Учреждение Российской академии наук
Математический институт им. В.А.Стеклова РАН

На правах рукописи
УДК 519.7+519.213

Серов Александр Александрович

ОЦЕНКИ РАСПРЕДЕЛЕНИЙ РАССТОЯНИЙ ОТ СЛУЧАЙНОЙ БУЛЕВОЙ ФУНКЦИИ ДО АФФИННЫХ И КВАДРАТИЧНЫХ ФУНКЦИЙ

01.01.05 — теория вероятностей и математическая статистика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата физико-математических наук

Москва 2011

Работа выполнена в Учреждении Российской академии наук Математическом институте им. В. А. Стеклова РАН.

Научный руководитель: доктор физико-математических наук А. М. Зубков

Официальные оппоненты: доктор физико-математических наук, профессор Г. И. Ивченко

кандидат физико-математических наук, доцент С. И. Чечёта

Ведущая организация: Механико-математический факультет Московского государственного университета им. М. В. Ломоносова

Защита диссертации состоится 12 мая 2011 года в 14 часов на заседании диссертационного совета Д 002.022.01 в МИАН по адресу: 119991, г. Москва, ул. Губкина, д. 8.

С диссертацией можно ознакомиться в библиотеке МИАН.

Автореферат разослан апреля 2011 года.

Ученый секретарь диссертационного
совета Д 002.022.01 в МИАН
доктор физико-математических наук В. А. Ватутин

Общая характеристика работы

Актуальность темы

Понятие булевой функции сформировалось во второй половине XIX века в работах одного из основоположников математической логики английского математика Джорджа Буля (G. Boole, 1815-1864). В первой половине XX века булевы функции приобрели фундаментальное значение для оснований математики. Вместе с тем длительное время булевы функции оставались невостребованными в прикладных областях.

Существенные изменения произошли в середине XX века, когда бурное развитие техники связи, приборостроения и вычислительной техники потребовало создания адекватного математического аппарата. В этот период происходит становление таких прикладных отраслей математики, как теория конечных функциональных систем, теория информации, теория кодирования и, наконец, теоретическая криптография.

Практика показала плодотворность применения аппарата теории булевых функций к проблемам анализа и синтеза дискретных устройств, осуществляющих обработку и преобразование информации.

Как известно из практики математических исследований, линейность (в математическом смысле) изучаемого объекта упрощает его исследование. Линейность с успехом используется в алгебре, теории систем, математической кибернетике и других разделах математики. С другой стороны, для построения надёжных криптографических систем важна как раз нелинейность, а существование свойств, близких к свойствам линейных функций, считается слабостью. Наличие таких свойств противоречит фундаментальным принципам построения криптографических систем.

Одной из мер нелинейности булевой функции f является величина N_f, численно равная расстоянию (в метрике Хэмминга) от данной функции до множества аффинных функций $\mathbb{A}_n$.

С точки зрения теории кодирования множество аффинных функций представляет собой код Рида-Маллера первого порядка $RM(1, n)$, а значение N_f является верхней границей для радиуса покрытия кода

$RM(1,n)$ (см. Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн[1]). В случае четного n значение N_f в точности совпадает с радиусом покрытия кода $RM(1,n)$. При нечётном n точное значение радиуса покрытия кода $RM(1,n)$ известно лишь для некоторых значений n, а в остальных случаях имеются только его нижние и верхние оценки.

По аналогии с нелинейностью булевой функции f как расстояния до множества аффинных функций можно рассматривать также расстояние от f до множества булевых функций, представимых в виде многочленов второй степени (квадратичных функций).

В настоящей работе получены двусторонние оценки и асимптотические формулы для количеств булевых функций от n переменных, которые с заданной точностью аппроксимируются линейными, аффинными или квадратичными булевыми функциями. Используя термины теории вероятностей, можно сказать, что эти результаты описывают распределение расстояния от случайной равновероятной булевой функции до линейных, аффинных и квадратичных функций в области вероятностей больших уклонений. Доказана предельная теорема для расстояния Хемминга между случайной равновероятной булевой функцией от n переменных и множеством аффинных булевых функций от тех же переменных, дополняющая аналогичную теорему Б.В. Рязанова для расстояния до множества линейных булевых функций.

Цель работы

Цели работы:

— исследование предельного распределения расстояния Хемминга между случайной равновероятной булевой функцией от n переменных и множеством аффинных булевых функций,

— получение явных двусторонних оценок и асимптотических формул для количеств булевых функций от n переменных, которые с заданной точностью аппроксимируются линейными, аффинными или квадратичными булевыми функциями.

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

Научная новизна

Все полученные результаты являются новыми. Основные результаты работы состоят в следующем.

1. Доказана предельная теорема для расстояния Хемминга от случайной равновероятной булевой функции до множества аффинных булевых функций от n переменных.

2. Получены явные асимптотически точные двусторонние оценки для количеств булевых функций, которые с заданной погрешностью аппроксимируются линейными, аффинными или квадратичными булевыми функциями.

Методы исследования

В диссертации используются методы теории вероятностей и перечислительной комбинаторики.

Теоретическая и практическая ценность

Работа имеет теоретический характер. Результаты диссертации могут найти применение в теории кодирования, в теории конечных автоматов и теоретической кибернетике.

Апробация работы

Результаты диссертации докладывались на семинарах Отдела дискретной математики Математического института им. В. А. Стеклова РАН (г. Москва, 2007–2010 гг.), X Всероссийском Симпозиуме по прикладной и промышленной математике (г. Санкт-Петербург, 2009 г.), X Международном семинаре «Дискретная математика и её приложения» (г. Москва, 2010 г.), 9-й Международной конференции по компьютерному анализу данных и моделированию (г. Минск, 2010 г.).

Публикации

Основные результаты диссертации опубликованы в 5 работах, список которых приведён в конце автореферата [1–5].

Структура диссертации

Диссертация состоит из введения, четырёх глав и списка литературы. Общий объём диссертации составляет 87 страниц. Список литературы включает 18 наименований.

Краткое содержание диссертации

Во введении приведён краткий исторический обзор по тематике работы, изложены цели исследования, а также перечислены основные полученные результаты.

В первой главе диссертации доказывается предельная теорема для расстояния Хемминга между случайной равновероятной булевой функцией от n переменных и множеством аффинных булевых функций от тех же переменных, дополняющая аналогичную теорему Б.В. Рязанова для расстояния до множества линейных булевых функций.

Перейдём к более подробному изложению результатов главы 1.

Пусть $\mathbb{F}_2$ – поле из двух элементов. Для произвольного натурального числа n будем обозначать через $V_n = \mathbb{F}_2^n$ пространство n-мерных векторов с компонентами из $\mathbb{F}_2$. Между множеством $\mathbb{F}_2^{V_n} = \{f\colon V_n \to \mathbb{F}_2\}$ всех булевых функций от n переменных и пространством V_{2^n} можно установить взаимно однозначное соответствие, отождествляя функцию $f \in \mathbb{F}_2^{V_n}$ с вектором $\{f(x)|\ x \in V_n\}$.

Расстояние Хэмминга $\rho(f,g)$ между булевыми функциями $f, g \in \mathbb{F}_2^{V_n}$ определяется как число значений переменной $x \in V_n$, при которых $f(x) \neq g(x)$. Для произвольного множества булевых функций $A \subset \mathbb{F}_2^{V_n}$ и функции $f \in \mathbb{F}_2^{V_n}$ обозначим через $\rho(f,A) = \min\limits_{g\in A} \rho(f,g)$ расстояние Хэмминга от f до ближайшей к ней функции из множества A.

В множестве $\mathbb{F}_2^{V_n}$ всех булевых функций естественно выделяются: класс линейных функций

$$\mathbb{L}_n \,=\, \{f \,\in\, \mathbb{F}_2^{V_n} :\, f(x_1,\ldots,x_n) \,=\, a_1x_1 \oplus \ldots \oplus a_nx_n,\;\; a_1,\ldots,a_n \,\in\, \mathbb{F}_2\}\,,$$

класс аффинных функций

$$\mathbb{A}_n = \{f \in \mathbb{F}_2^{V_n} \colon f(x_1,\ldots,x_n) = a_0 \oplus a_1x_1 \oplus \ldots \oplus a_nx_n,\;\; a_0,\ldots,a_n \in \mathbb{F}_2\}$$

и класс квадратичных функций

$$\mathbb{Q}_n = \{f \in \mathbb{F}_2^{V_n} \colon f(x_1,\ldots,x_n) = \bigoplus_{1\leqslant i<j\leqslant n} b_{ij}x_ix_j \oplus \bigoplus_{i=1}^{n} a_ix_i \oplus a_0,\;\; b_{ij}, a_i \in \mathbb{F}_2\}\,,$$

где $\oplus$ — сложение в $\mathbb{F}_2$; очевидно, $\mathbb{L}_n \subset \mathbb{A}_n \subset \mathbb{Q}_n$. Мощности этих классов имеют следующий вид:

$$|\,\mathbb{L}_n| = 2^n,\;\; |\,\mathbb{A}_n| = 2^{n+1} \;\text{ и }\; |\,\mathbb{Q}_n| = 2^{\binom{n}{2}+n+1}.$$

Предельные теоремы для распределения расстояния между случайной булевой функцией и множеством линейных булевых функций доказаны в работе Б.В. Рязанова[2]. В частности, было показано, что если $f \in \mathbb{F}_2^{V_n}$ – случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^{V_n}$, то

$$\lim_{n\to\infty} \mathbf{P}\left\{\frac{\rho(f,\mathbb{L}_n) - a_n}{b_n} \leqslant x\right\} = 1 - e^{-e^x} \;\; \forall\, x \in \mathbb{R}, \tag{1}$$

где

$$a_n = 2^{n-1} - 2^{\frac{n-1}{2}}\sqrt{n\ln 2}\left(1 - \frac{\ln\ln 2^n + \ln 4\pi}{4n\ln 2}\right), \quad b_n = \frac{2^{\frac{n-1}{2}}}{2\sqrt{n\ln 2}}\,. \tag{2}$$

В совместной работе Б.В. Рязанова и С.И. Чечёты[3] доказаны предельные теоремы для распределения расстояния от случайной булевой функции до множества квадратичных булевых форм со свободным членом. В частности, показано, что для любого фиксированного x

[2] *Ryasanov B.V.* Probabilistic methods in the theory of approximation of discrete functions. — Probab. Meth. Discr. Math., Proc. 3rd Int. Petrozavodsk Conf., TVP/VSP, Moscow, 1993, pp. 403–412.

[3] *Рязанов Б.В., Чечёта С.И.* О приближении случайной булевой функции множеством квадратичных форм. — Дискретная математика., 1995, т. 7, № 3, с. 129–145.

$$\lim_{n\to\infty} \mathbf{P}\left\{\frac{\rho(f,\mathbb{Q}_n)-h_n}{s_n}\leqslant x\right\}=1-e^{-e^x}, \tag{3}$$

где

$$h_n=2^{n-1}-2^{\frac{n-2}{2}}n\sqrt{\ln 2}\left\{1+\frac{1}{2n}-\frac{4\ln\left(\pi n^2\ln 2\right)-\ln 2}{8n^2\ln 2}\right\},\quad s_n=\frac{2^{\frac{n-2}{2}}}{n\sqrt{\ln 2}}. \tag{4}$$

В главе 1 диссертации содержится доказательство теоремы, дополняющей результаты работы Б.В. Рязанова.

Теорема 1. *Если $f\in\mathbb{F}_2^{V_n}$ – случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^{V_n}$, то для любого фиксированного $x\in\mathbb{R}$*

$$\lim_{n\to\infty} \mathbf{P}\left\{\frac{\rho(f,\mathbb{A}_n)-a_n}{b_n}\leqslant x-\ln 2\right\}=1-e^{-e^x}, \tag{5}$$

где a_n и b_n определены в (2).

(Нумерация теорем, следствий и утверждений в автореферате отличается от их нумерации в тексте диссертации.)

Во второй главе диссертации получены двусторонние оценки окрестностей линейных кодов, а также вспомогательные оценки для сумм с биномиальными коэффициентами, которые возникают в главах 3 и 4.

Рассмотрим произвольный линейный код $\mathcal{C}$ длины n с минимальным расстоянием $d=\min\limits_{w\neq 0,\, w\in\mathcal{C}}\mathrm{wt}(w)$ и $n-k$ проверочными символами. В таком коде имеется 2^k кодовых слов.

Представим, как и в книге Р. Блейхута[4], окрестности кодовых слов в виде шаров целочисленного радиуса r. Если при $r=a$, $a\in\mathbb{Z}$, шары не пересекаются, а при $r=a+1$ пересекаются, то a называется *радиусом сферической упаковки* кода. Минимальное значение b радиуса r, при котором каждая точка V_n попадает в b-окрестность хотя бы одного кодового слова, называется *радиусом покрытия* кода.

[4] *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. — М.: Мир, 1986.

Нахождение количеств векторов $v \in V_n$, попадающих в r-окрестность кода $\mathcal{C}$, представляет практический интерес, причём при $r \leqslant a$ и $r \geqslant b$ справедливы тривиальные формулы, а в общем случае соответствующие точные формулы весьма сложны. В главе 2 для этих величин в случае $a < r < b$ получены двусторонние неравенства в терминах весового спектра кода.

Пространство V_n можно представить в виде объединения слоёв $V_n(i) = \{x \in V_n \colon \mathrm{wt}(x) = i\}$, т. е.

$$V_n = \bigcup_{i=0}^{2^n} V_n(i).$$

Введём обозначение

$$N_n^{(2)}(i, r) \stackrel{\text{def}}{=} \left|\{x \in V_n \colon \max\{\mathrm{dist}\,(x, 0), \mathrm{dist}\,(x, c)\} \leqslant r, \mathrm{wt}(c) = i\}\right|.$$

При фиксированном значении i правая часть не зависит от вектора c, $\mathrm{wt}(c) = i$, так как любой вектор веса i можно перевести в любой другой вектор такого же веса перенумерацией координат, которая не изменяет веса векторов и расстояние Хэмминга между ними.

Теорема 2. *Если известен весовой спектр кода $\mathcal{C}$, т.е. мощности множеств кодовых слов веса i*

$$W_i = V_n(i) \cap \mathcal{C}, \quad i \in \{0, 1, \ldots, n\},$$

то справедливы оценки для чисел элементов множеств $\mathbb{F}_2(\mathcal{C}, r) = \{v \in V_n \colon \mathrm{dist}\,(v, \mathcal{C}) \leqslant r\}$ при $r \leqslant n$

$$(1 - q(n, r))2^k \sum_{m=0}^{r} C_n^m \leqslant |\mathbb{F}_2(\mathcal{C}, r)| \leqslant 2^k \sum_{m=0}^{r} C_n^m,$$

где $q(n, r) = \frac{1}{2} \sum\limits_{i=1}^{n} |W_i| N_n^{(2)}(i, r) / \sum\limits_{m=0}^{r} C_n^m$.

Оценки теоремы 2 справедливы для более широкого класса кодов: достаточно потребовать, чтобы совокупность расстояний от кодового слова до всех остальных кодовых слов была одной и той же для всех кодовых слов.

Ряд явных двусторонних оценок для $N_n^{(1)}(r) \stackrel{\text{def}}{=} \sum\limits_{m=0}^{r} C_n^m$ и $N_n^{(2)}(i,r)$ получены в следующих трёх утверждениях.

Утверждение 1. *При $r \leqslant n/2$ справедливы оценки*

$$2^n\Phi\left(-\sqrt{nV\left(1-\tfrac{2r}{n}\right)}\right) \;\leqslant\; \sum_{m=0}^{r} C_n^m \;\leqslant\; 2^n\Phi\left(-\sqrt{nV\left(1-\tfrac{2(r+1)}{n}\right)}\right),$$

$$\frac{n^n}{r^r(n-r)^{n-r}\sqrt{2\pi nV\left(1-\frac{2r}{n}\right)}}\left(1-\frac{1}{nV\left(1-\frac{2r}{n}\right)}\right) < \sum_{m=0}^{r} C_n^m < \\ < \frac{n^n}{(r+1)^{r+1}(n-r-1)^{n-r-1}\sqrt{2\pi nV\left(1-\frac{2(r+1)}{n}\right)}},$$

где $\Phi(\cdot)$ — функция стандартного нормального распределения, $V(z) = (1-z)\ln(1-z) + (1+z)\ln(1+z)$.

Утверждение 2. *Если $0 \leqslant r \leqslant [n/2]$, то*

$$C_n^r(1+q) \leqslant \sum_{m=0}^{r} C_n^m \leqslant C_n^r \frac{1}{1-q}, \quad \textit{где} \quad q = \frac{r}{n-r+1},$$
$$C_k^{[k/2]} N_{n-k}^{(1)}(r-[k/2]) \leqslant N_n^{(2)}(k,r), \quad \textit{где} \quad 0 \leqslant k \leqslant n.$$

Утверждение 3. *Если $0 \leqslant r \leqslant [n/2]$ и $0 \leqslant k \leqslant n$, то*

$$N_n^{(2)}(k,r) \leqslant C_k^{k/2} C_{n-k}^{r-k/2} \frac{1+q_k}{(1-q_k)^2} \text{ при чётном } k,$$

$$N_n^{(2)}(k,r) \leqslant C_k^{[k/2]} C_{n-k}^{r-[k/2]} \frac{2}{(1-q_k)^2} \text{ при нечётном } k,$$

где $q_k = \frac{r-[k/2]}{n-[k/2]-r+1} < q = \frac{r}{n-r+1}$.

В третьей и четвёртой главах приводятся основные результаты диссертации: формулы и двусторонние оценки для чисел элементов множеств

$$\mathbb{F}_2(\mathbb{L}_n, r) = \{f \in \mathbb{F}_2^{V_n} \colon \rho(f, \mathbb{L}_n) \leqslant r\},$$
$$\mathbb{F}_2(\mathbb{A}_n, r) = \{f \in \mathbb{F}_2^{V_n} \colon \rho(f, \mathbb{A}_n) \leqslant r\},$$
$$\mathbb{F}_2(\mathbb{Q}_n, r) = \{f \in \mathbb{F}_2^{V_n} \colon \rho(f, \mathbb{Q}_n) \leqslant r\}$$

всех булевых функций от n переменных, расстояния от которых до множеств линейных $\mathbb{L}_n$, аффинных $\mathbb{A}_n$, квадратичных $\mathbb{Q}_n$ функций соответственно меньше или равны r. Известно[5], что $\mathbb{F}_2(\mathbb{A}_n, r) = \mathbb{F}_2^{V_n}$, если $r \geqslant 2^{n-1} - 2^{n/2-1}$.

В частности, из результатов работы Б.В. Рязанова[2] следует, что если $\mathbb{F}_2(\mathbb{L}_n, r)$ — множество всех булевых функций, расстояние Хемминга от которых до множества линейных функций (аффинных с нулевым свободным членом) не превосходит r, то при $n \to \infty$

$$\sup_{0 \leqslant r < 2^{n-1} - 2^{n/2-1}} \left| 2^{-2^n} |\mathbb{F}_2(\mathbb{L}_n, r)| - \left(1 - e^{-e^{-x(n,r)}}\right) \right| \to 0\,, \tag{6}$$

где $x(n, r)$ определяется равенством

$$r = 2^{n-1} - \sqrt{2^{n-1}\left(n \ln 2 - \tfrac{1}{2} \ln(4\pi n \ln 2) + x(n, r)\right)}.$$

Это означает, что для основной массы булевых функций от n переменных расстояние до множества линейных функций при $n \to \infty$ имеет вид

$$2^{n-1} - \sqrt{2^{n-1}\left(n \ln 2 - \tfrac{1}{2} \ln n\right)} + O\left(\sqrt{2^n/n}\right).$$

Сравнение (1) и (5) показывает степень увеличения окрестности множества $\mathbb{A}_n$ аффинных функций по сравнению с окрестностью множества $\mathbb{L}_n$ линейных функций.

[5] *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

Основным результатом главы 3 является следующее утверждение.

Теорема 3. *Если* $n \geqslant 2$, *то*

$$(1 - Q(n,r))2^{n+1} \sum_{m=0}^{r} C_{2^n}^m \leqslant |\,\mathbb{F}_2(\mathbb{A}_n, r)| \leqslant 2^{n+1} \sum_{m=0}^{r} C_{2^n}^m,$$

$$\left(1 - \tfrac{1}{2}\,Q(n,r)\right) 2^n \sum_{m=0}^{r} C_{2^n}^m \leqslant |\,\mathbb{F}_2(\mathbb{L}_n, r)| \leqslant 2^n \sum_{m=0}^{r} C_{2^n}^m,$$

где $Q(n,r) = 0$ *при* $0 \leqslant r < 2^{n-2}$,

$$Q(n,r) < \frac{1}{15}\, 2^{-\left(c_r^2 - \frac{3}{2}\right)n} \exp\left\{\frac{2(c_r^2 n)^{3/2}}{2^{n/2}}\right\}$$

при $n \geqslant 8$, $r = 2^{n-1} - c_r\sqrt{2^{n-1} n \ln 2} \geqslant 0,\ c_r > 1$.

Неравенства теоремы 3 позволяют получать оценки для левого хвоста распределения расстояния от случайной булевой функции до множеств аффинных и линейных булевых функций.

Отношения верхних и нижних оценок в теореме 3 стремятся к 1, если $n \to \infty$ и $r < 2^{n-1} - c\sqrt{2^{n-1} n \ln 2}$, $c > \sqrt{1,5} = 1,2247\ldots$

С помощью утверждения 1 показано, что в области «больших уклонений» (где $1 - e^{-e^{-x(n,r)}} \to 0$) относительная погрешность приближения величины $2^{-2^n}|\mathbb{F}_2(\mathbb{L}_n, r)|$ величиной $1 - e^{-e^{-x(n,r)}}$ быстро растет с уменьшением r.

Следствие 1. *Если* $c > 1$ *и* $n, r \to \infty$ *так, что выполняется условие* $r < 2^{n-1} - c\sqrt{2^{n-1} n \ln 2}$, *то при достаточно больших* n

$$\frac{|\mathbb{F}_2(\mathbb{L}_n, r)|}{2^{2^n}\left(1 - e^{-e^{-x(n,r)}}\right)} < \frac{1,07}{c}\,.$$

Из результатов работы Б.В. Рязанова и С.И. Чечёты[6] (см. формулу (3)) следует, что если $\mathbb{F}_2(\mathbb{Q}_n, r)$ — множество всех булевых функций, расстояние Хемминга от которых до множества квадратичных функций не превосходит r, то при $n \to \infty$

$$\sup_{0 \leqslant r < 2^{n-1} - 2^{n/2-1}\sqrt{\ln 2}} \left|2^{-2^n}|\mathbb{F}_2(\mathbb{Q}_n, r)| - \left(1 - e^{-e^{-x(n,r)}}\right)\right| \to 0, \qquad (7)$$

[6] *Рязанов Б.В., Чечёта С.И.* О приближении случайной булевой функции множеством квадратичных форм. — Дискретная математика., 1995, т. 7, № 3, с. 129–145.

где $x(n,r)$ определяется равенством

$$r = 2^{n-1} - 2^{\frac{n}{2}-1}\sqrt{n^2\ln 2 + n\ln 2 - 2\ln n - \ln(\pi\ln 2) + \ln\sqrt[4]{2} + 2x(n,r)}. \quad (8)$$

Это означает, что для основной массы булевых функций от n переменных расстояние до множества квадратичных функций при $n \to \infty$ имеет вид

$$2^{n-1} - \sqrt{2^{n-2}\left(n^2\ln 2 + n\ln 2 - 2\ln n\right)} + O\left(2^{n/2}/n\right).$$

Основным результатом главы 4 является следующее утверждение.

Теорема 4. *Если $n \geqslant 3$, то*

$$(1 - Q(n,r))2^{\binom{n}{2}+n+1}\sum_{m=0}^{r} C_{2^n}^m \leqslant |\,\mathbb{F}_2(\mathbb{Q}_n, r)| \leqslant 2^{\binom{n}{2}+n+1}\sum_{m=0}^{r} C_{2^n}^m,$$

где $Q(n,r) = 0$ при $0 \leqslant r < 2^{n-3}$,

$$Q(n,r) < \frac{2^{-n^2\left(c_r^2-3\right)/6+n+1}}{n^2}\exp\left\{\frac{(c_r n)^3}{7\cdot 2^{n/2}}\right\}$$

при $n \geqslant 15$ и $r = 2^{n-1} - c_r n\sqrt{2^{n-2}\ln 2} \geqslant 0$, $c_r > 1$.

Неравенства теоремы 4 позволяют получать оценки для левого хвоста распределения расстояния от случайной булевой функции до множества квадратичных булевых функций.

Отношения верхних и нижних оценок в теореме 4 стремятся к 1, если $n \to \infty$ и $r < 2^{n-1} - c\,n\sqrt{2^{n-2}\ln 2}$, $c > \sqrt{3} = 1,7321\ldots$

С помощью утверждения 1 показано, что в области «больших уклонений» (где $1 - e^{-e^{-x(n,r)}} \to 0$) относительная погрешность приближения величины $2^{-2^n}|\mathbb{F}_2(\mathbb{Q}_n, r)|$ величиной $1 - e^{-e^{-x(n,r)}}$ быстро растет с уменьшением r.

Следствие 2. *Если $c > 1$ и $n, r \to \infty$ так, что выполняется условие $r < 2^{n-1} - c\sqrt{2^{n-2}(n^2+n)\ln 2}$, то при достаточно больших n*

$$\frac{|\mathbb{F}_2(\mathbb{Q}_n, r)|}{2^{2^n}\left(1 - e^{-e^{-x(n,r)}}\right)} < \frac{1,5}{c}.$$

Автор выражает глубокую благодарность своему научному руководителю д.ф.-м.н. А. М. Зубкову за постановку интересных задач, постоянное внимание к работе и критические замечания.

Работы автора по теме диссертации

[1] *Зубков А.М., Серов А.А.* Оценки числа булевых функций, имеющих аффинные приближения заданной точности. — Дискретн. матем., 2010, т. 22, № 4, с. 3–19.

[2] *Серов А.А.* Предельное распределение расстояния между случайной булевой функцией и множеством аффинных функций. — Теория вероятн. и её примен., 2010, т. 55, № 4, с. 791–795.

[3] *Зубков А.М., Серов А.А.* Оценки числа булевых функций, имеющих аффинные приближения заданной точности. — Обозрение прикладной и промышленной математики, 2009, т. 16, вып. 2, с. 337–339.

[4] *Зубков А.М., Серов А.А.* Оценки числа булевых функций, имеющих аффинные приближения заданной точности. — Материалы X Международного семинара «Дискретная математика и её приложения» (Москва, МГУ, 1-6 февраля 2010 г.). М.: Изд-во механико-математического факультета МГУ, 2010, с. 230–232.

[5] *Serov A.A., Zubkov A.M.* On the number of Boolean functions in a given neighbourhood of the affine functions set. — Computer Data Analysis and Modeling: Complex Sthohastic Data and Systems: Proc. of the 9^{th} Intern. Conf., Minsk, Sept. 7–11, 2010. Vol. 2, p. 67–70.