac{m^{2k}}{n} \cdot \ln n < \frac{k}{4}$,
3) $l = m^{\frac{1}{k}} + O(1)$ и существует $\lambda > 0$ такое что $\lim\limits_{n\to\infty} \frac{m}{\log_2^k n^{\frac{1}{2}}} \leqslant 1 - \lambda$,
4) $l = \frac{m}{4} + o(1)$ и $\lim\limits_{n\to\infty} \frac{m}{\log_{\frac{4}{3}} n} < \frac{2}{3}$.

В **главе 2** рассматриваются коды *средней* мощности:

$$8nl < m < \frac{2^n}{\sum\limits_{i=0}^{k_0(l)} \binom{n}{i}}.$$

где $k_0(l)$ - некоторое целое число. При доказательстве используются свойства взаимного расположения кодовых слов в шарах различного радиуса, свойства кодов Рида-Маллера первого порядка и свойства сумм биномиальных коэффициентов. Неравномерность распределения по шарам имеется на шарах различного радиуса от k до n.

Теорема 4 *Пусть l — фиксированное натуральное число и $k_0(l)$ — некоторое натуральное число. Тогда в булевом кубе размерности n при достаточно больших n не существует кодов, равномерно распределенных со степенью l по шарам, мощности m, удовлетворяющей неравенствам:*

$$8nl < m < \frac{2^n}{\sum\limits_{i=0}^{k_0(l)} \binom{n}{i}}.$$

В **главе 3** рассматривается вопрос существования l-РРШ кодов большой мощности

$$\lambda \frac{2^n}{n^s} < m \leqslant 2^{n-1},$$

где λ — некоторое положительное число, $s > k_0(l)$. Эти параметры выбираются так, чтобы диапазоны средней и большой мощности пересекались. В этой главе доказывается, что для достаточно больших n не существует l-РРШ кодов в указанном диапазоне. В случае кодов большой мощности мы выделим два семейства мощностей, первое семейство рассмотрим в теореме 5, а второе — в теореме 6.

Теорема 5 *Пусть l — фиксированное натуральное число. Числа $s \in \mathbb{N}$, $u > 1$, c_s — некоторая константа (своя для каждого s) и m удовлетворяют соотношениям:*

$$\frac{ul^2}{4} \frac{2^n}{\sum\limits_{i=0}^{s} \binom{n}{i}} \leqslant m \leqslant \left(\frac{n}{s^2} + c_s \right) \frac{2^n}{\sum\limits_{i=0}^{s} \binom{n}{i}}, \qquad s > 1.$$

$$\frac{ul^2}{4} \cdot \frac{2^n}{n+1} \leqslant m \leqslant 2^{n-1}, \qquad s = 1.$$

Тогда для достаточно больших n в булевом кубе размерности n не существует l-РРШ кодов мощности m.

Кроме того, в случае $s = 1$ в булевом кубе размерности n не существует l-РРШ кодов, если n удовлетворяет следующим условиям:

$$n > \frac{u}{u-1} \left(3l + 1 + \frac{ul^2}{4} \right), \quad n \geqslant 6l + 3 + \frac{ul^2}{2}.$$

Отметим, что случай $s = 1$ покрывает почти все двоичные коды. Кроме того, к нему относятся все уравновешенные коды. При этом неравномерность распределения по шарам имеется уже на шарах радиусов 1 и 2.

Основная идея доказательства — подсчет пар кодовых слов на некотором расстоянии k двумя способами (верхняя и нижняя оценки) и сравнение полученных величин. В общем случае неравномерность распределения по шарам имеется уже на шарах радиусом до $2s$.

Теорема 6 *Пусть l — фиксированное натуральное число. Тогда в булевом кубе размерности n не существует кодов, равномерно распределенных по шарам со степенью l, следующей мощности m:*

$$\lambda_1 \frac{2^n}{\sum\limits_{i=0}^{s} \binom{n}{i}} \leqslant m \leqslant \lambda_2 \frac{2^n}{\sum\limits_{i=0}^{s} \binom{n}{i}}$$

при достаточно больших n, λ_1 и λ_2 — некоторые положительные числа.

Положительные числа λ_1 и λ_2 выбираем так, чтобы первое и второе семейства мощностей пересекались.

В **главе 4** рассматриваются l-упаковки большого радиуса, $R > \left(\frac{1}{2} - \frac{1}{2^{l+1}}\right) \cdot n$.

Теорема 7 *Пусть l — фиксированное натуральное число. Для достаточно больших n если существует l-упаковка радиуса $R = \tau n$, то*

$$\tau < \frac{1}{2}\left(1 - 2\frac{\binom{m/2}{l+1}}{\binom{m}{l+1}}\right),$$

где $\binom{m/2}{l+1} = \frac{\frac{m}{2}\left(\frac{m}{2}-1\right)\ldots\left(\frac{m}{2}-l\right)}{(l+1)!}$ — определено и для нечетных m.

Получена явная верхняя оценка мощности l-упаковки в зависимости от ее радиуса $R = \tau n$:

Следствие 1 *В условиях теоремы при $\frac{1}{2} - \frac{1}{2^{l+1}} < \tau < \frac{1}{2}$, мощность l-упаковки радиуса $R = \tau n$ при достаточно больших n удовлетворяет условию*

$$m < \frac{l(l+1)}{4a(\tau)} + \frac{1}{2a(\tau)}\sqrt{\left(\frac{l(l+1)}{2}\right)^2 - 4a(\tau)c_l},$$

где $a(\tau) = (2\tau - 1) \cdot 2^l + 1$ и c_l не зависит от τ.

В **главе 5** рассматриваются матрицы специального вида, так называемые *подходящие* матрицы. Понятие подходящей (k_0, k, p, t)-матрицы было введено Таранниковым Ю. В.[13]:

Определение 3 *Пусть $B = (b_{ij})$ — это $(2^k \times p)$ матрица с 2^k строками и p столбцами, клетки которой заполнены символами из множества $\{1, 2, *\}$. Пусть k_0 и t — это натуральные числа. Мы предполагаем, что*

(а) для любых двух строк i_1 и i_2 существует столбец j, такой что $b_{i_1 j} = 1$, $b_{i_2 j} = 2$ или $b_{i_1 j} = 2$, $b_{i_2 j} = 1$.

(б) для любой строки i выполняется неравенство $\sum_{j=1}^{p} b_{ij} \leqslant t$ (знаки $*$ не дают в суммы никакого вклада).

(в) в каждой строке число единиц не превосходит k_0.

Если матрица B удовлетворяет всем свойствам (а), (б), (в), то мы говорим, что B является подходящей *(k_0, k, p, t)-матрицей.*

Интерес представляет нижняя граница отношения $\frac{t}{t+k}$ параметров подходящей (k_0, k, p, t)-матрицы. В этой главе доказывается, что

Теорема 8 *Для любой подходящей (k_0, k, p, t)-матрицы выполняется неравенство $\frac{t}{t+k} \geqslant \frac{1}{\log_2(\sqrt{5}+1)} = 0.5902\ldots$*

и что можно построить подходящую (k, k, p, t)-матрицу с соотношением параметров, сколь угодно близким к нижней границе:

Теорема 9 *Для любого $\varepsilon > 0$ существует подходящая (k, k, p, t)-матрица, для которой $\frac{t}{t+k} < \frac{1}{\log_2(\sqrt{5}+1)} + \varepsilon$.*

Матрицы с минимальным отношением $\frac{t}{t+k}$ используются в [10] для построения корреляционно-иммунных функций с высокой нелинейностью.

Благодарности

Автор выражает искреннюю благодарность своему научному руководителю кандидату физико-математических наук Юрию Валерьевичу Таранникову за постановку задач, постоянное внимание, многочисленные плодотворные обсуждения и помощь в работе.

[13] Tarannikov Yu. New constructions of resilient Boolean functions with maximal nonlinearity // Fast Software Encryption. 8th International Workshop, FSE 2001 Yokohama, Japan, April 2–4, 2001. Revised Papers, Lecture Notes in Computer Science, V. 2355, 2002, pp. 66–77.

Список литературы

[1] Ярыкина М. С. Несуществование двоичных кодов, равномерно распределенных по шарам. // Дискретный анализ и исследование операций. 2008, №2, с. 65–97.

[2] Ярыкина М. С. Применение оценок для сумм биномиальных коэффициентов при решении некоторых задач теории кодирования и криптографии. // Математические вопросы кибернетики. Вып. 12. — М.: Физматлит, 2003. — С. 87–108.

[3] Федорова М. С. О неравенствах для параметров комбинаторных матриц специального вида. // Вестник Московского Университета. Серия 15. Вычислительная математика и кибернетика. 2002, №2, с.45–49.

[4] Федорова М. С. О соотношениях между параметрами матриц специального вида. // Современные исследования математики и механики. Труды XXIII конференции молодых ученых механико-математического факультета МГУ (9–14 апреля 2001г.) Москва, Изд-во центра прикладных исследований при мех-мат факультете МГУ, 2001, том 3, стр. 334–337.

[5] Федорова М. С. О неравенствах для параметров матриц специального вида. // Труды международной школы-семинара «Дискретная математика и математическая кибернетика», Ратмино, 31 мая–3 июня 2001г. Москва 2001, стр. 26.

[6] Федорова М. С. Равномерно распределить двоичные наборы по шарам не всегда возможно. // Труды Пятой научной молодежной школы по дискретной математике и ее приложениям (Москва, 13–16 ноября 2001 г.). М., Изд-во центра прикладных исследований при мех-мат факультете МГУ, 2001, с. 94–100.

[7] Ярыкина М. С. Об оценках для l-упаковок большого радиуса. // Труды V международной конференции «Дискретные модели в теории управляющих систем», Ратмино, 26 мая–29 мая 2003г. Москва 2003, стр. 94.

[8] Ярыкина М. С. Несуществование двоичных кодов, равномерно распределенных по шарам, почти всех мощностей // Материалы VI

молодежной научной школы по дискретной математике и ее приложением (Москва, 16–21 апреля 2007г), ч. III, С. 52–56.

[9] Ярыкина М.С. Двоичные коды почти всех мощностей не могут быть равномерно распределенными по шарам // Материалы IX международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения ак. О.Б. Лупанова, Изд-во мех-мат фак. МГУ, 2007 С. 464–467.

[10] Fedorova M., Tarannikov Yu. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices // Progress in Cryptology — Indocrypt 2001, Chennai, India, December 16–20, 2001, Proceedings, Springer-Verlag, 2001, V. 2247, pp. 254–266.
http://eprint.iacr.org/2001/083 16 pp.

Ярыкиной М.С. принадлежит теорема о нижней оценке о соотношениях матриц специального вида.

[11] Fedorova M., Tarannikov Yu. On impossibility of uniform distribution of codewords over spheres in some cases. // Proceedings of 2002 IEEE International Symposium on Information Theory ISIT2002, Lausanne, Switzerland, June 30 - July 05, 2002, p. 344.

Федоровой М.С. принадлежат основные результаты.

[12] Fedorova M., New results on impossibility of uniform distribution of codewords over spheres // Proceedings of Eighth International Workshop on Algebraic and Combinatorial Coding Theory, Tsarskoe Selo, Russia, September, 2002, pp. 104–107.

[13] Yarykina M. S. The Impossibility of Uniform Distribution of Codewords over Spheres. // Proceedings of the NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security, Zvenigorod, Russia, 8–18 September, 2007. IOS press, 2008, vol.18, pp. 315–331.