

УДК 519.722

НЕСУЩЕСТВОВАНИЕ ДВОИЧНЫХ КОДОВ, РАВНОМЕРНО РАСПРЕДЕЛЁННЫХ ПО ШАРАМ*)

М. С. Ярыкина

Рассматривается вопрос существования двоичных кодов размерности n , равномерно распределённых со степенью l по шарам. Доказывается, что такие коды не существуют для почти всех значений мощности кода m при достаточно больших n .

Введение

Двоичные коды, равномерно распределённые по подкубам n -мерного булева куба, изучаются в нескольких областях математики. Примерами таких кодов являются 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. По нашим сведениям равномерное распределение двоичных наборов по шарам не изучалось до работы [3], хотя представляется, что двоичные коды, наборы которых равномерно распределены по сферам, могут иметь некоторые полезные приложения. Например, такие коды можно использовать в качестве хеширующей функции, а также тогда, когда все слова на выходе канала связи имеют примерно одинаковую вероятность декодирования.

В [3] Ю. В. Таранников изучал коды, равномерно распределённые со степенью 1 по шарам, и привёл полное описание таких кодов, в том числе нашёл их количество при любом n .

В [4, 6] рассматривались коды, равномерно распределённые со степенью l по шарам, и было доказано несуществование таких кодов для некоторых диапазонов мощностей. В этих работах были рассмотрены коды малой мощности и поддиапазон для случая большой мощности.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 08-01-00863), программы «Ведущие научные школы» (проект НШ-4470.2008.1) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Синтез и сложность управляющих систем»).

В этой статье приводится полное доказательство несуществования кодов, равномерно распределённых со степенью l по шарам (при любом натуральном l); в [5] были опубликованы краткие тезисы.

Определения. Пусть V^n — множество двоичных наборов длины n (вершин булева куба размерности n). Кодом C (множеством двоичных наборов) назовём произвольное подмножество из V^n .

Мощностью кода C называется число двоичных наборов в нём (обозначается через $|C|$). В дальнейшем мощность кода C будем также обозначать через $m = m(C)$. *Подкодом* кода C называется такое подмножество двоичных наборов из C , у которых совпадают некоторые разряды (наборы, у которых в компонентах i_1, \dots, i_h находятся $\sigma_1, \dots, \sigma_h$ соответственно, где $\sigma_i \in \{0, 1\}$, $i = 1, \dots, h$). *Расстоянием (Хемминга) $d(x, y)$* между двумя наборами x и y называется число компонент, в которых эти наборы различаются. Множество $S_r(x) = \{y \in V^n \mid d(x, y) \leq r\}$ называется *шаром* радиуса r с центром $x \in V^n$. *Весом $w(S_r(x), C)$* шара $S_r(x)$ в коде C называется мощность множества $S_r(x) \cap C$.

Определение 1. Пусть l — натуральное число. Код $C \subseteq V^n$ называется *равномерно распределённым по шарам* со степенью l (l -РРШ кодом), если $\max_x \{w((S_r(x), C))\} - \min_x \{w((S_r(x), C))\} \leq l$ при каждом r , $0 \leq r \leq n$.

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

Полное описание кодов, равномерно распределённых по шарам со степенью 1 (1-РРШ кодов), было дано в [3].

Утверждение 1. Пусть $C \subseteq V^n$, $|C| \leq 2^{n-1}$. Если C — 1-РРШ код, то либо $|C| \leq 2$, либо $n \leq 4$, либо $n = 6$, $|C| = 4$.

Утверждение 2. Число различных 1-РРШ кодов в V^n равно

$$\left\{ \begin{array}{lll} 2^{2^n} & \text{при} & n \leq 2, \\ 80 & \text{при} & n = 3, \\ 334 & \text{при} & n = 4, \\ 2818 & \text{при} & n = 6, \\ 3 \cdot 2^n + 2 & \text{при} & n \geq 5, n \text{ нечётно}, \\ (n+3)2^n + 2 & \text{при} & n \geq 8, n \text{ чётно}. \end{array} \right.$$

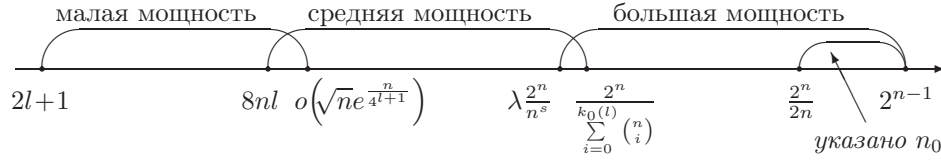
Как видно из приведённых выше утверждений, при $n \geq 7$ не существует кодов, равномерно распределённых по шарам со степенью 1 мощности $m \geq 3$.

В данной статье без ограничения общности мы рассматриваем только коды мощности $m \leq 2^{n-1}$ и доказываем следующее утверждение.

Теорема 1. Пусть l — фиксированное натуральное число, n — натуральное число и $2l + 1 \leq m \leq 2^{n-1}$. Тогда при каждом достаточно большом n в булевом кубе размерности n не существует l -РРШ кодов мощности m .

Для одного поддиапазона мощности кода удалось указать значение n_0 такое, что при любом $n > n_0$ не существует l -РРШ кодов.

Выделим три диапазона мощности кода: коды малой мощности, средней мощности и большой мощности.



Коды малой мощности — это коды, мощность m которых удовлетворяет условию $m \geq 2l + 1$, $m = o\left(\sqrt{n}e^{\frac{n}{4^{l+1}}}\right)$. Границей диапазона кодов малой мощности является некоторая последовательность $m = m(n)$, удовлетворяющая указанному выше условию (от выбора этой последовательности зависит, начиная с какого значения n размерности булева куба будут выполнены условия теоремы несуществования).

Коды средней мощности — это коды, мощность m которых лежит в диапазоне $8nl < m < 2^n / \left(\sum_{i=0}^{k_0(l)} \binom{n}{i}\right)$, где $k_0(l)$ — некоторое целое число, определяемое ниже.

Коды большой мощности — это коды, мощность m которых удовлетворяет неравенству $\lambda \cdot 2^n / n^s < m \leq 2^{n-1}$, где положительное число λ и $s > k_0(l)$ выбраны так, что диапазоны средней и большой мощности пересекаются.

В данной статье мы приводим полные доказательства во всех указанных случаях, включая ранее рассмотренные.

1. Коды малой мощности

Рассмотрим произвольную функцию $M(n) = o\left(\sqrt{n}e^{\frac{n}{4^{l+1}}}\right)$. Под кодами *малой мощности* будем понимать коды, мощность m которых удовлетворяет условию $2l + 1 \leq m \leq M(n) = o\left(\sqrt{n}e^{\frac{n}{4^{l+1}}}\right)$. Полное доказательство несуществования таких кодов было приведено в [4]. Кроме

того, в ней были рассмотрены случаи l , растущего вместе с m . Здесь для полноты изложения приводим доказательство теоремы для фиксированного l .

Теорема 2. Пусть l — фиксированное натуральное число и $m = m(n) \geq 2l + 1$. Тогда если $\frac{m}{\sqrt{n}e^{\frac{n}{4^{l+1}}}} \rightarrow 0$ или $m = o\left(\sqrt{n}e^{\frac{n}{4^{l+1}}}\right)$ при $n \rightarrow \infty$, то при каждом достаточно большом n в булевом кубе размерности n не существует l -РРШ кодов мощности m .

Для доказательства теоремы нам понадобится

Лемма 1 ([4]). Пусть $\alpha = \alpha(n) < \frac{1}{2}$. Тогда при $n \rightarrow \infty$

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

Формулировки подобных утверждений содержатся в качестве задач в [1].

Доказательство теоремы 2. Для того чтобы доказать несуществование РРШ-кодов, покажем, что при выполнении условий теоремы существует R такое, что имеются шары радиуса R веса 0 и веса не менее $l + 1$.

Пусть $R = R(n) = \alpha(n)n$, где $\alpha(n) < \frac{1}{2}$ при всех n . Легко видеть, что средний вес $P_R(C)$ шара радиуса R кода C равен $P_R(C) = \frac{1}{2^n} m \sum_{i=0}^R \binom{n}{i}$.

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

Подкод C' будем строить следующим образом. В коде C найдём $l + 1$ двоичных наборов (напомним, что $2l + 1 \leq m$), которые в совокупности совпадают в наибольшем числе компонент. Число совпадающих компонент обозначим через t . Оценим снизу число t .

Пусть матрица $A = A(C)$ размера $m \times n$ кода C ($m = |C|$, $C \subset V^n$) имеет вид $(v_1, v_2, \dots, v_m)^*$, $v_i \in C$, где $*$ — знак транспонирования.

В матрице A найдём число B подматриц размера $(l + 1) \times 1$, состоящих либо из одних нулей, либо из одних единиц (подматрицы получаем из матрицы A вычёркиванием любых $m - (l + 1)$ строк и $n - 1$ столбцов). Рассмотрим i -й столбец матрицы A . Без ограничения общности можно

считать, что в нём имеется не больше $m/2$ единиц. Пусть число единиц в этом столбце равно $m/2 - h$, а число нулей равно $m/2 + h$, где h неотрицательное число. Число способов выбора $l + 1$ строк из матрицы A с единицей в i -м столбце равно $\binom{m/2-h}{l+1}$, а с нулем — $\binom{m/2+h}{l+1}$. Следовательно, в i -м столбце имеется $b = \binom{m/2-h}{l+1} + \binom{m/2+h}{l+1}$ подматриц указанного вида. Это число минимально, если $h = 0$ (доказательство см. в [4]). Значит, 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. Так как в матрице A имеется n столбцов, то в ней имеется $B \geq 2n\binom{m/2}{l+1}$ подматриц указанного вида.

С другой стороны, число подматриц указанного вида в матрице A равно $B = \binom{m}{l+1} \cdot t'$, где $\binom{m}{l+1}$ — число способов выбора $l + 1$ строк, t' — среднее число (по всем выборкам из $l + 1$ строки) совпадающих компонент в $l + 1$ строках в совокупности.

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

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

Итак, имеется $l + 1$ наборов кода C , которые совпадают в t компонентах. Удалив совпадающие компоненты, получаем подкод C' , состоящий из $l + 1$ наборов длины $n - t$.

Средний вес $P_R(C')$ шара радиуса R кода C' равен

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

Если R , m и l таковы, что $P_R(C) \rightarrow 0$ и $P_R(C') \rightarrow l + 1$ при $n \rightarrow \infty$, то при достаточно больших n для шаров радиуса R не выполняется условие равномерного распределения кода по шарам.

Осталось доказать, что такое R существует, т. е. справедливы соотношения:

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

Так как $R = \alpha(n) \cdot n$, то $\frac{1}{2} \left(1 - \frac{t}{n}\right) < \alpha(n) < \frac{1}{2}$. 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 построим такой подкод C' кода C мощности $l + 1$, что C' попадает в один шар требуемого радиуса.

Оценим $\beta = 1 - 2\alpha(n)$:

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

При каждом фиксированном l и любом достаточно большом n выполняется неравенство $\beta > \frac{1}{2^{l+2}}$. Следовательно, по пункту 2 леммы и условию теоремы при $n \rightarrow \infty$ имеем

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

Значит, при любом достаточно большом n существует шар радиуса R веса 0. С другой стороны, при $n \rightarrow \infty$ имеем

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

Значит, при любом достаточно большом n существует шар радиуса R веса не менее $l + 1$. Теорема 2 доказана.

2. Коды средней мощности

В этом разделе мы рассмотрим двоичные коды, мощность которых изменяется от линейной по n до $2^n/n^s$. Мы докажем, что начиная с некоторого n не существует кодов, равномерно распределённых по шарам со степенью l , мощность которых лежит в указанном диапазоне.

Этот случай оказался самым сложным для доказательства. При доказательстве основной теоремы используются свойства кодов Ридда–Маллера, свойства для сумм биномиальных коэффициентов и свойства взаимного расположения шаров различного радиуса в булевом кубе.

2.1. Вспомогательные результаты

Лемма 2. Пусть C — некоторый код в булевом кубе такой, что любой шар радиуса k имеет вес не более l_0 . Кроме того, существует шар радиуса r ($r \leq k$) с центром γ_0 веса l_0 . Тогда шар радиуса $2k - r$ с центром γ_0 имеет вес l_0 .

ДОКАЗАТЕЛЬСТВО. Без ограничения общности можно считать, что центр шара радиуса r , в котором содержится ровно l_0 наборов кода, находится в точке $\{0 \dots 0\}$ — это шар $S_r(\bar{0})$.

Рассмотрим все шары радиуса k , содержащие шар $S_r(\bar{0})$. В каждом таком шаре нет кодовых наборов вне шара $S_r(\bar{0})$, так как любой шар радиуса меньшего или равного k содержит не более l_0 кодовых наборов.

Докажем, что в объединении указанных выше шаров имеется шар $S_{2k-r}(\bar{0})$ радиуса $2k - r$, в котором содержится ровно l_0 кодовых наборов.

С этой целью рассмотрим произвольный набор β , принадлежащий шару $S_{2k-r}(\bar{0})$ радиуса $2k - r$, и покажем, что он принадлежит какому-либо из указанных выше шаров радиуса k .

Если в наборе β содержится не более k единичных компонент, утверждение очевидно. Пусть теперь в наборе β содержится не более $2k - r$ и не менее k единичных компонент. Заменяем в наборе β произвольные k единичных компонент нулями. Получим набор γ , содержащий не более $k - r$ единичных компонент. Имеем $d(\gamma, \beta) = k$, $d(\gamma, \bar{0}) \leq k - r$. Пусть α — произвольный набор из шара $S_r(\bar{0})$. Тогда $d(\alpha, \bar{0}) \leq r$ и $d(\gamma, \alpha) \leq d(\gamma, \bar{0}) + d(\bar{0}, \alpha) \leq k - r + r = k$ для любого $\alpha \in S_r(\bar{0})$. Отсюда следует, что $S_k(\gamma) \supset S_r(\bar{0})$ и $\beta \in S_k(\gamma)$. Следовательно, шар $S_k(\gamma)$ искомый. Лемма 2 доказана.

Лемма 3. Пусть C — некоторый код в булевом кубе такой, что все шары радиуса k имеют вес не более l . Тогда существует шар радиуса $\left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor$, имеющий вес не более l .

ДОКАЗАТЕЛЬСТВО проведем индукцией по l .

База индукции: $l = 1$.

Докажем, что существует шар радиуса $2k$, имеющий вес не более единицы.

По условию любой шар радиуса k содержит не более одного набора из S . Отсюда следует, что кодовое расстояние больше $2k$ (так как два набора, находящиеся друг от друга на расстоянии $2k$, содержатся также в некотором шаре радиуса k).

Рассмотрим шар радиуса $2k$ с центром в кодовом слове. В этом шаре нет других кодовых наборов. Следовательно, этот шар является искомым.

Шаг индукции: $l - 1 \longrightarrow l$.

Пусть r — минимальный радиус шара, в котором содержится ровно l кодовых наборов. Рассмотрим два случая.

Случай 1. Пусть $r \leq \left\lfloor \frac{2^l - 2}{2^l - 1} k \right\rfloor$. По лемме 2 существует шар радиуса $2k - r$, в котором содержится не более l кодовых наборов. При $r \leq \left\lfloor \frac{2^l - 2}{2^l - 1} k \right\rfloor$ имеем $2k - r \geq 2k - \left\lfloor \frac{2^l - 2}{2^l - 1} k \right\rfloor = \left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor$. Значит, существует шар радиуса $\left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor$ и веса не более l .

Случай 2. Пусть $r > \left\lfloor \frac{2^l - 2}{2^l - 1} k \right\rfloor$. Тогда в любом шаре радиуса $\left\lfloor \frac{2^l - 2}{2^l - 1} k \right\rfloor$ содержится не более $l - 1$ кодовых наборов. Следовательно, по предположению индукции в случае $l_0 = l - 1$ существует шар радиуса

$$\left\lfloor \frac{2^{l-1}}{2^{l-1} - 1} \cdot \left\lfloor \frac{2^l - 2}{2^l - 1} k \right\rfloor \right\rfloor \geq \left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor,$$

в котором содержится не более $l - 1$ кодовых наборов (значит, не более l наборов).

Таким образом, при любом r существует шар радиуса $\left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor$, содержащий не более l кодовых наборов. Шаг индукции завершён. Лемма 3 доказана.

В дальнейшем, мы будем использовать следующее обозначение:

$$\widehat{k}_0 = \widehat{k}_0(l) = (2^l - 1) \left\lceil 2 \cdot 2^l + 2^l \log_2 l - 2 \right\rceil. \quad (1)$$

Лемма 4. Пусть l — фиксированное натуральное число. Тогда найдётся такое k_0 , где $k_0 \geq \widehat{k}_0$ (\widehat{k}_0 зависит только от l), что при любых $k > k_0$ и $n \geq 2 \frac{2^l}{2^l - 1} k + 2^l + 2$ выполнено неравенство

$$\sum_{i=0}^{\left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor} \binom{n}{i} > 2^l \sum_{i=0}^{k+1} \binom{n}{i}. \quad (2)$$

Замечание 1. Покажем, как при конкретном l найти k_0 , удовлетворяющее условиям леммы. Рассмотрим неравенство (2) при $k = \widehat{k}_0$. Найдём (например, с помощью компьютера) значение n , начиная с которого выполнено неравенство, и обозначим это значение через $n_1(\widehat{k}_0)$. Сравним $n_1(\widehat{k}_0)$ и $n_0(\widehat{k}_0) = 2 \frac{2^l}{2^l - 1} \widehat{k}_0 + 2^l + 2$.

Если $n_1(\widehat{k}_0) \leq n_0(\widehat{k}_0)$, то положим $k_0 = \widehat{k}_0$.

Если $n_1(\widehat{k}_0) > n_0(\widehat{k}_0)$, то вычислим k_0 из условия $n_1(\widehat{k}_0) \leq n_0(k_0)$. А именно, $n_1(\widehat{k}_0) \leq 2 \frac{2^l}{2^l - 1} k_0 + 2^l + 2$, или $k_0 \geq (n_1(\widehat{k}_0) - 2^l - 2) \frac{2^l - 1}{2 \cdot 2^l}$ (возьмём наименьшее целое k_0 , удовлетворяющее этому неравенству). Обоснование данного алгоритма вычисления k_0 изложено в доказательстве.

Например, в случае $l = 2$ имеем $\widehat{k}_0 = 30$ и $n_1(30) = 143$, $n_0(30) = (8/3) \cdot 30 + 6 = 86$. Поскольку $143 \geq 86$, находим k_0 из условия $143 \leq (8/3) \cdot k_0 + 6$, или $k_0 \geq 51 \frac{3}{8}$. Значит, можно взять $k_0 = 52$.

Замечание 2. В случае $l = 2$ результат можно улучшить, если в процессе доказательства воспользоваться более точной оценкой. Тогда $\widehat{k}_0 = 24$ и $n_1(24) = 118$, $n_0(24) = 70$. Поскольку $118 \geq 70$, находим k_0 из условия $118 \leq \frac{8}{3} \cdot k_0 + 6$. Значит, можно взять $k_0 = 42$.

ДОКАЗАТЕЛЬСТВО леммы 4. Пусть $k > k_0$. Представим k в виде $k = (2^l - 1)p + s$, где $s \in \{0, 1, \dots, 2^l - 2\}$. Тогда

$$\left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor = \left\lfloor \frac{2^l}{2^l - 1} ((2^l - 1)p + s) \right\rfloor = 2^l p + s.$$

Значит, неравенство (2) принимает вид

$$\sum_{i=0}^{2^l p + s} \binom{n}{i} > 2^l \sum_{i=0}^{(2^l - 1)p + s + 1} \binom{n}{i}. \quad (3)$$

Докажем неравенство (3) индукцией по параметру p (для каждого $s \in \{0, 1, \dots, 2^l - 2\}$).

1. *База индукции:* $p = p_0 = \widehat{k}_0 / (2^l - 1) = \lceil 2 \cdot 2^l + 2^l \log_2 l - 2 \rceil$.

В качестве базы индукции берем указанное выше p_0 в силу того, что шаг индукции мы можем сделать только для $p \geq p_0 = \lceil 2 \cdot 2^l + 2^l \log_2 l - 2 \rceil$.

Неравенство (3) выполняется при некотором фиксированном p (при всех n , больших некоторого $n_1(p)$), если p удовлетворяет условию: $2^l p + s > (2^l - 1)p + s + 1 \Leftrightarrow p > 1$. Если биномиальные коэффициенты представить в виде многочленов по степеням n , то степень $2^l p + s$ многочлена в левой части будет больше, чем степень $(2^l - 1)p + s + 1$ многочлена в правой части. Следовательно, начиная с некоторого $n_1 = n_1(p)$, неравенство (3) будет верным. База индукции доказана.

2. Шаг индукции $p \longrightarrow p+1$. Из левой части неравенства (3) вычтем правую. При $p+1$ имеем

$$\begin{aligned}
 A &= \sum_{i=0}^{2^l(p+1)+s} \binom{n}{i} - 2l \sum_{i=0}^{(2^l-1)(p+1)+s+1} \binom{n}{i} \\
 &> \text{(по предположению индукции)} \\
 &> \sum_{i=2^lp+s+1}^{2^l(p+1)+s} \binom{n}{i} - 2l \sum_{i=(2^l-1)p+s+2}^{(2^l-1)(p+1)+s+1} \binom{n}{i} \\
 &= \left[\binom{n}{2^lp+s+1} + \binom{n}{2^lp+s+2} + \cdots + \binom{n}{2^lp+s+2^l} \right] \\
 &- 2l \left[\binom{n}{(2^l-1)p+s+2} + \cdots + \binom{n}{(2^l-1)p+s+2^l} \right] \\
 &= A_1 - 2l \cdot A_2.
 \end{aligned}$$

Воспользуемся следующим свойством биномиальных коэффициентов: если $n \geq 2i+k$, то

$$\binom{n}{i+k} \geq \binom{n}{i}. \quad (4)$$

Оценим снизу сумму A_1 . Согласно неравенству (4) минимальным является первое слагаемое. Поэтому

$$\underbrace{\left(\binom{n}{2^lp+s+1} + \binom{n}{2^lp+s+2} + \cdots + \binom{n}{2^lp+s+2^l} \right)}_{2^l \text{ слагаемых}} > 2^l \cdot \binom{n}{2^lp+s+1},$$

если $n \geq (2^lp+s+1) + (2^lp+s+2^l) = 2 \cdot 2^lp + 2s + 2^l + 1$.

Оценим сверху сумму A_2 . Согласно неравенству (4) максимальным является последнее слагаемое. Поэтому

$$\underbrace{\left(\binom{n}{(2^l-1)p+s+2} + \cdots + \binom{n}{(2^l-1)p+s+2^l} \right)}_{2^l-1 \text{ слагаемых}} < (2^l-1) \binom{n}{(2^l-1)p+s+2^l} < 2^l \binom{n}{(2^l-1)p+s+2^l},$$

если $n \geq 2((2^l - 1)p + s + 2^l) = 2 \cdot 2^l p + 2s + 2 \cdot 2^l - 2p$. Так как $p > 2^l$, то $2 \cdot 2^l - 2p < 2^l + 1$. Поэтому верхняя оценка для суммы A_2 верна при $n \geq 2 \cdot 2^l p + 2s + 2^l + 1$.

В результате имеем

$$A = A_1 - 2l \cdot A_2 > 2^l \cdot \binom{n}{2^l p + s + 1} - 2l \cdot 2^l \cdot \binom{n}{(2^l - 1)p + s + 2^l}.$$

Теперь достаточно доказать, что $A \geq 0$.

Выразим биномиальные коэффициенты через факториалы:

$$\begin{aligned} & \frac{n!}{(2^l p + s + 1)!(n - 2^l p - s - 1)!} \\ & > 2l \frac{n!}{((2^l - 1)p + s + 2^l)!(n - (2^l - 1)p - s - 2^l)!}, \\ & \underbrace{\frac{(n - (2^l - 1)p - s - 2^l)}{(2^l p + s + 1)} \cdot \dots \cdot \frac{(n - 2^l p - s)}{((2^l - 1)p + s + 2^l + 1)}}_{p-2^l+1 \text{ сомножителей}} > 2l. \end{aligned}$$

Воспользовавшись неравенством

$$\frac{a+1}{b+1} < \frac{a}{b}, \text{ если } a > b,$$

получаем неравенства

$$\begin{aligned} \frac{(n - (2^l - 1)p - s - 2^l)}{(2^l p + s + 1)} & < \frac{(n - (2^l - 1)p - s - 2^l - 1)}{(2^l p + s)} < \dots \\ & < \frac{(n - 2^l p - s)}{((2^l - 1)p + s + 2^l + 1)}, \end{aligned}$$

если $n - 2^l p - s > (2^l - 1)p + s + 2^l + 1$, или $n > 2 \cdot 2^l p - p + 2s + 2^l + 1$ (верно по условию леммы).

Отсюда следует, что

$$\begin{aligned} & \underbrace{\frac{(n - (2^l - 1)p - s - 2^l)}{(2^l p + s + 1)} \cdot \dots \cdot \frac{(n - 2^l p - s)}{((2^l - 1)p + s + 2^l + 1)}}_{p-2^l+1 \text{ сомножителей}} \\ & > \left(\frac{(n - (2^l - 1)p - s - 2^l)}{(2^l p + s + 1)} \right)^{p-2^l+1}. \end{aligned}$$

Следовательно, достаточно, чтобы выполнялось неравенство

$$\frac{(n - (2^l - 1)p - s - 2^l)}{(2^l p + s + 1)} > (2l)^{1/(p-2^l+1)}. \quad (5)$$

Убедимся в том, что при $p \geq 2 \cdot 2^l + 2^l \log_2 l - 1$ выполняется неравенство

$$(2l)^{1/(p-2^l+1)} \leq 1 + \frac{1}{2^l}, \quad \text{т. е.} \quad \left(1 + \frac{1}{2^l}\right)^{p-2^l+1} \geq 2l. \quad (6)$$

Последовательность $(1 + \frac{1}{n})^n$ неубывающая и $(1 + \frac{1}{2})^2 > 2$. Поэтому $(1 + \frac{1}{2^l})^{2^l} > 2$. Следовательно, учитывая указанное выше условие для p , имеем $p - 2^l + 1 \geq 2^l(1 + \log_2 l)$ и

$$\left(1 + \frac{1}{2^l}\right)^{p-2^l+1} \geq \left(1 + \frac{1}{2^l}\right)^{2^l(1+\log_2 l)} > 2^{(1+\log_2 l)} = 2l.$$

Таким образом, осталось проверить, что

$$\frac{(n - (2^l - 1)p - s - 2^l)}{(2^l p + s + 1)} > 1 + \frac{1}{2^l}.$$

Действительно, приведём обе части неравенства к общему знаменателю и перенесём слагаемые, не содержащие n , в правую часть. В результате получим $n > (2^l - 1)p + s + 2^l + (2^l p + s + 1) + \frac{1}{2^l}(2^l p + s + 1)$, т. е. $n > 2 \cdot 2^l p + 2s + 2^l + 2$. Шаг индукции доказан.

3. Следовательно, база индукции по p выполнена при $n \geq n_1(p)$, а шаг индукции верен при $n \geq n_0(p)$.

Если $n_1(p_0) \leq n_0(p_0)$, то положив $n_1(p_0) = n_0(p_0)$, получим требуемое.

Если $n_1(p_0) \geq n_0(p_0)$, то сделаем t шагов индукции до тех пор, пока не выполнится неравенство $n_1(p_0) \leq n_0(p_0 + t)$. Тогда утверждение леммы будет выполнено, начиная с $p = p_0 + t$. Лемма 4 доказана.

Лемма 5. При достаточно больших n булев куб размерности n можно покрыть $4n$ шарами радиуса $R = \frac{n}{2} - 2^l - 1$.

ДОКАЗАТЕЛЬСТВО. Сначала докажем лемму в случае $n = 2^t$.

При таких n существует код Рида–Маллера первого порядка; он соответствует всем линейным функциям. Мощность такого кода равна $2n$. Согласно свойствам кода Рида–Маллера (см. [2, гл. 14]) расстояние от любой вершины булева куба до кода Рида–Маллера не превосходит $\frac{n}{2} -$

$\frac{\sqrt{n}}{2}$. Рассмотрим множество шаров радиуса R с центрами в кодовых словах кода Рида–Маллера. Тогда при $R \geq \frac{n}{2} - \frac{\sqrt{n}}{2}$ это множество шаров является покрытием всего булева куба. Легко проверить, что при $n \geq 2^{2l+2} + 4 \cdot 2^{l+1} + 4$ выполнено неравенство $R = \frac{n}{2} - 2^l - 1 \geq \frac{n}{2} - \frac{\sqrt{n}}{2}$. В случае $n = 2^t$ лемма 5 доказана.

Докажем лемму при произвольном n . Пусть $n_1 = 2^t < n < n_2 = 2^{t+1}$.

При n_1 существует код Рида–Маллера C_1 мощности $2n_1$. Сопоставим коду C_1 матрицу A' , в которой каждая строка является кодовым набором. Таким образом, матрица A' имеет $2n_1$ строк и n_1 столбцов.

При n_2 существует код Рида–Маллера C_2 мощности $2n_2$. Сопоставим коду C_2 матрицу A'' , которая имеет вид

$$A'' = \begin{pmatrix} A' & A' \\ A' & \bar{A}' \end{pmatrix},$$

где \bar{A}' — матрица, полученная из матрицы A' заменой нулей на единицы, а единиц на нули.

Рассмотрим код C_n , соответствующий матрице A_n , которая состоит из первых n столбцов матрицы A'' . Докажем, что множество шаров радиуса $R(n)$ с центрами в наборах из C_n является покрытием вершин булева куба.

Для любого набора $\alpha = (\alpha_1 \alpha_2)$, где α_1 — набор длины n_1 , α_2 — набор длины $n - n_1$, существует такой кодовый набор $\gamma \in C_n$, что

$$d(\alpha, \gamma) \leq \frac{n}{2} - \frac{\sqrt{n_1}}{2}.$$

Сначала найдём кодовый набор $\gamma_1 \in C_1$ такой, что $d(\alpha_1, \gamma_1) \leq \frac{n_1}{2} - \frac{\sqrt{n_1}}{2}$. Набор γ_1 существует в силу свойств кода Рида–Маллера первого порядка. Заметим, что в матрице A_n есть две строки с началом γ_1 — это строки $(\gamma_1 \gamma_n)$ и $(\gamma_1 \bar{\gamma}_n)$, где γ_n имеет длину $n - n_1$, $\bar{\gamma}_n$ — набор, полученный из набора γ_n заменой нулей на единицы, а единиц на нули. Поэтому одно из расстояний $d(\alpha_2, \gamma_n)$ и $d(\alpha_2, \bar{\gamma}_n)$ не превосходит $(n - n_1)/2$. Выберем кодовый набор, для которого расстояние до α_2 минимально. Этот набор искомый:

$$\begin{aligned} d(\alpha, \gamma) &= d(\alpha_1, \gamma_1) + \min\{d(\alpha_2, \gamma_n), d(\alpha_2, \bar{\gamma}_n)\} \leq \frac{n_1}{2} - \frac{\sqrt{n_1}}{2} + \frac{n - n_1}{2} \\ &\leq \frac{n}{2} - \frac{\sqrt{n_1}}{2} \leq \frac{n}{2} - 2^l - 1. \end{aligned}$$

Таким образом, множество шаров радиуса R_n с центрами в наборах кода C_n действительно является покрытием вершин булева куба. Мощность кода C_n равна $2n_2$. Следовательно, $2n_2 = 4n_1 < 4n$. Лемма 5 доказана.

2.2. Основная теорема

Теорема 3. Пусть l — фиксированное натуральное число и $k_0(l)$ — некоторое натуральное число (его существование доказано в лемме 4). Тогда в булевом кубе достаточно большой размерности n не существует кодов, равномерно распределённых по шарам со степенью l и мощности m , удовлетворяющей условию: $8nl < m < 2^n / (\sum_{i=0}^{k_0(l)} \binom{n}{i})$.

ДОКАЗАТЕЛЬСТВО. Докажем от противного. Предположим, что l -РРШ код с такой мощностью m существует. Так как $m < 2^n / \sum_{i=0}^{k_0} \binom{n}{i}$, то имеется шар радиуса $k = k_0$ веса 0. Докажем по индукции, что если имеется шар радиуса k нулевого веса, то имеется шар радиуса $k + 1$ нулевого веса.

База индукции. $k = k_0$.

Индуктивный переход. Пусть имеется шар радиуса k веса 0. Тогда по лемме 3 имеется шар радиуса $R \geq \left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor$ веса не более l . В силу того, что код является РРШ кодом со степенью l , то любой шар радиуса R имеет вес не более $2l$. Рассмотрим 2 случая.

Если $n < 2 \cdot \frac{2^l}{2^l - 1} k + 2^l + 2$, то по лемме 5 все вершины булева куба покрываем $4n$ шарами радиуса R . Вес одного шара не более l , а остальных не более $2l$. Следовательно, мощность кода не превосходит $l + 2l(4n - 1)$, что противоречит условию теоремы.

Если $n \geq 2 \cdot \frac{2^l}{2^l - 1} k + 2^l + 2$, то в силу леммы 4 имеем

$$P_{k+1}(C) < P_{\left\lfloor \frac{2^l}{2^l - 1} k \right\rfloor}(C) \leq \frac{1}{2l} P_R(C) < \frac{1}{2l} \cdot 2l = 1.$$

Значит, существует шар радиуса $k + 1$ веса 0. Шаг индукции доказан.

Так как n фиксировано, а на каждом шаге индукции k увеличивается на единицу, то на некотором шаге индукции выполнится условие $n < 2 \cdot \frac{2^l}{2^l - 1} k + 2^l + 2$, т. е. мы придём к противоречию (смотри первый случай шага индукции). Теорема 3 доказана.

3. Коды большой мощности

В этом разделе мы рассмотрим l -РРШ коды, имеющие мощность m в следующем диапазоне: $\lambda \frac{2^n}{n^s} \leq m \leq 2^{n-1}$, где s — произвольное натуральное число, λ — некоторое положительное число.

В случае кодов большой мощности выделим два семейства мощностей. Для каждого семейства мощностей используется свой способ доказательства.

Первое семейство ($u > 1$ — некоторое фиксированное число, s — натуральное число):

$$\left\{ \frac{ul^2}{4} \cdot \frac{2^n}{n+1} \leq m(n) \leq 2^{n-1}, \frac{ul^2}{4} \cdot \frac{2^n}{\sum_{i=0}^2 \binom{n}{i}} \leq m(n) \leq \left(\frac{n}{4} + c_2\right) \frac{2^n}{\sum_{i=0}^2 \binom{n}{i}}, \right. \\ \left. \dots, \frac{ul^2}{4} \cdot \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \leq m(n) \leq \left(\frac{n}{s^2} + c_s\right) \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \right\};$$

второе семейство, состоящее из всех «больших» значений m , не попавших в первое семейство:

$$\left\{ \left(\frac{n}{4} + c_2\right) \frac{2^n}{\sum_{i=0}^2 \binom{n}{i}} \leq m(n) \leq \frac{ul^2}{4} \cdot \frac{2^n}{n+1}, \right. \\ \left(\frac{n}{9} + c_3\right) \frac{2^n}{\sum_{i=0}^3 \binom{n}{i}} \leq m(n) \leq \frac{ul^2}{4} \cdot \frac{2^n}{\sum_{i=0}^2 \binom{n}{i}}, \\ \dots, \left(\frac{n}{(s+1)^2} + c_{s+1}\right) \frac{2^n}{\sum_{i=0}^{s+1} \binom{n}{i}} \leq m(n) \leq \frac{ul^2}{4} \cdot \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \right\}.$$

Нечисленность кодов мощностей из первого семейства утверждает теорема 4, а из второго семейства — теорема 5.

3.1. Первое семейство

Лемма 6. Пусть p, q — натуральные числа, причём $p \leq q$. Тогда

$$\binom{p}{2} + \binom{q}{2} \leq \binom{p-1}{2} + \binom{q+1}{2}.$$

Лемма 7. Пусть s — фиксированное натуральное число. Тогда при любом $n > 2s$

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

ДОКАЗАТЕЛЬСТВО. Разложим биномиальные коэффициенты по формуле

$$\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!} = \frac{1}{i!}n^i + \frac{1}{i!} \cdot \frac{i(i-1)}{2} \cdot n^{i-1} + O(n^{i-2})$$

и представим сумму биномиальных коэффициентов в виде многочлена по n

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

Лемма 7 доказана.

Лемма 8. Пусть s — целое число и $n \geq 2s$.

Тогда пары кодовых наборов, находящихся на расстоянии $2s$ и $2s-1$ друг от друга, попадают в $\binom{2s}{s}$ шаров радиуса s .

Пары кодовых наборов, находящихся на расстоянии $2s-2$ и $2s-3$ друг от друга, попадают в $\binom{2s-2}{s-1} \cdot n$ шаров радиуса s .

Пары кодовых наборов, находящихся на расстоянии $2s-2t$ и $2s-(2t+1)$ друг от друга, попадают в $\binom{2s-2t}{s-t}n^t + O(n^{t-1}) = O(n^t)$ шаров радиуса s ($t \geq 2$).

ДОКАЗАТЕЛЬСТВО. Обозначим через p_k число шаров радиуса s , в каждом из которых одновременно содержится пара двоичных наборов, находящихся друг от друга на расстоянии k .

Для удобства записи доказательства рассмотрим наборы

$$\alpha = (0, 0, \dots, 0), \quad \beta_k = (\underbrace{1, \dots, 1}_{k \text{ единиц}}, 0, \dots, 0).$$

Найдём все центры γ шаров радиуса s , содержащих одновременно наборы α и β_k .

Сначала рассмотрим случай α и $\beta = \beta_{2s}$. Тогда $d(\alpha, \beta) = 2s$. Следовательно, любой искомый центр γ шара радиуса s должен удовлетворять

условию $d(\alpha, \gamma) = d(\beta, \gamma) = s$. Значит, в наборе γ содержится ровно s единиц, причём единичные компоненты в нём только те, которые в наборе β тоже единичные. Среди $2s$ единичных компонент набора β выберем s компонент, которые останутся единичными, а другие s компонент будут нулями. Таким образом, существует $\binom{2s}{s}$ возможных центров γ .

Теперь пусть α и $\beta = \beta_{2s-1}$. Любой искомый центр γ шара радиуса s должен удовлетворять условиям $d(\alpha, \gamma) \leq s$ и $d(\beta, \gamma) \leq s$. В этом случае набор γ содержит либо ровно $s - 1$ единицу, либо ровно s единиц, причём единичные компоненты в нём только те, которые в наборе β тоже единичные. Среди $2s$ единичных компонент набора β мы выберем либо s компонент, которые останутся единичными, либо $s - 1$ компонент, которые останутся единичными, другие $s - 1$ или s компонент будут нулями. Таким образом, имеется $\binom{2s-1}{s} + \binom{2s-1}{s-1} = \binom{2s}{s}$ возможных центров γ .

Теперь рассмотрим случай α и $\beta = \beta_{2s-2}$. В этом случае набор γ содержит либо $s - 2$ единицы (центр типа γ_1), либо $s - 1$ (центр типа γ_2), либо s единиц (центр типа γ_3):

$$\alpha = (0, 0, \dots, 0), \quad \beta = (\underbrace{1, \dots, 1}_{2s-2 \text{ единиц}}, 0, \dots, 0).$$

Центр γ_1 можно выбрать $\binom{2s-2}{s-2}$ способами, центр типа γ_2 можно выбрать $\binom{2s-2}{s-1} \cdot (n - (2s - 2) + 1)$ способами, центр типа γ_3 можно выбрать $\binom{2s-2}{s-1}$ способами. Таким образом, имеется

$$\begin{aligned} & \binom{2s-2}{s-2} + \binom{2s-2}{s-1} \cdot (n - (2s - 2)) + \binom{2s-2}{s-1} + \binom{2s-2}{s} \\ &= \binom{2s-2}{s-1} \cdot (n - 2s + 3) + 2 \binom{2s-2}{s-2} \end{aligned}$$

центров γ .

Легко показать, что при $n \geq 2s$ выполняется неравенство $p_{2k-2} \geq p_{2k}$.

Теперь рассмотрим случай α и $\beta = \beta_{2s-2k}$. Без ограничения общности можно рассмотреть следующие наборы:

$$\alpha = (0, 0, \dots, 0), \quad \beta = (\underbrace{1, \dots, 1}_{2s-2k \text{ единиц}}, 0, \dots, 0).$$

Пусть в координатной записи центра γ содержится $s - k$ единиц среди первых $2s - 2k$ компонент и t единиц среди остальных $n - 2s + 2k$ компонент. Поскольку должны выполняться неравенства $d(\alpha, \gamma) \leq s$

и $d(\beta, \gamma) \leq s$, то $t \leq k$. Таким образом, центр шара γ указанного выше вида можно выбрать $\binom{2s-2k}{s-k} \cdot ((n-2(s-k))^k + O(n^{k-1}))$ способами.

В остальных случаях, когда среди первых $2s-2k$ компонент центра γ число единиц не равно $s-k$ (больше или меньше), общее число таких центров не превосходит $O(n^{k-1})$. Лемма 8 доказана.

Теорема 4. Пусть l — фиксированное натуральное число, а числа $s \in \mathbb{N}$, $u > 1$, c_s — некоторая константа (зависящая от s) и m удовлетворяют соотношениям:

$$\frac{ul^2}{4} \cdot \frac{2^n}{n+1} \leq m \leq 2^{n-1} \text{ при } s = 1 \text{ и}$$

$$\frac{ul^2}{4} \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \leq m \leq \left(\frac{n}{s^2} + c_s \right) \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \text{ при } s > 1.$$

Тогда при любом достаточно большом 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 условиям:

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

Замечание 3. Отметим, что случай $s = 1$ покрывает почти все двоичные коды. Кроме того, к нему относятся все уравновешенные коды.

Замечание 4. Для каждого s и соответствующего ему диапазона мощностей можно утверждать о неравномерном распределении по шарам со степенью l уже для шаров, радиус которых не превосходит $2s$.

ДОКАЗАТЕЛЬСТВО теоремы 4. Идея доказательства состоит в следующем. Предположим, что C является l -РРШ кодом. Оценим число пар двоичных наборов из кода C , находящихся друг от друга на расстоянии не более $2s$, двумя способами. Первым способом мы получим нижнюю оценку, вторым — верхнюю. Затем мы покажем, что в условиях теоремы нижняя оценка больше верхней, т. е. придём к противоречию.

Рассмотрим код C размерности n и мощности m . Пусть P_s — средний вес шара радиуса s . Тогда

$$|C| = m = P_s \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \leq 2^{n-1}.$$

Число пар двоичных наборов кода C , находящихся друг от друга на расстоянии не более $2s$, обозначим через N . Оценим N снизу. Для каждого

набора α из C рассмотрим шар $S_{2s}(\alpha)$ радиуса $2s$ с центром α . Все наборы, находящиеся от набора α на расстоянии не более $2s$, попадут в шар $S_{2s}(\alpha)$. Вес этого шара не меньше $\lceil P_{2s} \rceil - l$, так как C является l -РРШ кодом. Значит, число искомых пар двоичных наборов, содержащих набор α , не меньше $\lceil P_{2s} \rceil - l$. Аналогичным образом рассмотрим все остальные наборы кода. Таким образом, каждая пара наборов (α_1, α_2) будет посчитана дважды: как пара, содержащая набор α_1 , и как пара, содержащая набор α_2 . Так как общее число наборов в коде C равно m , а число пар, содержащих каждый набор, не меньше $\lceil P_{2s} \rceil - l$, то общее удвоенное число пар удовлетворяет неравенству

$$2N \geq m \cdot (\lceil P_{2s} \rceil - l) \geq m \left(\frac{m}{2^n} \cdot \sum_{i=0}^{2s} \binom{n}{i} - l \right). \quad (7)$$

Оценим N сверху. Минимальный вес шара радиуса s обозначим через h . Тогда максимальный вес шара радиуса s не превышает $h + l$. Число шаров радиуса s и веса $h + i$ обозначим через t_i , $i = 0, \dots, l$. Тогда

$$\sum_{i=0}^l t_i = 2^n \quad (8)$$

— число всех шаров радиуса s в булевом кубе размерности n ,

$$\sum_{i=0}^l t_i (h + i) = m \cdot \sum_{i=0}^s \binom{n}{i} \quad (9)$$

— сумма весов всех шаров радиуса s в булевом кубе размерности n .

Каждая пара наборов, находящихся друг от друга на расстоянии $2s$, содержится в $\binom{2s}{s}$ шарах радиуса s . Каждая пара наборов, находящихся друг от друга на расстоянии меньше $2s$, содержится не менее чем в $\binom{2s}{s}$ шарах радиуса s . Кроме того, просуммируем число пар наборов в каждом из 2^n шаров радиуса s булева куба размерности n . В каждом шаре радиуса s веса $h + i$ содержится $\binom{h+i}{2}$ пар наборов, находящихся друг от друга на расстоянии не более $2s$, а число шаров радиуса s веса $h + i$ равно t_i . Поэтому

$$\binom{2s}{s} N \leq \sum_{i=0}^l t_i \binom{h+i}{2}. \quad (10)$$

В силу леммы 6 при любых i и j таких, что $0 < i \leq j < l$, выполняется неравенство

$$\binom{h+i}{2} + \binom{h+j}{2} \leq \binom{h+i-1}{2} + \binom{h+j+1}{2}. \quad (11)$$

Преобразуем правую часть выражения (10) с помощью неравенства (11). Будем применять неравенство (11) к различным парам слагаемых, пока не получим два крайних слагаемых

$$\sum_{i=0}^l t_i \binom{h+i}{2} \leq t'_0 \binom{h}{2} + t'_l \binom{h+l}{2} = (t'_0 + t'_l) \frac{h(h-1)}{2} + t'_l \frac{2hl + l^2 - l}{2}.$$

При преобразованиях с помощью (11) суммы $\sum_{i=0}^l t_i$ и $\sum_{i=0}^l t_i(h+i)$ не изменяются. Поэтому ввиду равенств (8) и (9) величины t'_0 и t'_l удовлетворяют системе:

$$\begin{aligned} t'_0 + t'_l &= 2^n, \\ t'_0 h + t'_l (h+l) &= m \sum_{i=0}^s \binom{n}{i}. \end{aligned}$$

Отсюда следует, что $t'_l \cdot l = m \sum_{i=0}^s \binom{n}{i} - 2^n h$. Следовательно, оценка (10) примет вид

$$\binom{2s}{s} N \leq 2^n \cdot \frac{h(h-1)}{2} + \left(m \sum_{i=0}^s \binom{n}{i} - 2^n h \right) \frac{2h+l-1}{2}. \quad (12)$$

Используя полученные для N нижнюю и верхнюю оценки (7) и (12), имеем

$$\begin{aligned} \binom{2s}{s} m \left(\frac{m}{2^n} \cdot \sum_{i=0}^{2s} \binom{n}{i} - l - 1 \right) &\leq \\ &\leq 2 \left(2^n \frac{h(h-1)}{2} + \left(m \sum_{i=0}^s \binom{n}{i} - 2^n h \right) \frac{2h+l-1}{2} \right). \quad (13) \end{aligned}$$

Так как мощность кода m представлена в виде

$$m = P_s \frac{2^n}{\sum_{i=0}^s \binom{n}{i}},$$

то, подставив это значение m в неравенство (13), получаем

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

Разделив обе части полученного неравенства на 2^n и умножив на $\sum_{i=0}^s \binom{n}{i}$, имеем

$$\begin{aligned} \binom{2s}{s} \cdot P_s^2 \cdot \frac{\sum_{i=0}^{2s} \binom{n}{i}}{\sum_{i=0}^s \binom{n}{i}} - \binom{2s}{s} \cdot P_s \cdot (l+1) \\ \leq \sum_{i=0}^s \binom{n}{i} \cdot \left(h(h-1) + (P_s - h)(2h+l-1) \right). \quad (14) \end{aligned}$$

Теперь выразим суммы биномиальных коэффициентов через степени n . В силу леммы 7 при достаточно больших $n > 4s$ имеем

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

Таким образом, из двух последних равенств получаем

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

Преобразуем неравенство (14), заменив суммы биномиальных коэффициентов на соответствующие многочлены по степеням n :

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

Разделив обе части полученного неравенства на $\frac{n^{s-1}}{s!}$, получаем

$$\begin{aligned} & \left(n + \frac{3s - 3s^2}{2} + O\left(\frac{1}{n}\right) \right) P_s^2 - \frac{(2s)!}{s!} \cdot \frac{P_s}{n^{s-1}} \cdot (l+1) \\ & \leq \left(n + \frac{3s - s^2}{2} + O\left(\frac{1}{n}\right) \right) \left(h(h-1) + (P_s - h)(2h + l - 1) \right). \end{aligned} \quad (15)$$

Дальнейшее доказательство проведём отдельно для случая $s > 1$ и для случая $s = 1$.

Если $s > 1$, то из условия теоремы следует, что $\frac{P_s}{n^{s-1}} \leq \frac{P_s}{n} \cdot P_s = P_s^2 \cdot O\left(\frac{1}{n}\right)$. Поэтому слагаемым $\frac{(2s)!}{s!} \cdot \frac{P_s}{n^{s-1}} \cdot (l+1)$ можно пренебречь.

Перегруппируем слагаемые в неравенстве (15) таким образом, чтобы можно было получить нужную оценку. В левой части неравенства представим P_s^2 как $(P_s - h)(P_s - h - l) + (2P_s h + P_s l - h^2 - hl)$, а в правой части раскроем скобки во втором множителе:

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

Перенеся все слагаемые в левую часть и приведя подобные члены, получаем

$$\begin{aligned} Z = & \underbrace{\left(n + \frac{3s - 3s^2}{2} + O\left(\frac{1}{n}\right) \right) (P_s - h)(P_s - h - l)}_{=Z_1} \\ & + \underbrace{\left(n + \frac{3s - s^2}{2} + O\left(\frac{1}{n}\right) \right) P_s}_{=Z_2} \\ & - \underbrace{\left(s^2 + O\left(\frac{1}{n}\right) \right) (2P_s h + P_s l - h^2 - hl)}_{=Z_3} \leq 0. \end{aligned} \quad (16)$$

Для того чтобы доказать несуществование l -РРШ кодов, покажем, что в условиях теоремы левая часть неравенства (16) (при достаточно больших n) больше нуля, т. е. в наших обозначениях $Z = Z_1 + Z_2 - Z_3 > 0$.

Так как $P_s^2 - 2P_s h + h^2 + hl \geq 0$, то $P_s^2 \geq 2P_s h - h^2 - hl$ и

$$Z_3 = \left(s^2 + O\left(\frac{1}{n}\right) \right) (2P_s h + P_s l - h^2 - hl) \leq \left(s^2 + O\left(\frac{1}{n}\right) \right) (P_s^2 + P_s l).$$

Поэтому

$$\begin{aligned} Z_2 - Z_3 &\geq \left(n + \frac{3s - s^2}{2} + O\left(\frac{1}{n}\right) \right) P_s - \left(s^2 + O\left(\frac{1}{n}\right) \right) (P_s^2 + P_s l) \\ &= P_s \left(n + \frac{3s - s^2}{2} + O\left(\frac{1}{n}\right) - s^2 l - \left(s^2 + O\left(\frac{1}{n}\right) \right) P_s \right). \end{aligned}$$

Подставив вместо Z_1 , Z_2 и Z_3 полученные оценки, получим

$$\begin{aligned} Z = Z_1 + Z_2 - Z_3 &\geq \left(n + \frac{3s - 3s^2}{2} + O\left(\frac{1}{n}\right) \right) (P_s - h)(P_s - h - l) \\ &\quad + P_s \left(n + \frac{3s - s^2}{2} + O\left(\frac{1}{n}\right) - s^2 l - \left(s^2 + O\left(\frac{1}{n}\right) \right) P_s \right). \end{aligned} \quad (17)$$

Каждое слагаемое является квадратичной функцией относительно P_s . Во-первых, из свойств квадратичной функции следует, что для любого P_s выполнено неравенство

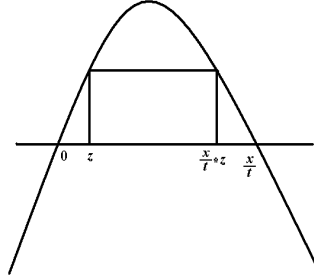
$$(P_s - h)(P_s - h - l) \geq -\frac{l^2}{4}. \quad (18)$$

Во-вторых, запишем второе слагаемое в виде

$$f(P_s) = P_s(X - tP_s), \quad (19)$$

где $X = n + \frac{3s - s^2}{2} + O\left(\frac{1}{n}\right) - s^2 l$, $t = s^2 + O\left(\frac{1}{n}\right)$.

Выражение (19) равно нулю при $P_s = 0$ и $P_s = X/t$, его график имеет вид параболы (см. граф



При этом для P_s из интервала $z \leq P_s \leq \frac{X}{t} - z$ выполнено неравенство

$$P_s(X - tP_s) \geq z(X - tz). \quad (20)$$

Положим $z = \frac{ul^2}{4}$. Тогда ограничения на P_s примут вид

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

или $\frac{ul^2}{4} \leq P_s \leq \frac{n}{s^2} + C_s$, где C_s — зависящая от s константа.

Применив неравенства (18) и (20) к выражению (17), получаем

$$\begin{aligned} Z &\geq -\frac{l^2}{4} \left(n + \frac{3s-3s^2}{2} + O\left(\frac{1}{n}\right) \right) \\ &\quad + \frac{ul^2}{4} \left(n + \frac{3s-s^2}{2} + O\left(\frac{1}{n}\right) - s^2l - \left(s^2 + O\left(\frac{1}{n}\right) \right) \frac{ul^2}{4} \right) \\ &= \frac{(u-1)l^2}{4}n + O(1). \end{aligned}$$

При $u > 1$ и достаточно больших n выражение $\frac{(u-1)l^2}{4}n + O(1)$ положительно.

Таким образом, мы получили, что с одной стороны справедливо неравенство $Z \leq 0$ (16), а с другой стороны $Z > 0$. Противоречие. При $s > 1$ теорема доказана.

Случай $s = 1$. В данном случае выражение (14) принимает вид:

$$\begin{aligned} 2 \cdot P_1^2 \cdot \frac{\sum_{i=0}^2 \binom{n}{i}}{\sum_{i=0}^1 \binom{n}{i}} - 2 \cdot P_1 \cdot (l+1) \\ \leq \sum_{i=0}^1 \binom{n}{i} \cdot \left(h(h-1) + (P_1 - h)(2h + l - 1) \right), \quad (21) \end{aligned}$$

а соответствующие суммы биномиальных коэффициентов равны соответственно

$$\sum_{i=0}^1 \binom{n}{i} = n + 1, \quad \sum_{i=0}^2 \binom{n}{i} = \frac{n^2 + n + 2}{2}, \quad 2 \cdot \frac{\sum_{i=0}^2 \binom{n}{i}}{\sum_{i=0}^1 \binom{n}{i}} = n + \frac{2}{n+1}.$$

Подставив эти выражения в (21), получим

$$P_1^2 \left(n + \frac{2}{n+1} \right) - 2 \cdot P_1 \cdot (l+1) \leq (n+1) \cdot \left(h(h-1) + (P_1-h)(2h+l-1) \right).$$

Действуя также, как и в общем случае, получаем

$$n(P_1-h)(P_1-h-l) + (n+1)P_1 + \frac{2}{n+1}P_1 - 2 \cdot P_1 \cdot (l+1) - (P_1^2 + P_1l) \leq 0,$$

$$n(P_1-h)(P_1-h-l) + P_1(n-3l-1-P_1) + \frac{2}{n+1}P_1 \leq 0.$$

Так как $\frac{2}{n+1}P_1 > 0$, то

$$n(P_1-h)(P_1-h-l) + P_1(n-3l-1-P_1) < 0. \quad (22)$$

Аналогично общему случаю из свойств квадратичной (относительно P_1) функции следует, что $(P_1-h)(P_1-h-l) \geq -\frac{l^2}{4}$ и

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

если $\frac{ul^2}{4} \leq P_1 \leq n-3l-1 - \frac{ul^2}{4}$.

Для доказательства теоремы нужно, чтобы выполнялись неравенства $\frac{ul^2}{4} \leq P_1 \leq \frac{n+1}{2}$. В условиях теоремы имеем $n \geq 6l + \frac{ul^2}{2} + 3$, что равносильно $n-3l-1 - \frac{ul^2}{4} \geq \frac{n+1}{2}$. Значит, при $n \geq 6l + \frac{ul^2}{4} + 3$, $\frac{ul^2}{4} \leq P_1 \leq \frac{n+1}{2}$ выражение (22) принимает вид:

$$-\frac{l^2}{4}n + \frac{ul^2}{4} \left(n-3l-1 - \frac{ul^2}{4} \right) \leq 0.$$

Разделив обе части неравенства на $\frac{l^2}{4}$ и приведя подобные члены, получаем

$$(u-1)n - u \left(3l+1 + \frac{ul^2}{4} \right) \leq 0. \quad (23)$$

Легко видеть, что при $u > 1$ и $n > \frac{u}{u-1} \left(3l+1 + \frac{ul^2}{4} \right)$ левая часть (23) больше нуля. Противоречие. Теорема 4 доказана.

3.2. Второе семейство

Для доказательства теоремы 5 нам понадобится

Лемма 9. Пусть x_1, \dots, x_k — произвольные натуральные числа такие, что $x_1 + \dots + x_k = S > 0$ и $\max\{x_i\} - \min\{x_i\} \leq l$. Тогда

$$\frac{S^2}{k} \leq x_1^2 + \dots + x_k^2 \leq \frac{S^2}{k} + \frac{kl^2}{4}.$$

Доказательство. *Нижняя оценка.* Ясно, что минимум суммы квадратов достигается, если все x_i равны между собой. Следовательно, все x_i равны $\frac{S}{k}$ и сумма их квадратов равна $k \cdot \frac{S^2}{k^2} = \frac{S^2}{k}$.

Верхняя оценка. Если $\min\{x_i\} = h$, то $\max\{x_i\} \leq h + l$.

Легко проверить, что для любых двух чисел x_i и x_j таких, что $h < x_i \leq x_j < h + l$, выполняется неравенство

$$x_i^2 + x_j^2 < (x_i - 1)^2 + (x_j + 1)^2.$$

Преобразуем сумму $\Sigma := x_1^2 + \dots + x_k^2$ следующим образом. Если имеются два числа x_i и x_j , удовлетворяющие условию $h < x_i \leq x_j < h + l$, то заменим x_i на $x_i - 1$, а x_j на $x_j + 1$. При этом сумма всех чисел не изменится, а сумма их квадратов в силу неравенства (24) увеличится. Если имеется только одно число $x_i \neq h$ и $x_i \neq h + l$, то x_i представим в виде $x_i = k_1 h + (1 - k_1)(h + l)$, где $k_1 = \frac{h+l-x_i}{l}$. В результате получаем

$$\Sigma = x_1^2 + \dots + x_k^2 \leq k_0 h^2 + (k - k_0)(h + l)^2, \quad S = k_0 h + (k - k_0)(h + l).$$

Из второго уравнения получаем, что $k_0 = \frac{k(h+l)-S}{l}$. Подставив полученное значение k_0 в оценку для Σ , имеем

$$\Sigma \leq \frac{k(h+l)-S}{l} h^2 + \frac{S-kh}{l} (h+l)^2 = -kh^2 + (2S-kl)h + lS. \quad (24)$$

Заметим, что полученная оценка является квадратичной относительно h . Поскольку коэффициент при h^2 отрицательный, величина $-kh^2 + (2S-kl)h + lS$ принимает наибольшее значение в вершине параболы, т. е. при $h_0 = \frac{2S-kl}{2k}$. Подставив полученное значение h_0 в неравенство (24), получаем

$$\Sigma \leq -k \left(\frac{2S-kl}{2k} \right)^2 + (2S-kl) \frac{2S-kl}{2k} + lS = \frac{S^2}{k} + \frac{kl^2}{4}.$$

Лемма 9 доказана.

Теорема 5. Пусть l — фиксированное натуральное число. Тогда в левом кубе достаточно большой размерности n не существует кодов мощности m , равномерно распределённых по шарам со степенью l , где

$$\lambda_1 \frac{2^n}{\sum_{i=0}^s \binom{n}{i}} \leq m \leq \lambda_2 \frac{2^n}{\sum_{i=0}^s \binom{n}{i}},$$

λ_1 и λ_2 — некоторые положительные числа.

Замечание 5. Положительные числа λ_1 и λ_2 выбираем так, чтобы первое и второе семейства мощностей пересекались.

Доказательство теоремы 5. Пусть C является l -РРШ кодом размерности n и мощности m .

Найдём число N пар кодовых наборов во всех шарах радиуса s двумя способами. Затем сравним две полученные величины и придём к противоречию.

Первый способ заключается в следующем. Обозначим через x_1, x_2, \dots, x_{2^n} веса шаров радиуса s . Так как каждый кодовый набор содержится ровно в $\sum_{i=0}^s \binom{n}{i}$ шарах радиуса s , то $S := x_1 + \dots + x_{2^n} = m \cdot \sum_{i=0}^s \binom{n}{i}$.

Число пар кодовых наборов в шаре радиуса s веса x_i равно $\frac{x_i(x_i-1)}{2}$. Следовательно, число пар кодовых наборов во всех шарах радиуса s равно

$$N = \sum_{i=0}^{2^n} \frac{x_i(x_i-1)}{2} = \frac{1}{2} \sum_{i=0}^{2^n} x_i^2 - \frac{1}{2} \sum_{i=0}^{2^n} x_i. \quad (25)$$

Так как C является l -РРШ кодом, то $\max\{x_i\} - \min\{x_i\} \leq l$. Значит, для оценки первого слагаемого можно применить лемму 9. Поэтому

$$\frac{S^2}{2^n} \leq \sum_{i=0}^{2^n} x_i^2 \leq \frac{S^2}{2^n} + \frac{2^n l^2}{4}.$$

Используя определение s и лемму 7, выразим S^2 через m , n и s :

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

Далее, подставив полученные выражения в (25), получаем

$$\begin{aligned}
& \frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(s!)^2} (n^{2s} + (3s - s^2)n^{2s-1} + O(n^{2s-2})) \\
& - \frac{m}{2} \cdot \frac{1}{s!} \left(n^s + \frac{3s - s^2}{2} n^{s-1} + O(n^{s-2}) \right) \leq N \\
& \leq \frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(s!)^2} (n^{2s} + (3s - s^2)n^{2s-1} + O(n^{2s-2})) \\
& - \frac{m}{2} \cdot \frac{1}{s!} \left(n^s + \frac{3s - s^2}{2} n^{s-1} + O(n^{s-2}) \right) + \frac{2^n l^2}{8}. \quad (26)
\end{aligned}$$

Число N пар кодовых наборов, находящихся во всех шарах радиуса s , первым способом получено.

Второй способ подсчёта числа всех пар кодовых наборов, находящихся во всех шарах радиуса s , заключается в следующем. В шарах радиуса s содержатся пары кодовых наборов, находящихся друг от друга на расстоянии от 1 до $2s$. Рассмотрим шары радиуса $2s$ с центрами в кодовых наборах. Разобьём эти шары на сферы радиусом от 1 до $2s$, оценим вес каждой сферы и число пар кодовых наборов, находящихся друг от друга на расстоянии 1, 2 и так далее до $2s$ отдельно. Затем получим общее число пар всех кодовых наборов, находящихся друг от друга на расстоянии не более $2s$ и эту оценку сравним с оценкой, полученной первым способом.

Сначала найдём объём шара радиуса k . Воспользовавшись леммой 7, получаем

$$V_k = \sum_{i=0}^k \binom{n}{i} = \frac{1}{k!} \left(n^k + \frac{3k - k^2}{2} n^{k-1} + O(n^{k-2}) \right). \quad (27)$$

Средний вес шара радиуса k равен $P_k = \frac{mV_k}{2^n}$, поскольку каждый кодовый набор содержится ровно в V_k шарах радиуса k , а в булевом n -мерном кубе имеется 2^n шаров радиуса k .

Поскольку C является l -РРШ кодом, то вес произвольного шара $S_k(x)$ радиуса k удовлетворяет неравенству

$$\frac{mV_k}{2^n} - l \leq w(S_k(x)) \leq \frac{mV_k}{2^n} + l. \quad (28)$$

Обозначим через $w(\rho_k(x))$ вес сферы радиуса k с центром в x . Вычислим его по формуле $w(\rho_k(x)) = w(S_k(x)) - w(S_{k-1}(x))$. Вес произвольной

сферы ρ_k радиуса k удовлетворяет неравенству

$$\begin{aligned} \min\{w(S_k(x))\} - \max\{w(S_{k-1}(x))\} &\leq w(\rho_k) \\ &\leq \max\{w(S_k(x))\} - \min\{w(S_{k-1}(x))\}. \end{aligned} \quad (29)$$

Обозначим через N_k число пар двоичных наборов кода C , находящихся друг от друга на расстоянии k . Для вычисления N_k рассмотрим сферу $\rho_k(\alpha)$ радиуса k с центром в наборе $\alpha \in C$. Все наборы, находящиеся от набора α на расстоянии k , попадут в сферу $\rho_k(\alpha)$. Вес этой сферы равен $w(\rho_k(\alpha))$. Аналогичным образом рассмотрим все остальные кодовые наборы. Таким образом, каждая пара наборов (α_1, α_2) будет посчитана дважды: как пара, содержащая набор α_1 , и как пара, содержащая набор α_2 . Поскольку $|C| = m$, число пар двоичных наборов кода C , находящихся друг от друга на расстоянии k , удовлетворяет неравенству

$$\frac{m}{2} \min\{w(\rho_k)\} \leq N_k \leq \frac{m}{2} \max\{w(\rho_k)\}. \quad (30)$$

Искомое число пар кодовых наборов во всех шарах радиуса s равно

$$N = \sum_{k=1}^{2s} N_k \cdot p_k, \quad (31)$$

где p_k — количество шаров радиуса s , в которые попадает каждая пара наборов, находящихся друг от друга на расстоянии k . Согласно лемме 8 выполняются равенства $p_{2k} = p_{2k-1}$. Поэтому сумму (31) можно представить в виде

$$N = (N_{2s} + N_{2s-1}) \cdot p_{2s} + (N_{2s-2} + N_{2s-3}) \cdot p_{2s-2} + (N_{2s-4} + N_{2s-5}) \cdot p_{2s-4} + \dots$$

Таким образом, достаточно оценить не сами N_k , а суммы вида $N_{2k} + N_{2k-1}$. Согласно (30) имеем

$$\begin{aligned} \frac{m}{2} \min\{w(\rho_{2k}) + w(\rho_{2k-1})\} &\leq N_{2k} + N_{2k-1} \leq \\ &\leq \frac{m}{2} \max\{w(\rho_{2k}) + w(\rho_{2k-1})\}. \end{aligned} \quad (32)$$

Отсюда, используя (29) и (28), получаем

$$\frac{m}{2^n} (V_{2k} - V_{2k-2}) - 2l \leq w(\rho_{2k}) + w(\rho_{2k-1}) \leq \frac{m}{2^n} (V_{2k} - V_{2k-2}) + 2l. \quad (33)$$

В дальнейшем для более компактной записи выкладок мы будем писать $t = x \pm 2l$ вместо двойного неравенства $x - 2l \leq t \leq x + 2l$.

Найдём разность объёмов шаров радиуса $2k$ и $2k - 2$ при каждом $k \leq s$, используя (27). Имеем

$$\begin{aligned} V_{2s} - V_{2s-2} &= \frac{1}{(2s)!} \left(n^{2s} + \frac{3 \cdot 2s - (2s)^2}{2} n^{2s-1} + O(n^{2s-2}) \right), \\ V_{2s-2} - V_{2s-4} &= \frac{1}{(2s-2)!} \left(n^{2s-2} + \frac{3 \cdot (2s-2) - (2s-2)^2}{2} n^{2s-3} + O(n^{2s-4}) \right); \end{aligned}$$

а при $k \geq 2$

$$V_{2s-2k} - V_{2s-2(k+1)} = \frac{1}{(2s-2k)!} \left(n^{2s-2k} + O(n^{2s-2k-1}) \right).$$

Теперь найдём оценки для всех сумм $N_{2k} + N_{2k-1}$, подставляя полученные значения в (33) и (32). Имеем

$$\begin{aligned} N_{2s} + N_{2s-1} &= \frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(2s)!} \left(n^{2s} + \frac{6s - 4s^2}{2} n^{2s-1} + O(n^{2s-2}) \right) \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l, \\ N_{2s-2} + N_{2s-3} &= \frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(2s-2)!} \left(n^{2s-2} + \frac{6s-6 - (2s-2)^2}{2} n^{2s-3} + O(n^{2s-4}) \right) \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l, \end{aligned}$$

а при $k \geq 2$

$$N_{2s-2k} + N_{2s-2k-1} = \frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(2s-2k)!} \left(n^{2s-2k} + O(n^{2s-2k-1}) \right) \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l.$$

Таким образом, искомая сумма N принимает вид:

$$\begin{aligned} N &= \sum_{k=1}^{2s} N_k \cdot p_k = \sum_{k=0}^{s-1} (N_{2s-2k} + N_{2s-2k-1}) \cdot p_{2s-2k} \\ &= \left(\frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(2s)!} \left(n^{2s} + \frac{6s-4s^2}{2} n^{2s-1} + O(n^{2s-2}) \right) \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l \right) \cdot \binom{2s}{s} \\ &\quad + \left(\frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(2s-2)!} \left(n^{2s-2} + \frac{6s-6 - (2s-2)^2}{2} n^{2s-3} + O(n^{2s-4}) \right) \right. \\ &\quad \left. \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l \right) \cdot \left(\binom{2s-2}{s-1} \cdot n + O(1) \right) \\ &\quad + \sum_{k=2}^{s-1} \left(\frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(2s-2k)!} \left(n^{2s-2k} + O(n^{2s-2k-1}) \right) \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l \right) \cdot O(n^k). \end{aligned}$$

Приведя подобные члены, получаем выражение числа пар N кодовых наборов во всех шарах радиуса s вторым способом:

$$N'' = \frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(s!)^2} \left(n^{2s} + (3s - s^2) n^{2s-1} + O(n^{2s-2}) \right) \pm \frac{m^2}{2 \cdot 2^n} \cdot 2l \cdot O(n^{s-1}). \quad (34)$$

Рассмотрим случай $m = \alpha \cdot \frac{2^n}{n^{s-1}} \cdot (s-1)!$. Имеем

$$\frac{m^2}{2 \cdot 2^n} \cdot \frac{1}{(s!)^2} = \alpha^2 \cdot \frac{(2^n)^2 \cdot ((s-1)!)^2}{n^{2s-2}} \cdot \frac{1}{2 \cdot 2^n} \cdot \frac{1}{(s!)^2} = \frac{\alpha^2 \cdot 2^n}{2s^2} \cdot \frac{1}{n^{2s-2}}.$$

При данном значении мощности кода оценки (34) и (26) примут вид:

$$\begin{aligned} N'' &= \frac{\alpha^2 \cdot 2^n}{2s^2} \cdot \frac{1}{n^{2s-2}} \left(n^{2s} + (3s - s^2) n^{2s-1} + O(n^{2s-2}) \right) \\ &\quad \pm \frac{\alpha^2 \cdot 2^n}{s^2} \cdot \frac{((s-1)!)^2}{n^{2s-2}} \cdot 2l \cdot O(n^{s-1}) \\ &= \frac{\alpha^2 \cdot 2^n}{2s^2} \left(n^2 + (3s - s^2) n + O(1) \pm O(n^{-s+1}) \right), \end{aligned}$$

$$\begin{aligned} &\frac{\alpha^2 \cdot 2^n}{2s^2} \cdot \frac{1}{n^{2s-2}} \left(n^{2s} + (3s - s^2) n^{2s-1} + O(n^{2s-2}) \right) \\ &\quad - \frac{\alpha \cdot 2^n}{2s} \cdot \frac{1}{n^{s-1}} \left(n^s + \frac{3s - s^2}{2} n^{s-1} + O(n^{s-2}) \right) \\ &\leq N' \leq \frac{\alpha^2 \cdot 2^n}{2s^2} \cdot \frac{1}{n^{2s-2}} \left(n^{2s} + (3s - s^2) n^{2s-1} + O(n^{2s-2}) \right) \\ &\quad - \frac{\alpha \cdot 2^n}{2s} \cdot \frac{1}{n^{s-1}} \left(n^s + \frac{3s - s^2}{2} n^{s-1} + O(n^{s-2}) \right) + \frac{2^n l^2}{8}. \end{aligned}$$

Верхняя и нижняя оценки для N' отличаются только наличием слагаемого $\frac{2^n l^2}{8}$ в верхней оценке.

Упростим верхнюю оценку для N' :

$$\begin{aligned} N' &\leq \frac{\alpha^2 \cdot 2^n}{2s^2} \left(n^2 + (3s - s^2) n + O(1) \right) \\ &\quad - \frac{\alpha \cdot 2^n}{2s} \left(n + \frac{3s - s^2}{2} + O(n^{-1}) \right) + \frac{2^n l^2}{8} \\ &= \frac{\alpha^2 \cdot 2^n}{2s^2} \left(n^2 + (3s - s^2) n - \frac{s}{\alpha} n + O(1) \right). \end{aligned}$$

Таким образом, разность между верхней и нижней оценками для N' равна $\frac{\alpha^2 \cdot 2^n}{2s^2} \cdot O(1)$.

Следовательно, с одной стороны

$$N = N'' = \frac{\alpha^2 \cdot 2^n}{2s^2} \left(n^2 + (3s - s^2)n + O(1) \right),$$

а с другой стороны

$$N = N' \leq \frac{\alpha^2 \cdot 2^n}{2s^2} \left(n^2 + (3s - s^2)n - \frac{s}{\alpha}n + O(1) \right).$$

Поскольку верхняя оценка отличается от нижней наличием слагаемого $-\frac{s}{\alpha}n$, то, начиная с некоторого n , оценка N' будет меньше оценки N'' . Противоречие. Теорема 5 доказана.

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

ЛИТЕРАТУРА

1. Гаврилов Г. П., Сапоженко А. А. Сборник задач по дискретной математике. М.: Наука, 1977.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. Таранников Ю. В. О классе булевых функций, равномерно распределённых по шарам со степенью 1 // Вестник Московского университета. Сер. 1. Математика. Механика. 1997. № 5. С. 18–22.
4. 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.
5. Ярыкина М. С. Несуществование двоичных кодов, равномерно распределённых по шарам, почти всех мощностей // Материалы VI молодежной научной школы по дискретной математике и ее приложениям (Москва, 16–21 апреля 2007 г.), Ч. III. С. 52–56.

- 6. Fedorova M., Tarannikov Yu.** On impossibility of uniform distribution of codewords over spheres in some cases. // Proc. of 2002 IEEE International symposium on information theory ISIT2002, Lausanne, Switzerland, June 30–July 05, 2002. P. 344.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьёвы горы,
119992 Москва,
Россия.
E-mail: marie@plushka.msk.ru

Статья поступила

13 января 2008 г.

Переработанный вариант —

4 марта 2008 г.