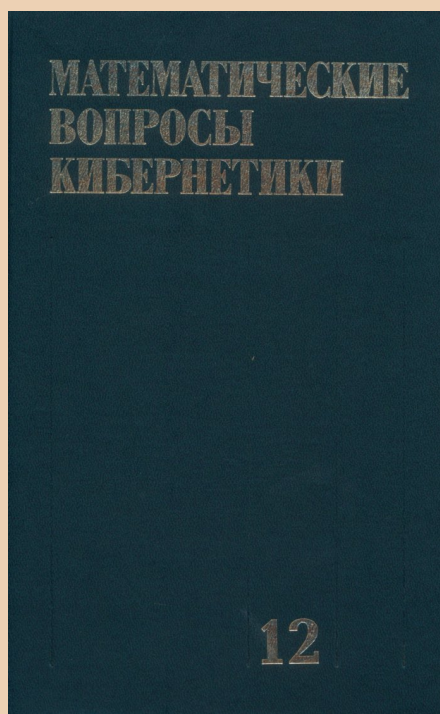




М. С. Ярыкина

**Применение оценок
для сумм
биномиальных
коэффициентов при
решении некоторых
задач теории
кодирования и
криптографии**

Рекомендуемая форма библиографической ссылки:
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. URL: <http://library.keldysh.ru/mvk.asp?id=2003-87>

ПРИМЕНЕНИЕ ОЦЕНОК ДЛЯ СУММ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ ПРИ РЕШЕНИИ НЕКОТОРЫХ ЗАДАЧ ТЕОРИИ КОДИРОВАНИЯ И КРИПТОГРАФИИ *)

М. С. ЯРЫКИНА

(МОСКВА)

§ 1. Введение

В этой работе с помощью оценок и неравенств для сумм биномиальных коэффициентов решаются некоторые задачи теории кодирования и криптографии.

В § 2 рассматривается задача существования кодов, равномерно распределенных по шарам со степенью l (l -РРШ кодов). Все такие коды при $l = 1$ (на языке их характеристических булевых функций) были описаны Ю. В. Таранниковым в [2]. Здесь излагаются результаты, утверждающие несуществование таких кодов при некоторых значениях параметров для произвольного l .

В п. 2.2 доказывается несуществование l -РРШ кодов малой мощности m , в частности доказано несуществование l -РРШ кодов со следующими параметрами:

- 1) l — константа и $\frac{m}{\sqrt{n}e^{n/4^{l+1}}} \rightarrow 0, n \rightarrow \infty$;
- 2) $l = k \log_2 m + O(1)$ и $\lim_{n \rightarrow \infty} \frac{m^{2k}}{n} \cdot \ln n < \frac{k}{4}$;
- 3) $l = m^{1/k} + O(1)$ и существует $\lambda > 0$ такое что $\lim_{n \rightarrow \infty} \frac{m}{\log_2^k n^{1/2}} \leq 1 - \lambda$;
- 4) $l = \frac{m}{4} + o(1)$ и $\lim_{n \rightarrow \infty} \frac{m}{\log_{4/3} n} < \frac{2}{3}$.

В п. 2.3 доказывается несуществование l -РРШ кодов большой мощности, а именно для каждого целого s и $u > 1$ не существует l -РРШ кодов мощности m такой, что:

$$\frac{ul^2}{4} \cdot \frac{2^n}{n^s + O(n^{s-1})} \leq m = m(n) \leq \frac{2^n}{s^2 n^{s-1} + O(n^{s-2})} \quad \text{при } s > 1;$$

$$\frac{ul^2}{4} \cdot \frac{2^n}{n+1} \leq m = m(n) \leq 2^{n-1} \quad \text{для } s = 1.$$

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 02-01-00985), программы поддержки научных школ НШ-1807.2003.1 и программы Университеты России УР.04.03.007.

В § 3 доказывается несуществование l -упаковок большого радиуса, а именно, для $R = \tau n$ (τ не зависит от n), где $\tau > \frac{1}{4}$. Получена следующая оценка: при

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

не существует l -упаковок для достаточно больших n .

В § 4 рассматривается задача существования матриц специального вида (подходящих (k_0, k, p, t) -матриц), введенных Ю. В. Таранниковым в [21] (подробнее можно прочитать об этом в [3]). Эти матрицы используются для построения устойчивых функций с криптографически оптимальными параметрами. Для этих матриц устанавливается нижняя оценка для представляющего большой интерес отношения их параметров $\frac{t}{t+k}$ и доказывается, что это отношение не может быть меньше, чем $\frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$ В то же время строится последовательность подходящих матриц, приближающая эту нижнюю границу со сколь угодно большой точностью.

Часть результатов, вошедших в данную работу, опубликована в [4–8, 14, 15].

§ 2. Равномерно распределить двоичные наборы по шарам не всегда возможно

В этом параграфе доказывается несуществование кодов, равномерно распределенных по шарам, при некоторых значениях параметров.

2.1. Определения и предшествующие результаты. Двоичные коды, равномерно распределенные по подкубам, изучались в нескольких областях математики и в приложениях, например, двоичные коды с наибольшим дуальным расстоянием, корреляционно-иммунные и устойчивые функции, ортогональные массивы. Такие коды используются для генерации псевдослучайных последовательностей, в криптографии и т. д. Равномерное распределение двоичных наборов по шарам не изучалось ранее [2], хотя представляется, что коды, двоичные наборы которых равномерно распределены по сферам, могут иметь некоторые полезные приложения. Например, такие коды можно использовать в качестве хеширующей функции, а также когда мы хотим, чтобы все слова на выходе связи имели примерно одинаковую вероятность декодирования.

Пусть V^n — множество двоичных векторов длины n . Кодом C (множеством двоичных наборов) назовем произвольное подмножество V^n .

Мощностью $|C|$ называется число двоичных наборов в нем.

Подкодом C' кода C называется такое множество двоичных наборов кода C , у которых в разрядах $i_1, \dots, i_h$ стоят $\sigma_1, \dots, \sigma_h$ соответственно, где $\sigma_i \in \{0, 1\}$, $i = 1, \dots, h$.

Любому коду C можно сопоставить булеву функцию f :

$$f(x) = \begin{cases} 1, & \text{если } x \in C, \\ 0, & \text{если } x \notin C. \end{cases}$$

И наоборот, любой булевой функции можно сопоставить код

$$C = \{x \in V^n \mid f(x) = 1\}.$$

Расстоянием $d(x, y)$ между двумя наборами x и y называется число компонент, в которых эти наборы различаются.

Шаром $S_r(x)$ с центром $x \in V^n$ радиуса r называется множество

$$S_r(x) = \{y \in V^n \mid d(x, y) \leq r\}.$$

Весом $\text{wt}(S_r(x), C)$ шара $S_r(x)$ для кода C называется мощность множества $S_r(x) \cap C$.

Шар радиуса r веса t назовем (r, t) -шаром, а веса не менее t — $(r, t)^*$ -шаром.

Определение 1. Пусть l — натуральное. Код $C \subseteq V^n$ называется *равномерно распределенным по шарам со степенью l* (или l -РРШ кодом), если для любых $x, y \in V^n$, $0 \leq r \leq n$, выполняется

$$|\text{wt}((S_r(x), C) - \text{wt}((S_r(y), C))| \leq l.$$

Если C является l -РРШ кодом, то легко видеть, что его дополнение — код $\bar{C}$ — также является l -РРШ кодом. Поэтому можно рассматривать только коды мощности не более 2^{n-1} .

Полное описание 1-РРШ кодов было дано в [2].

Теорема 1 [2]. Пусть $C \subseteq V^n$, $|C| \leq 2^{n-1}$. Если C — 1-РРШ код, то выполняется один из случаев:

$$1) |C| \leq 2; \quad 2) n \leq 4; \quad 3) n = 6, |C| = 4.$$

Теорема 2 [2]. Число различных 1-РРШ кодов в V^n равно

$$\begin{aligned} &2^{2^n} \quad \text{для } n \leq 2, \\ &80 \quad \text{для } n = 3, \\ &334 \quad \text{для } n = 4, \\ &2818 \quad \text{для } n = 6, \\ &3 \cdot 2^n + 2 \quad \text{для } n \geq 5, n \text{ нечетно,} \\ &(n + 3)2^n + 2 \quad \text{для } n \geq 8, n \text{ четно.} \end{aligned}$$

2.2. Несуществование равномерно распределенных со степенью l кодов малой мощности. Сначала докажем вспомогательную лемму. Формулировки подобных утверждений содержатся в качестве задач в [1].

Лемма 1. Пусть $\alpha = \alpha(n) < \frac{1}{2}$. Тогда:

$$\begin{aligned} 1) \frac{1}{2^n} \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} &\leq \frac{1-\alpha}{(1-2\alpha)^2} \cdot \frac{1}{n} \left(1 + O\left(\frac{1}{n}\right)\right); \\ 2) \frac{1}{2^n} \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} &\leq \sqrt{\frac{1-\alpha}{2\pi\alpha}} \cdot \frac{1}{1-2\alpha} \cdot \frac{1}{\sqrt{ne^{\left(\frac{(1-2\alpha)^2}{2} + O((1-2\alpha)^4)\right)}}} \left(1 + O\left(\frac{1}{n}\right)\right). \end{aligned}$$

Доказательство. С помощью формулы Стирлинга получаем

$$\begin{aligned}
 \frac{1}{2^n} \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} &= \frac{1}{2^n} \sum_{i=0}^{\lceil \alpha n \rceil} \frac{n(n-1) \cdots (n-i+1)}{i!} = \\
 &= \frac{1}{2^n} \binom{n}{\lceil \alpha n \rceil} \left(1 + \frac{\lceil \alpha n \rceil}{n - \lceil \alpha n \rceil + 1} + \right. \\
 &\quad \left. + \frac{\lceil \alpha n \rceil (\lceil \alpha n \rceil - 1)}{(n - \lceil \alpha n \rceil + 1)(n - \lceil \alpha n \rceil + 2)} + \dots + \frac{(\lceil \alpha n \rceil)!}{(n - \lceil \alpha n \rceil + 1) \cdots n} \right) < \\
 &< \frac{1}{2^n} \binom{n}{\lceil \alpha n \rceil} \left(1 + \frac{\lceil \alpha n \rceil}{n - \lceil \alpha n \rceil} + \left(\frac{\lceil \alpha n \rceil}{n - \lceil \alpha n \rceil} \right)^2 + \dots \right) < \\
 &< \frac{1}{2^n} \binom{n}{\lceil \alpha n \rceil} \frac{1}{1 - \frac{\lceil \alpha n \rceil}{n - \lceil \alpha n \rceil}} = \frac{1}{2^n} \binom{n}{\lceil \alpha n \rceil} \cdot \frac{n - \lceil \alpha n \rceil}{n - 2\lceil \alpha n \rceil} \leqslant \\
 &\leqslant \frac{n - \lceil \alpha n \rceil}{(n - 2\lceil \alpha n \rceil)^2} \leqslant \frac{1 - \alpha}{(1 - 2\alpha)^2} \cdot \frac{1}{n} \left(1 + O\left(\frac{1}{n}\right) \right),
 \end{aligned}$$

поскольку $\binom{n}{\lceil \alpha n \rceil} (n - 2\lceil \alpha n \rceil) < \sum_{i=\lceil \alpha n \rceil}^{n - \lceil \alpha n \rceil} \binom{n}{i} < 2^n$. Пункт 1) доказан.

Теперь докажем пункт 2).

При $\alpha < \frac{1}{2}$ верно $\frac{1}{12n} < \frac{1}{12(1-\alpha)n}$, и $\frac{1}{360(\alpha n)^3} + \frac{1}{360((1-\alpha)n)^3} \leqslant \frac{1}{180(\alpha n)^3} < \frac{1}{12\alpha n}$, поэтому

$$\begin{aligned}
 \frac{1}{2^n} \binom{n}{\lceil \alpha n \rceil} &= \frac{1}{2^n} \frac{n!}{(\lceil \alpha n \rceil)!(n - \lceil \alpha n \rceil)!} < \frac{1}{2^n} \frac{1}{\sqrt{2\pi n \alpha(1-\alpha)}} \frac{1}{\alpha^{\alpha n} (1-\alpha)^{(1-\alpha)n}} \times \\
 &\times \exp \left(\frac{1}{12n} - \frac{1}{12\alpha n} - \frac{1}{12(1-\alpha)n} + \frac{1}{360(\alpha n)^3} + \frac{1}{360((1-\alpha)n)^3} \right) < \\
 &< \frac{1}{2^n} \frac{1}{\sqrt{2\pi n \alpha(1-\alpha)}} \cdot \frac{1}{\alpha^{\alpha n} (1-\alpha)^{(1-\alpha)n}} = \\
 &= \frac{1}{\sqrt{2\pi n \alpha(1-\alpha)}} \cdot \left(\frac{1}{2\alpha^\alpha (1-\alpha)^{(1-\alpha)}} \right)^n.
 \end{aligned}$$

Пусть $\beta = 1/2 - \alpha$, тогда

$$\begin{aligned}
 2\alpha^\alpha (1-\alpha)^{(1-\alpha)} &= (1-2\beta)^{\left(\frac{1}{2}-\beta\right)} (1+2\beta)^{\left(\frac{1}{2}+\beta\right)} = \\
 &= \exp \left(\left(\frac{1}{2}-\beta\right) \ln(1-2\beta) + \left(\frac{1}{2}+\beta\right) \ln(1+2\beta) \right) = \\
 &= \exp \left(\left(\frac{1}{2}-\beta\right) \left(-2\beta - \frac{(2\beta)^2}{2} - \frac{(2\beta)^3}{3} + O(\beta^4)\right) + \right. \\
 &\quad \left. + \left(\frac{1}{2}+\beta\right) \left(2\beta - \frac{(2\beta)^2}{2} + \frac{(2\beta)^3}{3} + O(\beta^4)\right) \right) = \\
 &= \exp(2\beta^2 + O(\beta^4)).
 \end{aligned}$$

Отсюда, используя приведенные выше рассуждения, получаем

$$\begin{aligned}
 \frac{1}{2^n} \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} &= \frac{1}{2^n} \binom{n}{\lceil \alpha n \rceil} \frac{1-\alpha}{1-2\alpha} \leqslant \\
 &\leqslant \frac{1}{\sqrt{2\pi n \alpha(1-\alpha)}} \cdot \left(\frac{1}{2\alpha^\alpha (1-\alpha)^{(1-\alpha)}} \right)^n \frac{1-\alpha}{1-2\alpha} \leqslant \\
 &\leqslant \sqrt{\frac{1-\alpha}{2\pi\alpha}} \frac{1}{1-2\alpha} \frac{1}{\sqrt{n}e^{\left(\frac{(1-2\alpha)^2}{2} + O((1-2\alpha)^4)\right)n}} \left(1 + O\left(\frac{1}{n}\right) \right).
 \end{aligned}$$

Пункт 2) доказан.

Теорема 3. Пусть $l \in \mathbb{N}$ и $m = m(n) \geq 2l + 1$. Тогда для достаточно больших n не существует l -РРШ кодов мощности m в следующих случаях:

- 1) l — константа и $\frac{m}{\sqrt{n}e^{n/4^{l+1}}} \rightarrow 0$ при $n \rightarrow \infty$,
- 2) $l = k \log_2 m + O(1)$ и $\lim_{n \rightarrow \infty} \frac{m^{2k}}{n} \cdot \ln n < \frac{k}{4}$,
- 3) $l = m^{\frac{1}{k}} + O(1)$ и существует $\lambda > 0$ такое, что $\lim_{n \rightarrow \infty} \frac{m}{\log_2^k n^{1/2}} \leq 1 - \lambda$,
- 4) $l = \frac{m}{4} + o(1)$ и $\lim_{n \rightarrow \infty} \frac{m}{\log_{4/3} n} < \frac{2}{3}$.

Доказательство. Покажем сначала, что удовлетворяющие условиям 1)–4) шары $(R, 0)$ и $(R, l+1)^*$ существуют.

Пусть $R = \alpha(n)n$, $\alpha(n) < \frac{1}{2}$ для всех n . Тогда для $P_R(C)$, среднего веса шара радиуса R кода C , имеем

$$P_R(C) = \frac{1}{2^n} m(n) \sum_{i=0}^R \binom{n}{i}.$$

Построим подкод C' кода C и докажем, что существует шар радиуса R веса больше $P_R(C) + l$, если выполнены условия теоремы.

Будем строить подкод C' следующим образом. В коде C найдем $l+1$ двоичных наборов ($2l+1 \leq m$), которые совпадают в наибольшем числе компонент. Обозначим число совпадающих компонент t . Оценим, каким же мы можем выбрать t .

Построим матрицу кода C размера $m \times n$ ($m = |C|$, $C \subset V^n$) следующим образом. Выпишем наборы, принадлежащие коду C , друг под другом:

$$m \left\{ \underbrace{\begin{pmatrix} \dots \\ \dots \\ \vdots \\ \dots \end{pmatrix}}_n \begin{matrix} \leftarrow v_1 \in C \\ \leftarrow v_2 \in C \\ \vdots \\ \leftarrow v_m \in C \end{matrix} \right.$$

Обозначим эту матрицу $A = A(C)$. Каждая строка матрицы A есть координатная запись некоторого набора из кода C . Найдем число подматриц матрицы A размера $(l+1) \times 1$, состоящих либо из одних нулей, либо из одних единиц (подматрицы получаем из матрицы A вычеркиванием любых $m - (l+1)$ строк и $n - 1$ столбцов). Рассмотрим i -й столбец матрицы A . Можно считать, что единиц в нем не больше чем $m/2$. Пусть число единиц в этом столбце равно $m/2 - h$, а число нулей $m/2 + h$, где h — целое или полуцелое (т. е. число вида $n + 1/2$, где n — целое) неотрицательное число. Выбрать $l+1$ строк из матрицы A с единицей в i -м столбце можно $\binom{m/2-h}{l+1}$ способами, а с нулем — $\binom{m/2+h}{l+1}$ способами. Следовательно, всего в i -м столбце содержится $b = \binom{m/2-h}{l+1} + \binom{m/2+h}{l+1}$ подматриц указанного вида.

Докажем, что число подматриц минимально, если $h = 0$.

Если m четно, то $m/2$ и h целые. Рассмотрим разность

$$\begin{aligned} & \left(\binom{m/2+h}{l+1} + \binom{m/2-h}{l+1} \right) - \left(\left(\binom{m/2+h-1}{l+1} + \binom{m/2-h+1}{l+1} \right) \right) = \\ & = \left(\binom{m/2+h}{l+1} \right) - \left(\binom{m/2+h-1}{l+1} \right) - \left(\left(\binom{m/2-h+1}{l+1} \right) - \left(\binom{m/2-h}{l+1} \right) \right) = \\ & = \left(\binom{m/2+h-1}{l} \right) - \left(\binom{m/2-h}{l} \right) > 0 \quad \text{при } h \geq 1. \end{aligned}$$

Если m нечетно, рассмотрим производную по h выражения

$$b = \binom{m/2+h}{l+1} + \binom{m/2-h}{l+1} = \\ = \frac{1}{(l+1)!} \left(\left(\frac{m}{2} + h \right) \dots \left(\frac{m}{2} + h - l \right) + \left(\frac{m}{2} - h \right) \dots \left(\frac{m}{2} + h - l \right) \right),$$

где биномиальный коэффициент с нецелыми значениями понимается как $\binom{b}{n} = \frac{b(b-1)\dots(b-n+1)}{n!}$.

Обозначим

$$x = \left(\frac{m}{2} + h \right) \dots \left(\frac{m}{2} + h - l \right), \\ y = \left(\frac{m}{2} - h \right) \dots \left(\frac{m}{2} + h - l \right).$$

Тогда

$$b' = \frac{x}{m/2+h} + \frac{x}{m/2+h-1} + \dots + \frac{x}{m/2+h-l} - \\ - \frac{y}{m/2-h} - \frac{y}{m/2-h-1} - \dots - \frac{y}{m/2-h-l} = \\ = \left(\frac{x}{m/2+h} - \frac{y}{m/2-h} \right) + \dots + \left(\frac{x}{m/2+h-l} - \frac{y}{m/2-h-l} \right).$$

Легко показать, что каждая пара слагаемых положительна при $h > 0$, равна нулю при $h = 0$ и отрицательна $h < 0$. Следовательно, b принимает минимальное значение при $h = 0$.

Итак, мы получили, что в i -м столбце имеется $b = \binom{m/2-h}{l+1} + \binom{m/2+h}{l+1} \geq 2 \binom{m/2}{l+1}$ подматриц указанного вида. Всего столбцов n , следовательно, B , число подматриц указанного вида во всей матрице A , не превосходит $2n \binom{m/2}{l+1}$.

С другой стороны, число B подматриц указанного вида в матрице A равно произведению

$$\left(\begin{array}{c} \text{число способов} \\ \text{выбрать } l+1 \text{ строку} \end{array} \right) \cdot \left(\begin{array}{c} \text{среднее число совпа-} \\ \text{дающих компонент} \end{array} \right) = \binom{m}{l+1} \cdot t' = B.$$

Поэтому найдутся $l+1$ строк, имеющих $t \geq t'$ совпадающих компонент. Значит,

$$t \geq t' \geq \frac{2n \binom{m/2}{l+1}}{\binom{m}{l+1}}.$$

Итак, у нас есть $l+1$ наборов кода C , совпадающих в t компонентах. Удалим совпадающие компоненты, получим $l+1$ набор длины $n-t$. Получили подкод $C' \subseteq V^{n-t}$ мощности $l+1$.

Для $P_R(C')$, среднего веса шара радиуса R кода C' , имеем

$$P_R(C') = \frac{1}{2^{n-t}} (l+1) \sum_{i=0}^R \binom{n-t}{i} = (l+1) - \frac{l+1}{2^{n-t}} \sum_{i=0}^{n-t-R-1} \binom{n-t}{i}.$$

Если $m(n)$ и $l+1$ такие, что при $n \rightarrow \infty$ $P_R(C) \rightarrow 0$, $P_R(C') \rightarrow (l+1)$, то для достаточно больших n не существует l -РРШ кодов в V^n мощности $m(n)$. Теперь выберем R :

$$P_R(C') \rightarrow (l+1) \implies R > \frac{1}{2}(n-t), \\ P_R(C) \rightarrow 0 \implies R < \frac{1}{2}n.$$

Следовательно,

$$\frac{1}{2} \left(1 - \frac{t}{n}\right) < \alpha(n) < \frac{1}{2}.$$

Подставляя оценку для t , получаем

$$\frac{1}{2} \left(1 - \frac{2 \binom{m/2}{l+1}}{\binom{m}{l+1}}\right) < \alpha(n) < \frac{1}{2};$$

например, можно взять

$$\alpha(n) = \frac{1}{2} - \frac{\binom{m/2}{l+1}}{2 \binom{m}{l+1}}.$$

Для этого мы построим подкод C' кода C такой, что мощность C' равна $l+1$, и докажем, что весь C' попадает в один шар требуемого радиуса.

Оценим $\beta = 1 - 2\alpha(n)$:

$$\begin{aligned} \beta &= \frac{\binom{\frac{m}{2}}{l+1}}{\binom{m}{l+1}} = \frac{(\frac{m}{2})!(m-l-1)!}{m! \left(\frac{m}{2} - l - 1\right)!} \sim \frac{1}{2^{l+1}} \cdot \left(\frac{1 - \frac{2(l+1)}{m}}{1 - \frac{l+1}{m}}\right)^{l+1} \frac{\left(1 - \frac{l+1}{m}\right)^m}{\left(1 - \frac{l+1}{\frac{m}{2}}\right)^{\frac{m}{2}}} \sqrt{\frac{m-2(l+1)}{m-l-1}} = \\ &= \frac{1}{2^{l+1}} \cdot \left(1 - \frac{l+1}{m-(l+1)}\right)^{l+1} \left(1 + \frac{l+1^2}{m(m-2(l+1))}\right)^{\frac{m}{2}} \sqrt{1 - \frac{l+1}{m-l-1}}. \end{aligned}$$

С л у ч а й 1: $l = \text{const}$. Тогда $\beta > \frac{1}{2^{l+1}} \cdot \frac{1}{2} \cdot 1$ для достаточно больших n .

Следовательно, по п. 2) леммы и условию теоремы получаем

$$\begin{aligned} P_R(C) &= \frac{1}{2^n} m(n) \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} \leq \sqrt{\frac{1-\alpha}{2\pi\alpha}} \cdot \frac{1}{\beta} \cdot \frac{1}{\sqrt{n} e^{(\beta^2/2 + O(\beta^4))n}} \left(1 + O\left(\frac{1}{n}\right)\right) < \\ &< c_0 \cdot 2^{l+2} \cdot \frac{m(n)}{\sqrt{n} e^{n/2^{2l+3}}} = c' \frac{m(n)}{\sqrt{n} e^{n/2^{2l+3}}} \xrightarrow{n \rightarrow \infty} 0. \end{aligned}$$

Значит, при достаточно больших n существует $(R, 0)$ -шар. С другой стороны,

$$\begin{aligned} P_R(C') &= (l+1) - \frac{l+1}{2^{n-t}} \sum_{i=0}^{n-t-R-1} \binom{n-t}{i} > \\ &> (l+1) - c_0 \cdot 2^{l+1} \cdot \frac{(l+1)m(n)}{\sqrt{n} e^{n/2^{2l+3}}} = \\ &= (l+1) - c' \frac{m(n)}{\sqrt{n} e^{n/2^{2l+3}}} \xrightarrow{n \rightarrow \infty} (l+1). \end{aligned}$$

Значит, при достаточно больших n существует $(R, l+1)^*$ -шар. Случай 1 доказан.

С л у ч а й 2: $l = k \log_2 m + O(1)$. В этом случае

$$\begin{aligned} \beta &\sim \frac{1}{2^{k \log_2 m + O(1)}} \cdot \left(1 - \frac{k \log_2 m}{m - k \log_2 m}\right)^{k \log_2 m + O(1)} \times \\ &\times \left(1 + \frac{k \log_2^2 m}{m(m - 2k \log_2 m)}\right)^{\frac{m}{2}} \sqrt{1 - \frac{k \log_2 m}{m - k \log_2 m}} > \frac{1}{m^k} \cdot \frac{1}{2^{O(1)}} \cdot 1, \end{aligned}$$

и, по п. 2) леммы,

$$\begin{aligned} P_R(C) &= \frac{1}{2^n} m(n) \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} \leq \sqrt{\frac{1-\alpha}{2\pi\alpha}} \cdot \frac{1}{\beta} \cdot \frac{1}{\sqrt{n} e^{(\beta^2/2 + O(\beta^4))n}} \left(1 + O\left(\frac{1}{n}\right)\right) < \\ &< c_0 2^k \cdot \frac{m(n)}{\sqrt{n} e^{n/8m^{2k}}} = c' \frac{m^{k+1}(n)}{\sqrt{n}} \frac{1}{e^{n/8m^{2k}}} \leq \\ &\leq c' \left(\frac{kn}{4 \ln n}\right)^{\frac{1}{2k}} \cdot \left(\frac{k}{4 \ln n}\right)^{\frac{1}{2}} \cdot \frac{1}{e^{\frac{4n \ln n}{8kn}}} = c'_1 \frac{1}{(\ln n)^{1/2k + 1/2}} \xrightarrow{n \rightarrow \infty} 0. \end{aligned}$$

Аналогично случаю 1 доказывается, что $P_R(C) \xrightarrow[n \rightarrow \infty]{} (l+1)$.

С л у ч а й 3: $l = m^{1/k} + O(1)$. При этом

$$\beta \sim \frac{1}{2^{m^{1/k} + O(1)}} \cdot \left(1 - \frac{m^{\frac{1}{k}}}{m - m^{\frac{1}{k}}}\right)^{m^{\frac{1}{k}} + O(1)} \left(1 + \frac{m^{\frac{2}{k}}}{m(m - 2m^{1/k})}\right)^{\frac{m}{2}} \times \\ \times \sqrt{1 - \frac{m^{\frac{1}{k}}}{m - m^{\frac{1}{k}}}} > \frac{1}{2^{m^{\frac{1}{k}} + O(1)}} \left(\frac{1}{4}\right)^{\frac{m^{1/k}}{m^{1-1/k}-1}} \cdot 1.$$

Используя п. 1) леммы, получаем

$$P_R(C) = \frac{1}{2^n} m(n) \sum_{i=0}^{[\alpha n]} \binom{n}{i} \leq \frac{1-\alpha}{\beta^2} \cdot \frac{1}{n} \left(1 + O\left(\frac{1}{n}\right)\right) < \\ < c_0 \cdot \frac{m(n)}{n} 2^{2m^{1/k} \left(1 + \frac{2}{m^{1-1/k}-1}\right)} \leq \\ \leq \frac{(1-\lambda) \log_2^k n^{1/2}}{n} n^{(1-\lambda)^{1/k}} \xrightarrow[n \rightarrow \infty]{} 0.$$

Аналогично случаю 1 доказывается, что $P_R(C) \xrightarrow[n \rightarrow \infty]{} (l+1)$.

С л у ч а й 4: $l = \frac{m}{4} + o(1)$. При этом

$$\beta = \frac{1}{2^{m/4 + o(1)}} \cdot \left(1 - \frac{1}{3}\right)^{m/4 + o(1)} \left(1 + \frac{\frac{1}{16}}{1 - \frac{1}{2}}\right)^{m/2} \sqrt{1 - \frac{1}{3}} = \left(\frac{3}{4}\right)^{3/4 m + o(1)}$$

и, по п. 1) леммы, имеем

$$P_R(C) = \frac{1}{2^n} m(n) \sum_{i=0}^{[\alpha n]} \binom{n}{i} \leq c_0 \cdot \frac{m(n)}{n} \left(\frac{4}{3}\right)^{\frac{3}{2} m + o(1)} = \frac{\lambda \log_{4/3} n}{n} n^{\frac{3}{2} \lambda} \xrightarrow[n \rightarrow \infty]{} 0$$

при $\lambda < \frac{2}{3}$. Аналогично случаю 1 доказывается, что $P_R(C) \xrightarrow[n \rightarrow \infty]{} (l+1)$.

2.3. Несуществование равномерно распределенных со степенью l кодов большой мощности.

Теорема 4. Пусть $l \in \mathbb{N}$, $s \in \mathbb{N}$, $u > 1$ — некоторое число и $m = m(n)$ такое, что $\frac{ul^2}{4} \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \leq m(n) \leq \left(\frac{n}{s^2} + a(s)\right) \frac{2^n}{\sum_{i=0}^s \binom{n}{i}}$, $s > 1$. Тогда не существует l -РРШ кодов мощности m для достаточно больших n .

В случае $s = 1$ не существует l -РРШ кодов мощности m : $\frac{ul^2}{4} \frac{2^n}{n+1} \leq m(n) \leq 2^{n-1}$ для n , удовлетворяющих следующим условиям: $(u-1)n > 3ul + u + \frac{u^2 l^2}{4}$, $n \geq 6l + 3 + \frac{ul^2}{2}$.

Доказательство. Пусть C — код размерности n , мощность которого удовлетворяет условию $|C| = m = P_s \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \leq 2^{n-1}$, где P_s — средний

вес шара радиуса s .

Предположим, что C — l -РРШ код. Обозначим минимальный вес шара радиуса s через h . Тогда максимальный вес шара радиуса s не превышает $h + l$. Пусть t_i , $i = 0, \dots, l$, — число шаров радиуса s веса $h + i$. Очевидно, что $\sum_{i=0}^l t_i = 2^n$, $\sum_{i=0}^l t_i (h + i) = m \cdot \sum_{i=0}^s \binom{n}{i}$.

Пусть K — число пар двоичных наборов кода C на расстоянии не более $2s$. С одной стороны, для каждого набора α из кода рассмотрим шар радиуса $2s$ с центром α . Все искомые наборы попадут в этот шар, а вес этого шара не менее $\lfloor P_{2s} \rfloor - l$. Значит, число пар, содержащих α , не меньше $\lfloor P_{2s} \rfloor - l$. Также рассмотрим все остальные наборы кода. Таким образом, каждая пара будет посчитана дважды. В итоге получим нижнюю оценку удвоенного числа пар:

$$2K \geq m \cdot (\lfloor P_{2s} \rfloor - l) = m \left(\left\lfloor \frac{m \sum_{i=0}^{2s} \binom{n}{i}}{2^n} \right\rfloor - l \right) \geq m \left(\frac{m}{2^n} \cdot \sum_{i=0}^{2s} \binom{n}{i} - l - 1 \right).$$

С другой стороны, каждая пара наборов на расстоянии $2s$ содержится одновременно в $\binom{2s}{s}$ шарах радиуса s , каждая пара наборов на расстоянии $2s-1$ содержится одновременно в $2\binom{2s-1}{s}$, $2\binom{2s-1}{s} = \binom{2s}{s}$, шарах радиуса s , каждая пара наборов на расстоянии менее $2s-1$ содержится одновременно в $O(n)$ шарах радиуса s . Значит, каждая пара наборов на расстоянии не более $2s$ содержится одновременно не менее чем в $\binom{2s}{s}$ шарах радиуса s . В каждом шаре радиуса s веса $h+i$ содержится $\frac{(h+i)(h+i-1)}{2}$ пар наборов на расстоянии не более $2s$. Отсюда

$$\binom{2s}{s} K \leq \sum_{i=0}^l t_i \frac{(h+i)(h+i-1)}{2}.$$

Легко проверить, что при $0 < i < j < l$ выполняется

$$\frac{(h+i)(h+i-1)}{2} + \frac{(h+j)(h+j-1)}{2} \leq \frac{(h+i-1)(h+i-2)}{2} + \frac{(h+j+1)(h+j)}{2}.$$

Следовательно,

$$\begin{aligned} \binom{2s}{s} K &\leq \sum_{i=0}^l t_i \frac{(h+i)(h+i-1)}{2} \leq \\ &\leq t'_0 \frac{h(h-1)}{2} + t'_l \frac{(h+l)(h+l-1)}{2} = \\ &= (t'_0 + t'_l) \frac{h(h-1)}{2} + t'_l \frac{2hl + l^2 - l}{2}, \end{aligned}$$

где $t'_0 + t'_l = 2^n$ и $t'_0 h + t'_l (h+l) = m \sum_{i=0}^s \binom{n}{i}$; отсюда $t'_l = \frac{m \sum_{i=0}^s \binom{n}{i} - 2^n h}{l}$.

Значит,

$$\binom{2s}{s} K \leq 2^n \frac{h(h-1)}{2} + \left(m \sum_{i=0}^s \binom{n}{i} - 2^n h \right) \frac{2h+l-1}{2}.$$

Используя оценки K сверху и снизу, имеем

$$\begin{aligned} \binom{2s}{s} m \left(\frac{m}{2^n} \cdot \sum_{i=0}^{2s} \binom{n}{i} - l - 1 \right) &\leq \\ &\leq 2 \left(2^n \frac{h(h-1)}{2} + \left(m \sum_{i=0}^s \binom{n}{i} - 2^n h \right) \frac{2h+l-1}{2} \right). \end{aligned}$$

Теперь подставим в качестве m величину $P_s \frac{2^n}{\sum_{i=0}^s \binom{n}{i}}$. Получаем

$$\begin{aligned} \binom{2s}{s} P_s^2 \cdot \frac{2^n \sum_{i=0}^{2s} \binom{n}{i}}{\left(\sum_{i=0}^s \binom{n}{i} \right)^2} - \binom{2s}{s} P_s \cdot \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} (l+1) &\leq \\ &\leq 2^n h(h-1) + (P_s \cdot 2^n - 2^n h)(2h+l-1). \end{aligned}$$

Умножим обе части неравенства на $\frac{\sum_{i=0}^s \binom{n}{i}}{2^n}$ и получим:

$$\begin{aligned} \binom{2s}{s} P_s^2 \cdot \frac{\sum_{i=0}^{2s} \binom{n}{i}}{\sum_{i=0}^s \binom{n}{i}} - \binom{2s}{s} P_s (l+1) &\leq \\ &\leq (h(h-1) + (P_s - h)(2h+l-1)) \cdot \sum_{i=0}^s \binom{n}{i}. \quad (1) \end{aligned}$$

Выразим суммы биномиальных коэффициентов через степени n (можно считать, что $\frac{n}{2} > 2s$):

$$\begin{aligned} \sum_{i=0}^s \binom{n}{i} &= \frac{n(n-1) \cdots (n-s+1)}{s!} + \frac{n(n-1) \cdots (n-s+2)}{(s-1)!} + \dots = \\ &= \frac{n^s}{s!} + \left(-\frac{1+2+\dots+(s-1)}{s!} + \frac{1}{(s-1)!} \right) n^{s-1} + O(n^{s-2}) = \\ &= \frac{n^s}{s!} + n^{s-1} \left(\frac{1}{(s-1)!} - \frac{\frac{s(s-1)}{2}}{s!} \right) + O(n^{s-2}) = \\ &= \frac{n^s + \frac{3s-s^2}{2} n^{s-1} + O(n^{s-2})}{s!}, \\ \sum_{i=0}^{2s} \binom{n}{i} &= \frac{n^{2s} + (3s-2s^2)n^{2s-1} + O(n^{2s-2})}{(2s)!}. \end{aligned}$$

Из двух последних равенств следует

$$\binom{2s}{s} \cdot \frac{\sum_{i=0}^{2s} \binom{n}{i}}{\sum_{i=0}^s \binom{n}{i}} = \frac{1}{s!} \left(n^s + \frac{3s-3s^2}{2} n^{s-1} + O(n^{s-2}) \right).$$

Теперь подставим полученные равенства в неравенство (1):

$$\begin{aligned} \frac{1}{s!} \left(n^s + \frac{3s-3s^2}{2} n^{s-1} + O(n^{s-2}) \right) P_s^2 - \binom{2s}{s} P_s (l+1) &\leq \\ &\leq (h(h-1) + (P_s - h)(2h+l-1)) \frac{1}{s!} \left(n^s + \frac{3s-s^2}{2} n^{s-1} + O(n^{s-2}) \right). \end{aligned}$$

Разделим обе части равенства на $\frac{n^{s-1}}{s!}$:

$$\begin{aligned} \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) P_s^2 - \frac{(2s)!}{s!} \frac{P_s}{n^{s-1}} (l+1) &\leq \\ &\leq (h(h-1) + (P_s - h)(2h+l-1)) \left(n + \frac{3s-s^2}{2} + O\left(\frac{1}{n}\right) \right). \end{aligned}$$

Из условия теоремы следует, что $\frac{P_s}{n^{s-1}} \leq P_s^2 \cdot O\left(\frac{1}{n}\right)$ при $s > 1$. Значит, слагаемым $\frac{(2s)!}{s!} \frac{P_s}{n^{s-1}} (l+1)$ при $s > 1$ можно пренебречь. Случай $s = 1$ рассмотрим отдельно позже. Перегруппируем члены:

$$\begin{aligned} & \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) (P_s - h)(P_s - h - l) + \\ & + (2P_s h + P_s l - h^2 - hl) \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) + \\ & + (2P_s h + P_s l - P_s - h^2 - hl) \left(-n - \frac{3s-s^2}{2} - O\left(\frac{1}{n}\right) \right) \leq 0, \end{aligned}$$

или

$$\begin{aligned} & \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) (P_s - h)(P_s - h - l) + \\ & + P_s \left(n + \frac{3s-s^2}{2} + O\left(\frac{1}{n}\right) - (h+l) \left(s^2 + O\left(\frac{1}{n}\right) \right) \right) + \\ & + h(h+l-P_s) \left(s^2 + O\left(\frac{1}{n}\right) \right) \leq 0. \end{aligned}$$

Для того чтобы доказать несуществование l -РРШ кодов, покажем, что в условиях теоремы левая часть неравенства больше нуля.

Из того, что $P_s^2 - 2P_s h + h^2 + hl \geq 0$, следует, что

$$\begin{aligned} & \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) (P_s - h)(P_s - h - l) + \\ & + P_s \left(n + \frac{3s-s^2}{2} + O\left(\frac{1}{n}\right) - (h+l) \left(s^2 + O\left(\frac{1}{n}\right) \right) \right) + \\ & + h(h+l-P_s) \left(s^2 + O\left(\frac{1}{n}\right) \right) \geq \\ & \geq \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) (P_s - h)(P_s - h - l) + \\ & + s^2 P_s \left(\frac{n}{s^2} + \frac{3-s}{2s} + O\left(\frac{1}{n}\right) - l - P_s + O\left(\frac{P_s}{n}\right) \right). \end{aligned}$$

Из свойств параболы получим следующие неравенства. Во-первых, для любого P_s

$$(P_s - h)(P_s - h - l) \geq -\frac{l^2}{4},$$

во-вторых, если выполнено

$$\frac{ul^2}{4} \leq P_s \leq \frac{n}{s^2} + \text{const}(s) - \frac{ul^2}{4} \leq \frac{n}{s^2} + a(s),$$

то

$$s^2 P_s \left(\frac{n}{s^2} + \frac{3-s}{2s} + O\left(\frac{1}{n}\right) - l - P_s + O\left(\frac{P_s}{n}\right) \right) \geq s^2 \frac{ul^2}{4} \left(\frac{n}{s^2} + O(1) \right).$$

Значит, требуется выполнение соотношения

$$-\frac{l^2}{4} (n + O(1)) + \frac{ul^2}{4} (n + O(1)) \geq 0.$$

Это неравенство выполняется при $u > 1$ для достаточно больших n .

Теперь рассмотрим случай $s = 1$. Как было получено выше,

$$\begin{aligned} \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) P_s^2 - \frac{(2s)!}{s!} \frac{P_s}{n^{s-1}} (l+1) &\leq \\ &\leq (h(h-1) + (P_s - h)(2h+l-1)) \left(n + \frac{3s-s^2}{2} + O\left(\frac{1}{n}\right) \right). \end{aligned}$$

При $s = 1$ получаем

$$nP_1^2 - 2P_1(l+1) \leq (h(h-1) + (P_1 - h)(2h+l-1))(n+1).$$

Перегруппируем члены:

$$n(P_1 - h)(P_1 - h - l) + P_1(n - h - 3l - 1) + h(h + l - P_1) \leq 0.$$

Для того чтобы доказать несуществование l -РРШ кодов, покажем, что в условиях теоремы левая часть неравенства больше нуля. Во-первых,

$$n(P_1 - h)(P_1 - h - l) \geq -n \frac{l^2}{4}.$$

Во-вторых,

$$P_1(n - h - 3l - 1) + h(h + l - P_1) \geq P_1(n - 3l - 1 - P_1).$$

При $n \geq 6l + 3 + \frac{ul^2}{2}$ имеем $n - 3l - 1 \geq \frac{ul^2}{4} + \frac{n+1}{2}$. Отсюда

$$P_1(n - 3l - 1 - P_1) \geq u \frac{l^2}{4} \left(n - 3l - 1 - u \frac{l^2}{4} \right).$$

Следовательно,

$$\begin{aligned} n(P_1 - h)(P_1 - h - l) + P_1(n - h - 3l - 1) + h(h + l - P_1) &= \\ = -n \frac{l^2}{4} + u \frac{l^2}{4} \left(n - 3l - 1 - u \frac{l^2}{4} \right) &= \frac{l^2}{4} \left(-n + un - 3ul - u - \frac{u^2 l^2}{4} \right) \geq 0, \end{aligned}$$

для $u > 1$, $(u-1)n > 3ul + u + \frac{u^2 l^2}{4}$. Теорема доказана.

Эта теорема доказывает несуществование l -РРШ кодов для следующих интервалов мощностей:

$$\begin{aligned} s=1: \quad & \frac{ul^2}{4} \cdot \frac{2^n}{n+1} \leq m(n) \leq 2^{n-1}; \\ s=2: \quad & \frac{ul^2}{4} \cdot \frac{2^n}{n^2 + O(n)} \leq m(n) \leq \frac{2^n}{4n + O(1)}; \\ s=3: \quad & \frac{ul^2}{4} \cdot \frac{2^n}{n^3 + O(n^2)} \leq m(n) \leq \frac{2^n}{9n^2 + O(n)}; \\ & \dots \dots \dots \\ s: \quad & \frac{ul^2}{4} \cdot \frac{2^n}{n^s + O(n^{s-1})} \leq m(n) \leq \frac{2^n}{s^2 n^{s-1} + O(n^{s-2})}. \end{aligned}$$

Остается открытым вопрос существования l -РРШ кодов в следующих интервалах:

$$\begin{aligned} \frac{2^n}{4n + O(1)} \leq m(n) \leq ul^2 \cdot \frac{2^n}{4n + O(1)}, \\ \frac{2^n}{9n^2 + O(n)} \leq m(n) \leq ul^2 \cdot \frac{2^n}{4n^2 + O(n)}, \\ \dots \dots \dots \\ \frac{2^n}{s^2 n^{s-1} + O(n^{s-2})} \leq m(n) \leq ul^2 \cdot \frac{2^n}{4n^{s-1} + O(n^{s-2})}. \end{aligned}$$

Теорема 3 доказывает несуществование l -РРШ кодов мощности m , удовлетворяющих условиям $\frac{m}{\sqrt{n}e^{n/4^{l+1}}} \xrightarrow{n \rightarrow \infty} 0$, т. е. $m \ll \sqrt{n} \cdot e^{n/4^{l+1}} = o\left(\frac{2^n}{n^s}\right)$ для любого s .

§ 3. Оценка для l -упаковки большого радиуса

В этом параграфе рассматриваются l -упаковки большого радиуса. Если при передаче кодового слова в нем произошло не более R ошибок, мы сможем декодировать его списком из l элементов, содержащим кодовое слово.

О п р е д е л е н и е 2. Код C называется l -упаковкой, если каждый шар радиуса R содержит не более чем l наборов из кода C .

Наша цель — для l -упаковки C найти зависимость между ее мощностью и радиусом R . Рассматривается случай $R = \tau n$ (τ не зависит от n), где $\tau > \frac{1}{4}$, причем ищутся оценки вида $\tau > f(m)$ или $m > f(\tau)$, при выполнении которых обязательно существует шар веса $l+1$ радиуса τ для кода C мощности m для любого n , т. е. не существует l -упаковки с таким соотношением параметров. Случай $\tau < \frac{1}{4}$ подробно изучался, например, в [9, 10]; для случая $\tau > \frac{1}{4}$ автору известно только неравенство Плоткина $m > 1 + \frac{1}{4\tau-1}$ для $l=1$.

Т е о р е м а 5. Для достаточно больших n не существует l -упаковок при следующих соотношениях параметров:

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

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

Или, при $\frac{1}{2} - \frac{1}{2^{l+1}} < \tau < \frac{1}{2}$, получаем

$$m > \frac{\frac{l(l+1)}{2}}{(2\tau-1)2^l+1} + \frac{l(l+1)}{2} + \text{const} \cdot 2^l \left(2\tau - 1 + \frac{1}{2^l} \right),$$

где const — некоторая константа, зависящая от l .

З а м е ч а н и е. Заметим, что $m \rightarrow \infty$ при $\tau \rightarrow \frac{1}{2} - \frac{1}{2^{l+1}}$.

При конкретных малых l эти условия приобретают следующий вид. При $l=1$ — это в точности неравенство Плоткина; при $l=2$

$$\tau > \frac{3}{8} \left(1 + \frac{1}{m-1} \right), \text{ или } m > 1 + \frac{3}{8\tau-3};$$

при $l=3$

$$\tau > \frac{1}{16} \left(7 + \frac{6m-21}{m^2-4m+3} \right)$$

или, после приведения к общему знаменателю и выделения полного квадрата

$$m > 2 + \frac{3}{16\tau-7} + \sqrt{\left(\frac{3}{16\tau-7} - \frac{3}{2} \right)^2 - \frac{5}{4}};$$

при $l = 4$

$$\tau > \frac{1}{32} \left(15 + \frac{10m - 45}{m^2 - 4m + 3} \right) \text{ или } m > 2 + \frac{5}{32\tau - 15} + \sqrt{\left(\frac{5}{32\tau - 15} - \frac{5}{2} \right)^2 - \frac{21}{4}};$$

при $l \geq 5$ получается уравнение степени не меньше 3 (степень уравнения равна $\lceil l/2 \rceil$). Для каждого конкретного l приведем неравенство к виду

$$m^{\lceil l/2 \rceil} (2^{l+1}\tau - 2^l + 1) + \dots \geq 0.$$

Если $m_0(\tau)$ — старший корень этого уравнения, то при $m \geq m_0$ не существует l -упаковок мощности m .

Доказательство теоремы 5. Докажем, что при данных условиях существует шар радиуса $R = \lceil \tau n \rceil$ веса больше l . Для этого мы построим подкод C' кода C такой, что мощность C' равна $(l+1)$, и докажем, что весь C' попадает в один шар требуемого радиуса.

Будем строить подкод C' следующим образом. В коде C выберем $l+1$ двоичных наборов ($2l+1 \leq m$), которые совпадают хотя бы в t компонентах, где (см. доказательство теоремы 3)

$$t \geq \frac{2n \binom{m/2}{l+1}}{\binom{m}{l+1}}.$$

Для $P_R(C')$ — среднего веса шара радиуса R кода C' — выполняется соотношение

$$P_R(C') = \frac{1}{2^{n-t}} (l+1) \sum_{i=0}^R \binom{n-t}{i} = (l+1) - \frac{l+1}{2^{n-t}} \sum_{i=0}^{n-t-R-1} \binom{n-t}{i}.$$

Чтобы накрыть весь C' одним шаром, радиус шара должен удовлетворять следующему условию (так как $\frac{1}{2^n} \sum_{i=0}^{\lceil \alpha n \rceil} \binom{n}{i} \xrightarrow{n \rightarrow \infty} 0$ при $\alpha < \frac{1}{2}$):

$$R > \frac{1}{2}(n-t), \quad \text{т. е. } \tau > \frac{1}{2} \left(1 - 2 \frac{\binom{m/2}{l+1}}{\binom{m}{l+1}} \right).$$

При $l = 1$ это в точности соответствует неравенству Плоткина, а при $l > 1$

$$\frac{\binom{m/2}{l+1}}{\binom{m}{l+1}} = \frac{1}{2^{l+1}} \frac{1 \left(1 - \frac{2}{m}\right) \left(1 - \frac{4}{m}\right) \dots \left(1 - \frac{2l}{m}\right)}{1 \left(1 - \frac{1}{m}\right) \left(1 - \frac{2}{m}\right) \dots \left(1 - \frac{l}{m}\right)} \geq \frac{1}{2^{l+1}} \left(1 - \frac{\frac{l(l+1)}{2}}{m - \frac{l(l+1)}{2} + \frac{\text{const}}{m^2}} \right).$$

Обозначим $C_0 = \frac{l(l+1)}{2}$. Тогда получим

$$\begin{aligned} R > \frac{1}{2}(n-t) &= \frac{1}{2} \left(n - \frac{2n}{2^{l+1}} \left(1 - \frac{C_0}{m - C_0} + \frac{\text{const}}{m^2} \right) \right) = \\ &= \frac{1}{2} n \left(1 - \frac{1}{2^l} + \frac{1}{2^l} \frac{C_0}{m - C_0} + \frac{\text{const}}{m^2} \right). \end{aligned}$$

Применяя выражения для τ , с помощью преобразований получим

$$2\tau - \left(1 - \frac{1}{2^l} \right) > \frac{1}{2^l} \left(\frac{C_0}{m - C_0} + \frac{\text{const}}{m^2} \right),$$

$$\frac{1}{(2\tau - 1)2^l + 1} < \frac{m - C_0}{C_0 + \text{const} \cdot 2^l \left(2\tau - 1 + \frac{1}{2^l} \right)},$$

$$m > \frac{\frac{l(l+1)}{2}}{(2\tau - 1)2^l + 1} + \frac{l(l+1)}{2} + \text{const} \cdot 2^l \left(2\tau - 1 + \frac{1}{2^l} \right).$$

§ 4. Неравенства для параметров матриц специального вида

В этом параграфе рассматриваются матрицы специального вида, введенные в [21] и использующиеся для построения устойчивых функций с криптографически оптимальными параметрами. Для этих матриц устанавливается нижняя оценка для представляющего большой интерес отношения их параметров, а также показывается, что существует последовательность матриц, для которой предел отношения этих параметров равен нижней оценке.

Различные типы шифраторов используют булевы функции. Так, поточные шифраторы, основанные на регистрах сдвига с линейной обратной связью (LFSR), используют булевы функции в качестве нелинейных комбинаторов или нелинейных фильтров, блочные шифраторы используют булевы функции в «ящиках подстановок» и т. д. Булевы функции, используемые в шифраторах, должны удовлетворять некоторым специфическим свойствам для того, чтобы успешно противостоять различным криптографическим атакам.

Одно из наиболее важных желательных свойств булевых функций в поточных шифраторах, основанных на LFSR, это *корреляционная иммунность*, введенная Зигенталером [19]. Корреляционно-иммунные функции, на выходе которых нули и единицы встречаются с одинаковой частотой, называются *устойчивыми*. Другими важными свойствами являются нелинейность, алгебраическая степень и т. д.

Наиболее важной теоретической мотивацией для исследования высоко нелинейных устойчивых булевых функций является использование таких функций в качестве нелинейных комбинаторов в поточных шифраторах. Но с практической точки зрения число переменных в таких системах не может быть слишком велико (в противном случае ключ будет слишком длинным). При этом нужно заметить, что все важные функции с маленьким числом переменных уже найдены полным перебором, и исследовать таким образом, как будто бы уже нечего.

В то же самое время другим важным практическим типом являются поточные шифраторы, использующие булевы функции в качестве нелинейных фильтров. Здесь, вообще говоря, уже можно использовать функции с большим числом переменных. Но главные проблемы здесь заключаются в том, что эффективные (с точки зрения реализации) конструкции таких функций не могут быть найдены полным перебором, а также в том, что как было показано в [13], поточные шифраторы такого типа могут быть трансформированы при их анализе в эквивалентные (в некотором смысле) с худшей устойчивостью, но с той же нелинейностью, что облегчает атаки на них.

Приведенные соображения подчеркивают важность прямых эффективных конструкций булевых функций с большим числом переменных и оптимальным соотношением устойчивости и нелинейности.

Корреляционная иммунность (или устойчивость) — это свойство, важное в криптографии не только для поточных шифраторов. Это свойство является важным, если мы хотим, чтобы знание некоторого заданного числа входных разрядов не давало никакой (статистической) информации о выходном разряде.

Такой подход к рассмотрению этих функций применяется в [11, 12] и других работах.

В работах [18, 20, 22] было независимо доказано, что нелинейность m -устойчивой функции от n переменных не превосходит $2^{n-1} - 2^{m+1}$ при $m \leq n-1$. Было доказано, что если эта граница достигается, то $m > 0.5n - 2$. В работе [20] было доказано, что если эта граница достигается, то алгебраическая степень функции также является максимально возможной (т. е.

достигается равенство в *неравенстве Зигенталера*) и равна $n - t - 1$. В работах [17, 20, 21] построены эффективные конструкции t -устойчивых функций от n переменных с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$ при $m \geq \frac{2n-7}{3}$, $m \geq \frac{2n-9}{3}$ и $m \geq 0.6n - 1$, соответственно. Для того, чтобы получить этот результат, в [21] было введено понятие *подходящей* (k_0, k, p, t) -матрицы. В [21] было указано, что очень важной задачей является нахождение подходящей (k, k, p, t) -матрицы, в которой соотношение $\frac{t}{t+k}$ мало настолько, насколько это возможно. В работе [21] был приведен пример подходящей $(4, 4, 6, 6)$ -матрицы, для которой это отношение равно 0.6. В то же самое время вопрос о наименьшем возможном значении отношения $\frac{t}{t+k}$ для подходящих матриц был сформулирован в [21] как открытая проблема.

В настоящем параграфе исследуется проблема нахождения наименьшего возможного значения отношения $\frac{t}{t+k}$ для подходящих матриц и устанавливается, что это отношение не может быть меньше, чем $\frac{1}{\log_2(\sqrt{5}+1)} = 0.5902\dots$ В то же самое время строится последовательность подходящих матриц, приближающих эту нижнюю границу со сколь угодно большой точностью.

Определение 3 [21]. 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 $\sum_{j=1}^p b_{ij} \leq t$ (символы $*$ не дают в суммы никакого вклада);

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

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

Обозначим подходящую (k_0, k, p, t) -матрицу через $B_{k_0, k, p, t}$. В [21] приведены следующие примеры подходящих матриц:

$$\begin{aligned}
 B_{1,0,1,1} &= (1), \quad B_{1,1,1,2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \\
 B_{3,2,3,3} &= \begin{pmatrix} 2 & 1 & * \\ * & 2 & 1 \\ 1 & * & 2 \\ 1 & 1 & 1 \end{pmatrix}, \quad B_{3,3,4,5} = \begin{pmatrix} * & 1 & 2 & 2 \\ 2 & * & 1 & 2 \\ 2 & 2 & * & 1 \\ 1 & 2 & 2 & * \\ 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}, \\
 B_{4,4,6,6} &= \begin{pmatrix} 2 & 2 & 2 & * & * & * \\ 1 & 2 & * & 1 & 2 & * \\ 1 & 2 & * & * & 1 & 2 \\ 1 & 2 & * & 2 & * & 1 \\ * & 1 & 2 & 1 & 2 & * \\ * & 1 & 2 & * & 1 & 2 \\ * & 1 & 2 & 2 & * & 1 \\ 2 & * & 1 & 1 & 2 & * \\ 2 & * & 1 & * & 1 & 2 \\ 2 & * & 1 & 2 & * & 1 \\ 2 & * & 1 & 1 & 1 & 1 \\ 1 & 2 & * & 1 & 1 & 1 \\ * & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & * & 1 \\ 1 & 1 & 1 & 1 & 2 & * \\ 1 & 1 & 1 & * & 1 & 2 \end{pmatrix}.
 \end{aligned}$$

Подходящие матрицы используются в [21] для построения булевых функций с высокой устойчивостью. В частности, если существует подходящая (k, k, p, t) -матрица, то для $n - 2 \geq m \geq \frac{t}{t+k} n(1 + o(1))$ можно построить m -устойчивую функцию от n переменных с максимально возможной нелинейностью $2^{n-1} - 2^{m+1}$. Поэтому представляют интерес подходящие матрицы с как можно меньшей величиной отношения $\frac{t}{t+k}$, особенно в случае $k_0 = k$. Заметим, что из матриц, построенных в [21], наименьшей величиной отношения $\frac{t}{t+k}$ обладает матрица $B_{4,4,6,6}$, для которой $\frac{t}{t+k} = 0.6$. В [21] задача построения подходящих матриц с $\frac{t}{t+k} < 0.6$ и задача нахождения минимума этого отношения сформулированы как открытые проблемы. В настоящем параграфе решаются эти проблемы.

Теорема 6. *Не существует подходящей (k_0, k, p, t) -матрицы при $\frac{t}{t+k} < \frac{1}{\log_2(\sqrt{5}+1)} = 0.5902\dots$*

Доказательство. Булевым кубом B^p назовем множество всех наборов вида $(x_1, \dots, x_p)$, где $x_i \in \{1, 2\}$, l -м слоем булева куба называется множество наборов с l единицами. Мощность l -го слоя равна $\binom{p}{l}$. Подкуб булева куба $(B^p)^{\sigma_1, \dots, \sigma_k}_{i_1, \dots, i_k} = \{(x_1, \dots, x_p) : x_{i_j} = \sigma_j, j = 1, \dots, k\}$. Подкуб можно задать строкой $b = b((B^p)^{\sigma_1, \dots, \sigma_k}_{i_1, \dots, i_k}) = (b_1, \dots, b_p)$, где $b_i \in \{1, 2, *\}$ и $b_i = \sigma_i$, если $i \in \{i_1, \dots, i_k\}$, иначе $b_i = *$.

Из определения подходящей матрицы следует, что если не существует подходящей (k_0, k, p, t) -матрицы, то не существует и подходящей (k'_0, k, p, t) -матрицы для любого $k'_0 < k_0$. Поэтому теореме достаточно доказать для $k_0 = t$.

Возьмем произвольную подходящую (t, k, p, t) -матрицу. Рассмотрим ее как множество непересекающихся подкубов булева куба размерности p , считая каждую строку матрицы подкубом. Подкубы не пересекаются в силу свойства (а) подходящей матрицы. Если t четно, заменим в строках с нечетным числом единиц одну звездочку на единицу (в случае отсутствия в строке * припишем к матрице столбец из одних звездочек). При этом число подкубов, которые можно поместить в булев куб без пересечений, не уменьшится. Если t нечетно, аналогично поступим со строками с четным числом единиц. Теперь при четном t у нас есть строки только с четным числом единиц, а при нечетном — с нечетным. Если в матрице остались строки с суммой единиц и двоек, меньшей $t - 1$, будем заменять в них звездочки на двойки до тех пор, пока сумма единиц и двоек не станет больше $t - 1$. Рассмотрим подкуб, заданный строкой, в которой ровно s двоек и ровно k единиц. В l -й слой попадет $\binom{p-s-k}{l-k}$ наборов подкуба, если $l = k, \dots, p-s$, и ни одного набора при остальных l . Пусть t четно (для нечетного t выкладки аналогичны). Рассмотрим l -й слой булева куба. В него попадет $\binom{p-t/2}{l}$ наборов из каждого подкуба, заданного строкой, в которой ровно $t/2$ двоек и ровно 0 единиц, $\binom{p-t/2-1}{l-2}$ наборов из каждого подкуба, заданного строкой, в которой ровно $t/2 - 1$ двоек и ровно две единицы, и т. д. Обозначим число строк матрицы с i единицами через c_i . Тогда для любого l , $l = 0, 1, \dots, p$, выполнено неравенство

$$\sum_{i=0}^{t/2} c_{2i} \binom{p-t/2-i}{l-2i} \leq \binom{p}{l}.$$

Отсюда

$$\sum_{i=0}^{t/2} c_{2i} \frac{(p-t/2-i)!}{(l-2i)!(p-t/2-l+i)!} \leq \frac{p!}{l!(p-l)!}.$$

Заметим, что из подходящей (k_0, k, p, t) -матрицы добавлением столбцов из одних звездочек можно получить подходящую (k_0, k, p', t) -матрицу для любого $p' > p$. Следовательно, если не существует подходящей (k_0, k, p', t) -матрицы, то не существует и подходящей (k_0, k, p, t) -матрицы для любого $p < p'$. Поэтому в дальнейшем считаем p сколь угодно большим.

Пусть l целое. Обозначим $\alpha = l/p$. Тогда

$$\begin{aligned} \sum_{i=0}^{t/2} c_{2i} \frac{(p-\frac{t}{2}-i) \dots (p-\frac{t}{2}-\frac{t}{2}+1)}{(\alpha p-2i) \dots (\alpha p-t+1)(p(1-\alpha)-\frac{t}{2}+1) \dots (p(1-\alpha)-\frac{t}{2}+i)} &\leq \\ &\leq \frac{p(p-1) \dots (p-\frac{t}{2}-\frac{t}{2}+1)}{\alpha p(\alpha p-1) \dots (\alpha p-t+1)(p(1-\alpha)-\frac{t}{2}+1) \dots (p(1-\alpha)-1)(p(1-\alpha))}. \end{aligned}$$

Раскрывая скобки, имеем

$$\begin{aligned} \sum_{i=0}^{t/2} c_{2i} \frac{p^{t/2-i} + a_i^1 p^{t/2-i-1} + \dots}{((\alpha p)^{t-2i} + a_i^2 (\alpha p)^{t-2i-1} + \dots) (((1-\alpha)p)^i + a_i^3 ((1-\alpha)p)^{i-1} + \dots)} &\leq \\ &\leq \frac{p^t + b^1 p^{t-1} + \dots}{((\alpha p)^t + b^2 (\alpha p)^{t-1} + \dots) ((p(1-\alpha))^{t/2} + b^3 (p(1-\alpha))^{t/2-1} + \dots)}, \end{aligned}$$

где $a_i^1, a_i^2, a_i^3, b^1, b^2, b^3$ — числа, не зависящие от p .

Умножим обе части этого неравенства на $p^{t/2}\alpha^t$ и преобразуем дроби. Получаем

$$\begin{aligned} \sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha} \right)^i (1 + a_i/p + O(1/p^2)) &\leq \\ &\leq (1 + \max\{a_i\}/p + O(1/p^2)) \sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha} \right)^i \leq \\ &\leq \frac{1}{(1-\alpha)^{t/2}} (1 + b/p + O(1/p^2)), \end{aligned}$$

где a_i, b не зависят от p . Далее,

$$\begin{aligned} \sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha} \right)^i &\leq \frac{1}{(1-\alpha)^{t/2}} \frac{(1 + b/p + O(1/p^2))}{(1 + \max\{a_i\}/p + O(1/p^2))} \leq \\ &\leq \frac{1}{(1-\alpha)^{t/2}} (1 + b'/p + O(1/p^2)). \end{aligned}$$

Отсюда, учитывая, что мы можем взять p сколь угодно большим при фиксированных остальных параметрах, имеем

$$\sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha} \right)^i \leq \frac{1}{(1-\alpha)^{t/2}}.$$

Чтобы найти сумму c_i , возьмем $\alpha = \frac{\sqrt{5}-1}{2}$ (корень уравнения $\frac{\alpha^2}{1-\alpha} = 1$). Это число является иррациональным, однако мы его можем приблизить последовательностью рациональных чисел. Выберем последовательности l и p так, чтобы $l/p \rightarrow \frac{\sqrt{5}-1}{2}$. В результате для любых k_0 получаем

$$\sum_{i=0}^{\lfloor k_0/2 \rfloor} c_{2i} \leq \left(\frac{\sqrt{5}+1}{2} \right)^t.$$

Следовательно, $k \leq \log_2 \sum_{i=0}^{\lfloor k_0/2 \rfloor} c_{2i} \leq \log_2 \left(\frac{\sqrt{5}+1}{2} \right)^t$ и $\frac{t}{t+k} \geq \frac{1}{\log_2(\sqrt{5}+1)}$.

Теорема доказана.

Теорема 7. Для любого $\varepsilon > 0$ существует подходящая (k, k, p, t) -матрица, для которой $\frac{t}{t+k} < \frac{1}{\log_2(\sqrt{5}+1)} + \varepsilon$.

Доказательство. Построим сначала рекуррентно последовательность матриц, удовлетворяющих свойствам (а), (б) подходящих матриц, и число строк в которых не обязательно степень двойки. Обозначим число строк матрицы, полученной на шаге t , через $s(t)$.

На шаге t строим матрицу с суммой единиц и двоек не более t . Пусть у нас уже построены матрицы A_{t-1} и A_{t-2} с числом строк $s(t-1)$ и $s(t-2)$, удовлетворяющие свойствам подходящих матриц с максимальной суммой чисел в строке $(t-1)$ и $(t-2)$ соответственно. Будем считать, что матрицы A_{t-1} и A_{t-2} имеют одинаковое число столбцов (если это не так, припишем к одной из них столбцы из одних звездочек). Добавим к каждой из этих матриц справа по одному столбцу: к матрице A_{t-1} — из одних единиц, а к матрице A_{t-2} — из двоек. Напишем получившиеся матрицы одну над другой. Получившуюся матрицу назовем матрицей $A_t = \begin{pmatrix} A_{t-1} & 1 \\ A_{t-2} & 2 \end{pmatrix}$.

Матрица A_t является матрицей требуемого вида с максимальной суммой чисел в строке, не превосходящей t , и числом строк

$$s(t) = s(t-2) + s(t-1).$$

Значит, $s(t)$ образует последовательность Фибоначчи, и $s(t)$ асимптотически равно $\frac{1}{\sqrt{5}} \cdot \left(\frac{\sqrt{5}+1}{2}\right) \cdot \left(\frac{\sqrt{5}+1}{2}\right)^t$, если в качестве начальных взять матрицы $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$. При таком построении в матрице могут быть строки с числом единиц большим $k = \lfloor \log_2 s(t) \rfloor - 1$. Найдем отношение числа строк с числом единиц большим k к числу всех строк. Обозначим $l_j(t)$ число строк с j единицами в матрице A_t . По построению $l_0(t) = l_0(t-2)$, $l_j(t) = l_j(t-2) + l_{j-1}(t-1)$ для $j \geq 1$. Из рекуррентных соотношений следует, что

$$l_j(t) = \binom{\frac{t+j-2}{2}}{j} l_0(2) + \binom{\frac{t+j-4}{2}}{j-1} l_1(1) + a_2 l_2(b_2) + \dots + a_j l_j(b_j),$$

если $t+j$ чётно, и

$$l_j(t) = \binom{\frac{t+j-3}{2}}{j} l_0(1) + \binom{\frac{t+j-3}{2}}{j-1} l_1(2) + a_2 l_2(b_2) + \dots + a_j l_j(b_j),$$

если $t+j$ нечётно, где $a_2, \dots, a_j$ — некоторые числа, а $b_2, \dots, b_j$ равны 1 или 2 в зависимости от чётности $t+j$. Для рассматриваемых начальных матриц $l_0(1)=0$, $l_0(2)=1$, $l_1(1)=l_1(2)=1$, $l_j(1)=l_j(2)=0$ для $j \geq 2$. Следовательно,

$$l_j(t) = \binom{\frac{t+j-2}{2}}{j} + \binom{\frac{t+j-4}{2}}{j-1},$$

если $t+j$ чётно, и

$$l_j(t) = \binom{\frac{t+j-3}{2}}{j-1},$$

если $t+j$ нечётно.

Несложно проверить, что

$$\binom{\frac{t+j-2}{2}}{j} + \binom{\frac{t+j-4}{2}}{j-1} = \binom{\frac{t+j-2}{2}}{j} \left(1 + \frac{2j}{t+j-2}\right) \leq 3 \binom{\frac{t+j-2}{2}}{j}$$

при $t \geq 2$, $j \geq 2$ и

$$\frac{\binom{\frac{t+j-2}{2}}{j}}{\binom{\frac{t+j}{2}}{j+2}} = \frac{(j+1)(j+2)}{\frac{t+j}{2} \left(\frac{t-j}{2} - 1\right)} \geq 1,$$

если $j \geq -\frac{7}{5} + \sqrt{\frac{9}{25} + \frac{1}{5}t(t-2)}$. Отсюда

$$\frac{\sum_{j=k+1}^t l_j(t)}{s(t)} \leq \text{const} \frac{\sum_{j=k+1}^t \binom{\lfloor \frac{t+j}{2} \rfloor - 1}{j}}{\left(\frac{\sqrt{5}+1}{2}\right)^t} \leq \text{const} \frac{(t-k) \binom{\lfloor \frac{t+k-1}{2} \rfloor}{k+1}}{\left(\frac{\sqrt{5}+1}{2}\right)^t} \leq$$

(при $k = \lfloor t \log_2 \left(\frac{\sqrt{5}+1}{2} \right) + \log_2 \left(\frac{\sqrt{5}+1}{2\sqrt{5}} \right) - 1 \rfloor$, обозначив $v = \log_2 \left(\frac{\sqrt{5}+1}{2} \right)$ и используя формулу Стирлинга)

$$\begin{aligned} &\leq \text{const} \cdot t \frac{\sqrt{\frac{t(1+v)/2}{tv(t/2+v/2-v)}} \frac{\left(\frac{1}{2}t(1+v)\right)^{t(1+v)/2}}{(tv)^{tv} \left(\frac{1}{2}t(1-v)\right)^{t(1-v)/2}} = \\ &= \text{const} \sqrt{t} \frac{(1+v)^{t(1+v)/2}}{(2v)^{tv} (1-v)^{t(1-v)/2} \left(\frac{\sqrt{5}+1}{2}\right)^t} = \\ &= \text{const} \sqrt{t} \left(\frac{(1+v)^{(1+v)/2}}{\left(\frac{\sqrt{5}+1}{2}\right)^2 v^v (1-v)^{(1-v)/2}} \right)^t. \\ &\qquad\qquad\qquad = 0.92 \dots < 1 \end{aligned}$$

Таким образом, в матрице A_t количество строк с числом единиц, большим k , по отношению к числу всех строк мало. Выкинем из матрицы A_t строки с числом единиц большим k . Так как их количество при больших t меньше 2^k , то в матрице, в силу выбора k , останется не менее 2^k строк. Теперь матрица удовлетворяет свойству (в) подходящей матрицы при $k_0 = k$. Затем выкинем еще несколько любых строк, чтобы число строк стало равным 2^k . Тем самым мы построили подходящую (k, k, p, t) -матрицу для некоторого p .

Таким образом, при $t \rightarrow \infty$ для построенной так последовательности подходящих (k, k, p, t) -матриц

$$\frac{t}{t+k} = \frac{t}{t + \lfloor t \log_2 \left(\frac{\sqrt{5}+1}{2} \right) + \log_2 \left(\frac{\sqrt{5}+1}{2\sqrt{5}} \right) - 1 \rfloor} \rightarrow \frac{1}{\log_2(\sqrt{5}+1)}.$$

Отсюда следует утверждение теоремы.

Автор выражает благодарность научному руководителю Ю. В. Таранникову за постановку задач, внимание к работе и ценные советы.

СПИСОК ЛИТЕРАТУРЫ

1. Гаврилов Г. П., Сапоженко А. А. Сборник задач по дискретной математике. — М.: Наука, 1977.
2. Таранников Ю. В. О классе булевых функций, равномерно распределенных по шарам со степенью 1 // Вестник МГУ. Математика. Механика. — 1997. — № 5. — С. 18–22.
3. Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — М.: Наука, С. 91–148
4. Федорова М. С. О соотношениях между параметрами матриц специального вида // Современные исследования математики и механики. Тр. XXIII конф. молодых ученых мех-мат фак-та МГУ (9–14 апреля 2001 г.). Т. 3. — М.: Изд-во центра прикладных исследований при мех-мат фак-те МГУ, 2001. — С. 334–337.
5. Федорова М. С. О неравенствах для параметров матриц специального вида // Тр. международной школы-семинара «Дискретная математика и математическая кибернетика», Ратмино, 31 мая–3 июня 2001 г. — М.: Изд-во МАКС Пресс, 2001. — С. 26.
6. Федорова М. С. Равномерно распределить двоичные наборы по шарам не всегда возможно // Тр. 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 фак-те МГУ, 2001. — С. 94–100.
7. Федорова М. С. О неравенствах для параметров комбинаторных матриц специального вида // Вестник МГУ. Вычислительная математика и кибернетика. — 2002. — № 2. — С. 45–49.

8. Ярыкина М. С. Об оценках для l -упаковок большого радиуса // Тр. V международной конф. «Дискретные модели в теории управляющих систем», Ратмино, 26 мая – 29 мая 2003 г. — М.: ВМиК МГУ, 2003. — С. 94-95.
9. Ashikhmin A., Barg A., Litsyn S. A new upper bound on codes decodable into size-2 lists // Numbers, Information and Complexity. — Boston: Kluwer publishers, 2000. — P. 239–244.
10. Blinovskiy V. Bounds for Multiple Packing in q -ary Hamming Space // Proceedings of ISIT 2002, Lausanne, Switzerland, June 30 – July 5, 2002. — P. 401.
11. Canetti R., Dodis Y., Halevi S., Kushilevitz E., Sahai A. Exposure-resilient functions and all-or-nothing transforms // In Advanced in Cryptology: Eurocrypt 2000, Proceedings, Lecture Notes in Computer Science. — V. 1807. — 2000. — P. 453–469.
12. Chor B., Goldreich O., Hastad J., Friedman J., Rudich S., Smolensky R. The bit extraction problem or t -resilient functions // IEEE Symp. on Foundations of Computer Science. — 1985. — V. 26. — P. 396–407.
13. Ding C., Xiao G., Shan W. The stability theory of stream ciphers // Lecture Notes in Computer Science. — V. 561. — Springer-Verlag. — 1991.
14. 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. V. 2247. — Springer-Verlag, 2001. — P. 254–266.
15. 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.
16. 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. — P. 104–107.
17. Pasalic E., Maitra S., Johansson T., Sarkar P. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity // WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001. — Electronic Notes in Discrete Mathematics. V. 6. — Elsevier Science, 2001.
18. Sarkar P., Maitra S. Nonlinearity bounds and constructions of resilient Boolean functions // In Advanced in Cryptology: Crypto 2000, Proceedings. — Lecture Notes in Computer Science. — 2000. — V. 1880. — P. 515–532.
19. Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Transactions on Information theory. — 1984. — V. IT-30, № 5. — P. 776–780.
20. Tarannikov Yu. On resilient Boolean functions with maximal possible nonlinearity // Proceedings of Indocrypt 2000. — Lecture Notes in Computer Science. — Springer-Verlag, 2000. — V. 1977. — P. 19–30.
21. 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. — Springer-Verlag, 2002. — V. 2355. — P. 66–77.
22. 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. — P. 264–274.

Поступило в редакцию 9 IX 2002