Math-Net.Ru

Общероссийский математический портал

А. В. Бобу, А. Э. Куприянов, А. М. Райгородский,
Асимптотическое исследование задачи о максимальном
числе ребер однородного гиперграфа с одним запре-
щенным пересечением, *Матем. сб.*, 2016, том 207, но-
мер 5, 17–42

DOI: <https://doi.org/10.4213/sm8473>

Использование Общероссийского математического портала Math-Net.Ru под-
разумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.207.199.55

26 апреля 2023 г., 18:01:05

УДК 519.112.74+519.176

А. В. Бобу, А. Э. Куприянов, А. М. Райгородский

Асимптотическое исследование задачи о максимальном числе ребер однородного гиперграфа с одним запрещенным пересечением

Исследуются величины $m(n, k, t)$ максимально возможного числа ребер в k -однородном гиперграфе, обладающем тем свойством, что никакие два ребра не пересекаются по t вершинам. Подробно рассматривается случай, когда $k \sim k'n$, $t \sim t'n$ при $n \rightarrow \infty$, а $k' \in (0, 1)$, $t' \in (0, k')$ – фиксированные константы. В случае $2t < k$ доказывается асимптотическая точность верхней оценки Франкла–Уилсона, в случае $2t \geq k$ приводятся новые нижние оценки величины $m(n, k, t)$. На основании последних получены верхние оценки классической в теории кодирования величины $A(n, 2\delta, \omega)$ – максимального числа двоичных векторов длины n и веса ω , находящихся друг от друга на хэмминговом расстоянии не менее 2δ .

Библиография: 38 названий.

Ключевые слова: гиперграфы с одним запрещенным пересечением ребер, теорема Франкла–Уилсона, равновесные коды, исправляющие ошибки, проблема Нельсона–Хадвигера.

DOI: 10.4213/sm8473

§ 1. Введение

Напомним, что *гиперграфом* называется пара $H = (V, E)$, где V – конечное множество, называемое *множеством вершин*, а E – некоторая совокупность, состоящая из подмножеств множества V и называемая *множеством ребер*. Гиперграф называется *k -однородным*, если в каждом его ребре ровно k вершин. В частности, 2-однородный гиперграф – это обычный граф.

Одна из классических задач экстремальной комбинаторики состоит в отыскании максимального числа $m(n, k, t)$ ребер в k -однородном гиперграфе на n вершинах, у которого никакие два ребра не могут пересекаться ровно по t вершинам, $t < k$:

$$m(n, k, t) = \max\{m : \exists H = (V, E), |V| = n, |E| = m, \forall A \in E \quad |A| = k, \\ \forall A, B \in E \quad |A \cap B| \neq t\}.$$

Эта задача имеет большое значение для теории кодирования, где она носит название задачи о кодах с запрещенным расстоянием (см. [1], [2]). Суть в том,

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 15-01-03530), Программы Президента РФ поддержки молодых докторов наук (грант № МД-6008.2015.1) и Программы Президента РФ поддержки ведущих научных школ (грант № НШ-2964.2014.1).

что ребра k -однородного гиперграфа на n вершинах можно естественно интерпретировать как слова равновесного двоичного кода веса k , и тогда условие отсутствия пересечений мощности t эквивалентно условию отсутствия хэммингова расстояния величины $2(k - t)$. Наконец, задача допускает интерпретацию в терминах дистанционных графов, которые исключительно важны для таких задач комбинаторной геометрии, как проблема Борсука (см. [3]–[7]) и проблема Нельсона–Хадвигера (см. [8]–[14], а также § 5 настоящей работы). В этом случае рассматривают граф $G(n, k, t) = (V(n, k), E(n, k, t))$, у которого

$$V(n, k) = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = k\},$$

$$E(n, k, t) = \{\{\mathbf{x}, \mathbf{y}\} : |\mathbf{x} - \mathbf{y}| = \sqrt{2(k - t)}\},$$

где $|\mathbf{x} - \mathbf{y}|$ – евклидово расстояние в $\mathbb{R}^n$. Ясно, что $m(n, k, t) = \alpha(G(n, k, t))$, коль скоро для произвольного графа G мы определяем величину $\alpha(G)$ как максимальную мощность *независимого множества вершин* графа, т.е. такого множества его вершин, которые попарно не соединены ребрами (величину $\alpha(G)$ называют *числом независимости* графа). Отметим, что в настоящей работе будут по существу использованы обе интерпретации.

В 1981 г. в работе [15], ставшей классической, П. Франкл и Р. М. Уилсон доказали следующую теорему.

ТЕОРЕМА 1. Пусть $t = k - q$, где q – степень простого числа. Тогда имеют место два случая:

1) если $2t < k$, то

$$m(n, k, t) \leq \sum_{i=0}^{q-1} C_n^i;$$

2) если $2t \geq k$, то

$$m(n, k, t) \leq \frac{C_n^d}{C_k^d} \left(\sum_{i=0}^{q-1} C_{n-d}^i \right)$$

$$\text{при } d = k - 2q + 1 = 2t - k + 1.$$

Если при $n \rightarrow \infty$ числа k и t достаточно малы в сравнении с n , то теорема 1 асимптотически точна. В частности, весьма детальное исследование случая, когда k и t фиксированы, а $n \rightarrow \infty$, проведено в статье [16]. Однако в противоположной ситуации, называемой в теории кодирования *асимптотической*, все намного сложнее. А именно, в работах [17], [18] была доказана следующая теорема.

ТЕОРЕМА 2. Пусть $k \leq n/2$, $2t \geq k$ и $t = k - q$, где q – степень простого числа. Положим $d = 2t - k + 1$. Пусть, далее, $d_1, d_2 \in \mathbb{N}$ таковы, что $d_1 + d_2 = d$. Положим $n_1 = n - d_1$, $k_1 = k - d_1$. Определим натуральное число r из соотношения

$$(k_1 - d_2 + 1) \left(2 + \frac{d_2 - 1}{r + 1} \right) \leq n_1 < (k_1 - d_2 + 1) \left(2 + \frac{d_2 - 1}{r} \right).$$

Тогда

$$m(n, k, t) \leq \frac{C_{n_1}^{d_2+2r} C_n^{d_1}}{C_{k_1}^{d_2+r} C_{n_1-k_1}^r C_k^{d_1}} \left(\sum_{i=0}^{q-1} C_{n_1}^i \right).$$

Конечно, не очевидно, что двойное неравенство в формулировке теоремы 2 определяет некоторое натуральное r , причем единственным образом. Однако элементарными преобразованиями легко получить следующее неравенство:

$$\frac{(d_2 + 1)(k_1 - d_2 + 1)}{n_1 - 2k_1 + 2d_2 - 2} - 1 \leq r < \frac{(d_2 + 1)(k_1 - d_2 + 1)}{n_1 - 2k_1 + 2d_2 - 2}.$$

Таким образом, можно явно указать значение параметра r :

$$r = \left\lceil \frac{(d_2 + 1)(k_1 - d_2 + 1)}{n_1 - 2k_1 + 2d_2 - 2} - 1 \right\rceil.$$

Видно, что теорема 2 касается случая 2) теоремы 1. В работах [17], [18] показано, что теорема 2 значительно уточняет оценку из случая 2) теоремы 1 в классе ситуаций, который и носит название асимптотического и который мы сейчас опишем. Итак, пусть даны числа $k' \in (0, 1)$, $t' \in (0, k')$. Пусть, далее, $k \sim k'n$, $t \sim t'n$ при $n \rightarrow \infty$. С учетом формулы Стирлинга нетрудно убедиться в том, что в указанных предположениях все интересующие нас оценки имеют вид $(c + o(1))^n$, где $c > 1$ — константа, т.е. их логарифмы асимптотически равны $n \ln c$. И две оценки разнятся значительно, если у них разные величины c . Оказалось (см. [18]), что при $2t \geq k$ оценки из теоремы 2 значительно сильнее оценок Франкла–Уилсона. (Правда, оптимум всякий раз получался при $d_1 = 0$.)

Таким образом, естественно возникают вопросы:

- 1) точна ли теорема 1 в случае 1)?
- 2) точна ли теорема 2 или и ее можно улучшать?

На вопрос 1) мы дадим ответ в § 2. А в § 3 и § 4 мы получим ряд нетривиальных нижних границ для функции $m(n, k, t)$ при $2t \geq k$ и увидим, насколько тесно такая проблематика связана с классическими задачами теории кодирования об отыскании границ для кодов, исправляющих ошибки. Подчеркнем, что всякий раз речь будет идти только об асимптотических ситуациях.

§ 2. Точность теоремы 1 в случае 1)

Пусть, как и предполагается в асимптотической ситуации, $k \sim k'n$, $t \sim t'n$ при $n \rightarrow \infty$, причем имеет место случай 1) теоремы 1, т.е. $2t < k$. Тогда верхняя оценка Франкла–Уилсона с учетом формулы Стирлинга имеет величину вида

$$\left(\frac{1}{(k' - t')^{k' - t'} (1 - k' + t')^{1 - k' + t'}} + o(1) \right)^n.$$

Часто такие величины записывают с помощью функции энтропии: $H(a) = -a \ln a - (1 - a) \ln(1 - a)$. Однако у нас будет в дальнейшем много разных сложных биномиальных коэффициентов, и мы будем для максимальной прозрачности использовать обозначение

$$c_x^y = \frac{x^x}{y^y (x - y)^{x - y}},$$

для которого, очевидно,

$$C_{f(n)}^{g(n)} = (c_x^y + o(1))^n,$$

где $f(n)$ – любая функция, имеющая асимптотику xn при $n \rightarrow \infty$, а $g(n)$ – любая функция, имеющая асимптотику yn при $n \rightarrow \infty$. Здесь, разумеется, $0 < y < x$. Формально при $x = y$ полагаем $c_x^y = 1$. В этих терминах оценка из случая 1) теоремы 1 имеет вид

$$m(n, k, t) \leq (c_1^{k'-t'} + o(1))^n.$$

Покажем, что

$$m(n, k, t) \geq (c_1^{k'-t'} + o(1))^n.$$

Именно в этом смысле мы понимаем слово “точность” из названия параграфа. С указанной целью введем новую величину

$$f(n, k, t) = \max \{ m : \exists H = (V, E), |V| = n, |E| = m, \forall A \in E \quad |A| = k, \\ \forall A, B \in E \quad |A \cap B| \geq t \}.$$

Иными словами, теперь мы запрещаем ребрам гиперграфа иметь в пересечении меньше t вершин, а не ровно t вершин, как это было раньше. Ясно, что $m(n, k, t) \geq f(n, k, t + 1)$.

Задача отыскания величины $f(n, k, t)$ также является классической проблемой на стыке экстремальной комбинаторики и теории кодирования. Хотя она исключительно трудна, но все-таки значительно проще нашей основной задачи, и сейчас она полностью решена. Справедлива следующая теорема (см. [19]–[21]).

ТЕОРЕМА 3. Пусть $2k - t \leq n$. Тогда

$$f(n, k, t) = \max_{r: 0 \leq r \leq k-t} \sum_{i=r}^{\min\{2r, k-t\}} C_{t+2r}^{t+i} C_{n-2r}^{k-t-i}.$$

Доказательство теоремы весьма непростое, но легко понять, как устроен гиперграф с числом ребер, равным одной из сумм, фигурирующих в формулировке. Фиксируется произвольное множество A вершин, имеющее мощность $t + 2r$, и в качестве ребер берутся все k -элементные подмножества множества вершин, мощность пересечения которых с A не меньше $t + r$: уже внутри A такие ребра пересекаются хотя бы по t вершинам, а это нам и нужно.

Величина r , на которой достигается максимум в теореме 3, также известна. Для нас достаточно того, что она имеет вид $r \sim r'n$, где

$$r' = \frac{(k' - t')t'}{1 - 2k' + 2t'}.$$

Отметим, что условие $2k - t \leq n$ означает всего лишь, что не каждые два k -элементных подмножества n -элементного множества пересекаются по t и более элементам. Иначе, очевидно, $f(n, k, t) = C_n^k$. Также заметим, что нам нужно значение r' для параметров $n, k, t + 1$, но оно такое же, как приведенное выше, поскольку $t + 1$ и t в асимптотике одинаковы. В итоге имеем

$$m(n, k, t) \geq f(n, k, t + 1) \geq (c_{t'+2r'}^{t'+r'} c_{1-t'-2r'}^{k'-t'-r'} + o(1))^n.$$

Остается доказать, что

$$c_{t'+2r'}^{t'+r'} c_{1-t'-2r'}^{k'-t'-r'} = c_1^{k'-t'}.$$

Положим

$$\begin{aligned} a = t' + 2r' &= \frac{t'}{1 - 2k' + 2t'}, & b = 1 - a &= \frac{1 - 2k' + t'}{1 - 2k' + 2t'}, \\ c = k' - t', & & d = 1 - k' + t'. \end{aligned}$$

Тогда

$$c_{t'+2r'}^{t'+r'} c_{1-t'-2r'}^{k'-t'-r'} = \frac{a^a}{(ad)^{ad}(ac)^{ac}} \cdot \frac{b^b}{(bc)^{bc}(bd)^{bd}} = \frac{1}{(c^c d^d)^{a+b}} = \frac{1}{c^c d^d} = c_1^{k'-t'},$$

и точность оценки из случая 1) теоремы 1 установлена.

§ 3. О нижних границах в случае, когда $2t \geq k$

3.1. Оценки с помощью теоремы 3. Мы могли бы и в текущем случае попробовать применить оценку из теоремы 3 (см. § 2). К сожалению (и это интуитивно ожидаемо), чем ближе t к k , тем худшим получается результат. На рис. 1 и рис. 2 наглядно показан этот эффект. На обоих рисунках по горизонтали откладывается t' в пределах от $k'/2$ до k' . По вертикали откладывается оценка величины $\ln m(n, k'n, t'n)/n$ — это либо нижняя оценка из теоремы 3 (она названа AKh в честь ее авторов Алсведе и Хачатряна), либо верхняя оценка из теоремы 2 (она обозначена Upper). На рис. 1 изображен случай $k' = 0.5$, на рис. 2 — случай $k' = 0.1$.

Рис. 1. Сравнение оценки из теоремы 3 и оценки из теоремы 2 при $k' = 0.5$:
 ---- AKh; — Upper

Рис. 2. Сравнение оценки из теоремы 3 и оценки из теоремы 2 при $k' = 0.1$:
 ---- AKh; — Upper

3.2. Граница Варшавова–Гилберта. Следующая простая идея о том, как можно преодолеть трудность, возникшую в п. 3.1, состоит в использовании границ для кодов, исправляющих ошибки. В наших обозначениях $m(n, k, t) \geq h(n, k, t - 1)$, где

$$h(n, k, t) = \max \left\{ m : \exists H = (V, E), |V| = n, |E| = m, \forall A \in E \quad |A| = k, \right. \\ \left. \forall A, B \in E \quad |A \cap B| \leq t \right\}.$$

Иными словами, теперь мы не разрешаем ребрам пересекаться по $t + 1$ и более вершинам.

Следующая теорема дает классическую границу Варшавова–Гилберта (см. [1], [22]–[24]).

ТЕОРЕМА 4. Пусть $2k - t \leq n$. Тогда

$$h(n, k, t) \geq \frac{C_n^k}{\sum_{i=t+1}^k C_k^i C_{n-k}^{k-i}}$$

и величина в правой части неравенства имеет вид $(c(k', t') + o(1))^n$, коль скоро $k \sim k'n$, $t \sim t'n$ при $n \rightarrow \infty$.

Как и в п. 3.1, мы приведем рис. 3 с $k' = 0.5$ и рис. 4 с $k' = 0.1$, показывающие, как соотносятся оценки из теоремы 2 с оценками из теорем 3 и 4 (на этих рисунках оценка из теоремы 4 обозначена VG). Видно, что при t' , расположенных ближе к $k'/2$, получается довольно хорошая оценка за счет теоремы 3, а ближе к правой границе интервала значений t' выигрывает теорема 4. Все это пока совсем просто и ожидаемо. Надо бы улучшить оценки в середине интервала. В следующем параграфе мы попытаемся в некотором смысле “склеить” конструкции, дающие оценки из теорем 3 и 4.

В очень небольшом диапазоне параметров граница Зиновьева–Эриксона (см. [25]) дает чуть лучший результат, нежели граница Варшавова–Гилберта. Однако ни здесь, ни где-либо в дальнейшем это улучшений не дает, и потому границу мы не приводим.

Рис. 3. Сравнение оценок из теорем 3 и 4 и оценки из теоремы 2 при $k' = 0.5$:
 ---- AKh; VG; — Upper

Рис. 4. Сравнение оценок из теорем 3 и 4 и оценки из теоремы 2 при $k' = 0.1$:
 ---- AKh; VG; — Upper

3.3. “Склейка” конструкций из теорем 3 и 4. Идейно то, что мы сейчас сделаем, переключается с тем, что сделано в работе [26]. Суть в следующем. Мы помним (см. пояснение после формулировки теоремы 3), что в конструкции из теоремы 3 фиксируется некоторое множество A мощности $t + 2r$ и рассматриваются все k -элементные множества, которые имеют с A больше $t + r$ общих элементов. Любые два таких k -элементных множества пересекаются больше чем по t элементам. Попробуем теперь построить много таких конструкций, стараясь следить за тем, чтобы множества из разных конструкций пересекались меньше, чем по t элементам. Возможно, для этого достаточно просто взять много $(t + 2r)$ -элементных множеств, у которых попарные пересечения

имеют мощности, не превосходящие некоторого t_1 , подобранного правильно¹. В самом деле, справедлива следующая теорема.

ТЕОРЕМА 5. Пусть, как и в теореме 3, $2k - t \leq n$ и $0 \leq r \leq k - t$. Положим $t_1 = 3t + 2r - 2k$ и допустим, что $2(t + 2r) - t_1 \leq n$. Тогда

$$m(n, k, t) \geq \frac{C_n^{t+2r} \sum_{i=r+1}^{\min\{2r, k-t\}} C_{t+2r}^{t+i} C_{n-t-2r}^{k-t-i}}{\sum_{j=t_1}^{t+2r} C_{t+2r}^j C_{n-t-2r}^{t+2r-j}}.$$

ДОКАЗАТЕЛЬСТВО. Условие $2(t + 2r) - t_1 \leq n$ гарантирует, что применима теорема 4 и, стало быть, существует такая совокупность $(t + 2r)$ -элементных множеств $\mathcal{F}$, что для любых двух множеств $A, B \in \mathcal{F}$ выполнено $|A \cap B| < t_1$ и

$$|\mathcal{F}| = \frac{C_n^{t+2r}}{\sum_{j=t_1}^{t+2r} C_{t+2r}^j C_{n-t-2r}^{t+2r-j}}.$$

Составим совокупность множеств $\mathcal{G}$ следующим образом. Для фиксированного множества $A \in \mathcal{F}$ рассмотрим все k -элементные множества, пересекающиеся с ним больше, чем по $t + r$ элементам, и возьмем объединение полученных совокупностей по всем множествам A . Иначе говоря,

$$\mathcal{G}_A = \{V : |V| = k, |A \cap V| > t + r\}, \quad \mathcal{G} = \bigcup_{A \in \mathcal{F}} \mathcal{G}_A.$$

Убедимся в том, что совокупность $\mathcal{G}$ искома. Прежде всего, докажем, что любые два множества $U, V \in \mathcal{G}$ не пересекаются по t элементам. С одной стороны, понятно, что если $U, V \in \mathcal{G}_A$, то $|U \cap V| > t$. С другой стороны, пусть $U \in \mathcal{G}_A, V \in \mathcal{G}_B$. Покажем, что $|U \cap V| < t$. Действительно, поскольку выполнено неравенство $|A \cap B| < t_1$, то внутри множества $A \cap B$ множества U и V имеют самое большее $t_1 - 1$ общих элементов. Кроме того, непосредственно из определения совокупностей $\mathcal{G}_A$ и $\mathcal{G}_B$ следует, что

$$|(\{1, \dots, n\} \setminus A) \cap U| < k - t - r, \quad |(\{1, \dots, n\} \setminus B) \cap V| < k - t - r.$$

Стало быть, в дополнении к множеству $A \cap B$ множества U и V имеют менее $2(k - t - r)$ общих элементов. Окончательно получаем

$$|U \cap V| < t_1 + 2(k - t - r) = t,$$

что и требовалось.

Теперь ясно, что для разных множеств A, B совокупности $\mathcal{G}_A, \mathcal{G}_B$ не пересекаются. При этом величина $|\mathcal{G}_A|$ от $A \in \mathcal{F}$ не зависит, откуда

$$|\mathcal{G}| = |\mathcal{F}| \cdot |\mathcal{G}_A| = \frac{C_n^{t+2r} \sum_{i=r+1}^{\min\{2r, k-t\}} C_{t+2r}^{t+i} C_{n-t-2r}^{k-t-i}}{\sum_{j=t_1}^{t+2r} C_{t+2r}^j C_{n-t-2r}^{t+2r-j}}.$$

Теорема доказана.

¹Хотелось бы, конечно, брать просто $t_1 = t$, но в дальнейшем будет видно, что так делать нельзя.

Как и ожидалось, теорема 5 усиливает на “центральных” участках теоремы 3 и 4. Однако соотношения между результатами разных теорем отнюдь не тривиальны. Приведем два стандартных рисунка. На рис. 5 изображен случай $k' = 0.5$, на рис. 6 – случай $k' = 0.1$. Видно, что при $k' = 0.5$ теорема 5 лишь на малом диапазоне преобладает над теоремами 3 и 4. А при $k' = 0.1$, напротив, участок превосходства теоремы 5 значителен. На рис. 7 и рис. 8 четко разграничены зоны действия разных теорем. Например, из рис. 7 следует, что для t' от 0.25 до примерно 0.37 превалирует теорема 3, затем где-то до 0.47 сильнее теорема 5 (теорема 5 на всех рисунках обозначена Glue), а дальше лучше всех работает теорема 4.

Рис. 5. Сравнение оценок из теорем 3–5 и оценки из теоремы 2 при $k' = 0.5$:
 ---- AKh; VG; -.-.- Glue; — Upper

Рис. 6. Сравнение оценок из теорем 3–5 и оценки из теоремы 2 при $k' = 0.1$:
 ---- AKh; VG; -.-.- Glue; — Upper

Рис. 7. Зоны действия оценок из теорем 3–5 при $k' = 0.5$ Рис. 8. Зоны действия оценок из теорем 3–5 при $k' = 0.1$

3.4. “Склейка” конструкций из теорем 3 и 4 с “выкидыванием”.

Следующее уточнение оценки величины $m(n, k, t)$ можно попытаться получить так. Склеиваем, как и в п. 3.3, конструкции из теорем 3 и 4. Однако вместо t_1 берем $s > t_1$. Естественно, мы уже не можем гарантировать, что с пересечением любых двух множеств в такой конструкции все в порядке. Но мы можем выкинуть из конструкции что-то “вредоносное” и в итоге все же реализовать нужный запрет.

ТЕОРЕМА 6. Пусть $2k - t \leq n$ и $0 \leq r \leq k - t$. Положим $t_1 = 3t + 2r - 2k$ и допустим, что $2(t + 2r) - t_1 \leq n$. Пусть, далее, $t_1 < s < t + 2r$. Пусть, наконец, $\mathcal{F}$ – такая совокупность $(t + 2r)$ -элементных множеств, что для любых двух множеств $A, B \in \mathcal{F}$ выполнено $|A \cap B| < s$ и

$$|\mathcal{F}| = \frac{C_n^{t+2r}}{\sum_{j=s}^{t+2r} C_{t+2r}^j C_{n-t-2r}^{t+2r-j}}.$$

Тогда

$$m(n, k, t) \geq |\mathcal{F}| \left(C_{t+2r}^{t+r+1} C_{n-t-2r}^{k-t-r-1} - |\mathcal{F}| \cdot C_{n-t-2r}^{k-t-r-1} \cdot \max_{t_1 \leq i < s} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1} \right).$$

ДОКАЗАТЕЛЬСТВО. Заметим, что существование совокупности $\mathcal{F}$ гарантируется теоремой 4. Действуем почти так же, как в доказательстве теоремы 5:

$$\mathcal{G}_A = \{V : |V| = k, |A \cap V| = t + r + 1\}, \quad \mathcal{G} = \bigcup_{A \in \mathcal{F}} \mathcal{G}_A.$$

Теперь мы построим совокупность $\mathcal{S} \subset \mathcal{G}$, в которой для любых двух множеств A и B выполнено $|A \cap B| \neq t$. Положим

$$\mathcal{S}_A = \bigcap_{B \in \mathcal{F}} \{V \in \mathcal{G}_A : |V \cap (A \cap B)| < t_1\}, \quad \mathcal{S} = \bigcup_{A \in \mathcal{F}} \mathcal{S}_A.$$

Для множеств из совокупности $\mathcal{S}$ уже применимы оценки из доказательства теоремы 5. Действительно, если $U \in \mathcal{S}_A, V \in \mathcal{S}_B$, то по определению совокупностей $\mathcal{S}_A$ и $\mathcal{S}_B$ имеем

$$|U \cap (A \cap B)| < t_1, \quad |V \cap (A \cap B)| < t_1,$$

а значит, внутри пересечения $A \cap B$ множества U и V имеют, как и ранее, самое большее t_1 общих элементов. Повторяя рассуждения из доказательства теоремы 5, получаем, что $|U \cap V| < t$.

Поскольку $m(n, k, t) \geq |\mathcal{S}|$, остается вычислить величину $|\mathcal{S}|$. Заметим, что

$$|\mathcal{G}_A| = C_{t+2r}^{t+r+1} C_{n-t-2r}^{k-t-r-1}.$$

В совокупность $\mathcal{S}_A$ не попали те множества из совокупности $\mathcal{G}_A$, которые для какого-нибудь $B \in \mathcal{F}$ пересекаются с множеством $A \cap B$ хотя бы по t_1 элементам (мы эти множества из $\mathcal{G}_A$ “выкинули”). Если $|A \cap B| = i$, где $t_1 \leq i < s$, то количество таких множеств есть

$$C_{n-t-2r}^{k-t-r} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1}.$$

В самом деле, чтобы получить все такие множества, сначала мы выбираем j элементов в множестве $A \cap B$; для этого есть ровно C_i^j способов. Выбрать $t+r-j+1$ элементов в множестве $A \setminus B$ можно $C_{t+2r-i}^{t+r-j+1}$ способами. Для выбора оставшихся элементов, лежащих в $\{1, \dots, n\} \setminus A$, есть еще $C_{n-t-2r}^{k-t-r-1}$ способов. Отсюда

$$|\mathcal{G}_A \setminus \mathcal{S}_A| \leq |\mathcal{F}| \cdot C_{n-t-2r}^{k-t-r-1} \cdot \max_{t_1 \leq i < s} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1}.$$

Совокупности $\mathcal{S}_A, \mathcal{S}_B$ не пересекаются. Поэтому

$$\begin{aligned} |\mathcal{S}| &= \sum_{A \in \mathcal{F}} |\mathcal{S}_A| = \sum_{A \in \mathcal{F}} (|\mathcal{G}_A| - |\mathcal{G}_A \setminus \mathcal{S}_A|) \\ &\geq \sum_{A \in \mathcal{F}} \left(C_{t+2r}^{t+r+1} C_{n-t-2r}^{k-t-r-1} - |\mathcal{F}| \cdot C_{n-t-2r}^{k-t-r-1} \cdot \max_{t_1 \leq i < s} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1} \right) \\ &= |\mathcal{F}| \left(C_{t+2r}^{t+r+1} C_{n-t-2r}^{k-t-r-1} - |\mathcal{F}| \cdot C_{n-t-2r}^{k-t-r-1} \cdot \max_{t_1 \leq i < s} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1} \right). \end{aligned}$$

Теорема 6 доказана.

Естественно, теорема 6 может давать улучшения лишь в случае, когда вычитаемое в оценке из этой теоремы мало в сравнении с уменьшаемым. Действительно, улучшения невелики, но они есть, о чем свидетельствуют наши обычные графики. На рис. 9 представлен случай $k' = 0.5$, на рис. 10 – случай $k' = 0.1$. Оценка теоремы 6 обозначена на них Super Glue. Вертикальные линии на этих графиках как раз свидетельствуют о ситуации, когда вычитаемое в оценке теоремы стало больше уменьшаемого. На рис. 11 и рис. 12 разграничены зоны действия теорем 3–6.

Рис. 9. Сравнение оценок из теорем 3–6 и оценки из теоремы 2 при $k' = 0.5$:
 ---- AKh; VG; ----- Glue; ----- Super Glue; — Upper

Рис. 10. Сравнение оценок из теорем 3–6 и оценки из теоремы 2 при $k' = 0.1$:
 ---- AKh; VG; ----- Glue; ----- Super Glue; — Upper

Рис. 11. Зоны действия оценок из теорем 3–6 при $k' = 0.5$ Рис. 12. Зоны действия оценок из теорем 3–6 при $k' = 0.1$

3.5. “Склейка” с двухкратным “выкидыванием”. Сформулируем и докажем многопараметрическую теорему, которая включает в себя все уже доказанные результаты и которая, как мы увидим позднее, дает весьма сильные границы.

ТЕОРЕМА 7. Пусть, как обычно, $2k - t \leq n$. Пусть, далее, f, r, l, t_1, s, x – натуральные числа, удовлетворяющие неравенствам

$$\begin{aligned} t + r + l &\leq k, & t + 2r + l &\leq f \leq n, & x &\leq l, \\ 2(t + 2r) - f &\leq t_1 = 2t + r - x - k < s < t + 2r, \\ n - f &\geq k - t - r - l - 1. \end{aligned}$$

Введем обозначение

$$|\mathcal{F}| = \frac{C_f^{t+2r}}{\sum_{j=s}^{t+2r} C_{t+2r}^j C_{f-t-2r}^{t+2r-j}}.$$

Тогда выполнена оценка

$$m(n, k, t) \geq |\mathcal{F}| \cdot C_{n-f}^{k-t-r-l-1} \cdot (C_{t+2r}^{t+r+1} C_{f-t-2r}^l - C_1 - C_2),$$

где слагаемые C_1 и C_2 имеют вид

$$C_1 = |\mathcal{F}| \cdot C_{f-t-2r}^l \cdot \max_{t_1 \leq i < s} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1},$$

$$C_2 = |\mathcal{F}| \cdot C_{t+2r}^{t+r+1} \cdot \max_{0 \leq i < s} \sum_{j=x+1}^l C_{t+2r-i}^j C_{f-2t-4r+i}^{l-j}.$$

ДОКАЗАТЕЛЬСТВО. Разобьем для удобства наше рассуждение на отдельные этапы.

Этап 1. Зафиксируем множество $F = \{1, \dots, f\} \subseteq \{1, \dots, n\}$. Для всякого $A \subset F$ введем обозначение $\bar{A} = F \setminus A$. По теореме 4 существует такая совокупность $\mathcal{F}$, состоящая из $(t+2r)$ -элементных подмножеств множества F , что ее мощность равна той самой величине, которую мы в формулировке теоремы обозначили $|\mathcal{F}|$, и что любые два множества из совокупности $\mathcal{F}$ пересекаются менее чем по s элементам.

Будем составлять совокупность $\mathcal{G}$ более или менее стандартным образом: для каждого $A \in \mathcal{F}$ положим

$$\mathcal{G}_A = \{V : |V| = k, |V \cap A| = t + r + 1, |V \cap \bar{A}| = l\}, \quad \mathcal{G} = \bigcup_{A \in \mathcal{F}} \mathcal{G}_A.$$

Отличие от того, что делалось, например, в теореме 6, состоит в том, что в теореме 6 фактически $f = n$, $l = k - t - r - 1$. Теперь же и по f , и по l появляется свобода. При этом в части $\{1, \dots, n\} \setminus \{1, \dots, f\}$ выбор “хвостиков” для множеств V вовсе ничем не ограничен.

Этап 2. Теперь сделаем первую операцию “выкидывания”: она будет, по сути, такой же, как в теореме 6. А именно, выберем подсовокупность $\mathcal{S} \subset \mathcal{G}$ следующим способом:

$$\mathcal{S}_A = \bigcap_{B \in \mathcal{F}} \{V \in \mathcal{G}_A : |V \cap (A \cap B)| < t_1\}, \quad \mathcal{S} = \bigcup_{A \in \mathcal{F}} \mathcal{S}_A.$$

Полученную совокупность снова уменьшим (второе “выкидывание”), взяв подсовокупность $\mathcal{U} \subset \mathcal{S}$:

$$\mathcal{U}_A = \bigcap_{B \in \mathcal{F}} \{V \in \mathcal{S}_A : |V \cap (\bar{A} \cap B)| \leq x\}, \quad \mathcal{U} = \bigcup_{A \in \mathcal{F}} \mathcal{U}_A.$$

Этап 3. Покажем, что множества из итоговой совокупности $\mathcal{U}$ действительно не пересекаются по t элементам. Ясно, что если произвольные U и V лежат в одной и той же совокупности $\mathcal{U}_A$ для некоторого $A \in \mathcal{F}$ (а стало быть, в одной и той же совокупности $\mathcal{G}_A$), то пересекаются они более чем по t элементам.

Пусть теперь $U \in \mathcal{U}_A$, $V \in \mathcal{U}_B$, где $A, B \in \mathcal{F}$, $A \neq B$. Понятно, что

$$|(U \cap V) \cap (\{1, \dots, n\} \setminus F)| < k - t - r - l,$$

так как любое множество из совокупности $\mathcal{U}$ пересекается с $\{1, \dots, n\} \setminus F$ ровно по $k - t - r - l - 1$ элементам.

Оценим $|(U \cap V) \cap F|$. По построению внутри $A \cap B$ множества U и V имеют менее t_1 общих элементов (этим условием заданы совокупности $\mathcal{S}_A$ и $\mathcal{S}_B$, кроме того, $\mathcal{U}_A \subset \mathcal{S}_A$, $\mathcal{U}_B \subset \mathcal{S}_B$). Далее, внутри $\bar{A} \cap B$ множества U и V имеют не более x общих элементов по построению совокупности $\mathcal{U}_A$. Наконец, имеет место неравенство $|(U \cap V) \cap \bar{B}| \leq l$, поскольку $|V \cap \bar{B}| = l$.

В итоге

$$|U \cap V| < (k - t - r - l) + t_1 + x + l = t.$$

Этап 4. Остается доказать, что размер построенной совокупности $\mathcal{U}$ дает необходимую оценку. На этапе 3 мы, в частности, показали, что для разных $A, B \in \mathcal{F}$ совокупности $\mathcal{U}_A, \mathcal{U}_B$ не пересекаются. Поэтому

$$|\mathcal{U}| = \sum_{A \in \mathcal{F}} |\mathcal{U}_A| = \sum_{A \in \mathcal{F}} (|\mathcal{G}_A| - |\mathcal{G}_A \setminus \mathcal{S}_A| - |\mathcal{S}_A \setminus \mathcal{U}_A|).$$

Ясно, что

$$|\mathcal{G}_A| = C_{n-f}^{k-t-r-l-1} C_{t+2r}^{t+r+1} C_{f-t-2r}^l.$$

Оценим величину $|\mathcal{G}_A \setminus \mathcal{S}_A|$ для каждого множества $A \in \mathcal{F}$. Совокупность $\mathcal{G}_A \setminus \mathcal{S}_A$ состоит из тех множеств V , для которых существует такое множество $B \in \mathcal{F}$, что $|V \cap (A \cap B)| \geq t_1$. Зафиксируем $B \in \mathcal{F}$. Пусть $|A \cap B| = i$, где $t_1 \leq i < s$. Тогда число множеств, имеющих с $A \cap B$ не менее t_1 общих элементов, вычисляется как

$$C_{n-f}^{k-t-r-l-1} C_{f-t-2r}^l \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1}.$$

Значит, верна следующая оценка:

$$|\mathcal{G}_A \setminus \mathcal{S}_A| \leq |\mathcal{F}| \cdot C_{n-f}^{k-t-r-l-1} C_{f-t-2r}^l \cdot \max_{t_1 \leq i < s} \sum_{j=t_1}^i C_i^j C_{t+2r-i}^{t+r-j+1} = C_{n-f}^{k-t-r-l-1} C_1.$$

Аналогичным образом оценивается величина $|\mathcal{S}_A \setminus \mathcal{U}_A|$. Вновь зафиксируем множества $A, B \in \mathcal{F}$, и пусть $|A \cap B| = i$, где $0 \leq i < s$. Количество множеств из совокупности $\mathcal{S}_A$, пересекающихся с $\bar{A} \cap B$ более, чем по x элементам, не превышает величины

$$C_{t+2r}^{t+r+1} \sum_{j=x+1}^l C_{t+2r-i}^j C_{f-2t-4r+i}^{l-j}.$$

В самом деле, выбрать j элементов в множестве $\bar{A} \cap B$ можно C_{t+2r-i}^j способами, выбрать $l-j$ элементов в множестве $\bar{A} \cap \bar{B}$ можно $C_{f-2t-4r+i}^{l-j}$ способами и, наконец, для выбора $t+r+1$ элементов в множестве A есть ровно C_{t+2r}^{t+r+1} возможностей. Так же, как в предыдущем случае, мы получаем оценку

$$\begin{aligned} |\mathcal{S}_A \setminus \mathcal{U}_A| &\leq |\mathcal{F}| \cdot C_{n-f}^{k-t-r-l-1} C_{t+2r}^{t+r+1} \cdot \max_{0 \leq i < s} \sum_{j=x+1}^l C_{t+2r-i}^j C_{f-2t-4r+i}^{l-j} \\ &= C_{n-f}^{k-t-r-l-1} C_2. \end{aligned}$$

В итоге

$$|\mathcal{U}| \geq |\mathcal{F}| \cdot C_{n-f}^{k-t-r-l-1} \cdot (C_{t+2r}^{t+r+1} C_{f-t-2r}^l - C_1 - C_2).$$

Теорема 7 доказана.

ЗАМЕЧАНИЕ 1. Задача отыскания величины $m(n, k, t)$ равносильна задаче о величине $m(n, n - k, n - 2k + t)$. В самом деле, если $|A \cap B| = t$, то дополнения множеств A, B , имеющие мощности $n - k$, пересекаются по $n - 2k + t$ элементам. Это, очевидно, позволяет еще усилить теорему 7 (и реально усиливает).

Поскольку в теореме 7 много разных параметров, вычисления оптимальных оценок, вытекающих из теоремы 7 и замечания 1, весьма затратны. Для ускорения процедуры построения графиков была предпринята попытка отыскания явной формулы для оптимального значения параметра f . При этом все параметры представлялись в нашем стандартном асимптотическом виде как функции вида $\sim c' \cdot n$, $n \rightarrow \infty$. Например, $f \sim f'n$. Итоговая оценка записывалась в форме $(c(k', t', f', l', r', s', x') + o(1))^n$. Производная функции $c(k', t', f', l', r', s', x')$ по f' приравнивалась к нулю, и с помощью ресурса Wolfram Mathematica была найдена формула (которая, кстати, свидетельствует о том, что в данном случае уравнение на производную преобразовывается к квадратному)

$$f'_{\text{opt}} = \frac{-B - \sqrt{B^2 - 4AC}}{2A},$$

где

$$\begin{aligned} A &= k' - r' + s' - t', \\ B &= -(l' + 4k'r' - 2l'r' + s'(1 - k' + l' + r') + t'(2k' - l' - 2r' + s' - t')), \\ C &= (2r' + t')(l' + 2r' + t'). \end{aligned}$$

Разумеется, это лишь необходимое условие экстремума, и граница области оптимизации очень сложна, но численные эксперименты показали, что если подставлять в функцию $c(k', t', f', l', r', s', x')$ величину f'_{opt} вместо f' , то оценка получается не хуже (надо лишь заменять f'_{opt} единицей, если $f'_{\text{opt}} > 1$). К сожалению, для остальных параметров не удалось получить столь простых формул, и оптимальные значения x' и l' , приводимые ниже, – результат численной максимизации. Так или иначе, наша цель – получение нижних границ, и на рисунках, которые мы приведем в следующем параграфе, будет показано, насколько границы из теоремы 7 вкупе с замечанием 1 сильнее всех своих частных случаев.

В то же время не может не возникнуть вопрос: а необходимо ли такое количество параметров в теореме? Возможно, оптимум достигается при каких-то простейших ситуациях? Например, даже имея формулу для f'_{opt} , можно допустить, что на самом деле почти всегда $f'_{\text{opt}} = 1$. Также для l' есть тривиальный случай, когда $l' = k' - t' - r'$, и вполне можно рассмотреть лишь случай $x' = l'$. Конечно, сам факт превосходства теоремы 7 над частными случаями свидетельствует о том, что какие-то из параметров точногодились, но вот какие? На рис. 13–15 мы покажем, что все параметры важны. На всех рисунках $k' = 0.1$. На рис. 13 видно, что далеко не всегда $f'_{\text{opt}} = 1$ и что отличие оптимального параметра от единицы весьма значительно. На рис. 14 то же самое продемонстрировано относительно l' . Наконец, рис. 15 говорит о том, что выбор нетривиального x' существен на очень широком диапазоне значений t' . Некоторое колебание графиков на этих рисунках связано с недостаточной точностью вычислений при численной оптимизации.

Рис. 13. Сравнение оптимального значения параметра f' с единицей при $k' = 0.1$

Рис. 14. Сравнение оптимального значения параметра l' с $k' - t' - r'$ при $k' = 0.1$

Рис. 15. Сравнение оптимального значения параметра x' с l' при $k' = 0.1$

С другой стороны, есть ряд дополнительных соображений, в силу которых можно было бы даже увеличить количество параметров. Например, мы фиксируем множество $F = \{1, \dots, f\}$ и дальше строим все множества будущей совокупности, полагая мощности их пересечения с F равными $t + r + l + 1$. Во-первых, можно попытаться рассмотреть несколько таких конструкций (с разными $F \subset \{1, \dots, n\}$, имеющими мощность f), стараясь следить за тем, чтобы k -элементные множества из разных конструкций достаточно мало пересекались. Во-вторых, можно даже в одной конструкции аккуратнее поработать с кусочками k -элементных множеств, которые расположены в множестве $\{1, \dots, n\} \setminus F$ и имеют мощности $k - t - r - l - 1$. Сейчас мы тривиально оцениваем мощности пересечения этих кусочков величиной $k - t - r - l - 1$, но можно было бы попытаться и тут добиться уточнений. В-третьих, возможно и некоторое третье “выкидывание”. Однако наши численные эксперименты показали, что все эти идеи реальных улучшений оценки не дают. Именно поэтому мы оставили в формулировке теоремы 7 те и только те параметры, которые действительно сработали.

В свете всего сказанного замечательно то, что есть еще одна, совсем по-иному устроенная, конструкция, которая, удивительным образом на очень маленьких областях изменения параметров (k', t') дает границу, слегка превосходящую границу из теоремы 7 и замечания 1. Эту конструкцию мы опишем в следующем параграфе, где мы также приведем рисунки как с ее участием, так и с участием оценки из теоремы 7 и замечания 1.

3.6. Использование четных мощностей пересечения. Справедлива совсем простая

ТЕОРЕМА 8. *Имеют место два случая.*

1. Пусть n, k – четные натуральные числа, а t – нечетное число. Тогда

$$m(n, k, t) \geq C_{n/2}^{k/2}.$$

2. Если же n, k – нечетные натуральные числа, а t – четное число, то

$$m(n, k, t) \geq C_{(n-1)/2}^{(k-1)/2}.$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим случаи по отдельности. 1. Рассмотрим пары $\{1, 2\}, \{3, 4\}, \dots, \{n-1, n\}$. Ясно, что, выбрав любые $k/2$ пар из этого набора, мы получим множество мощности k . Число способов такого выбора есть, очевидно, $C_{n/2}^{k/2}$. Легко понять, что любые два множества из полученной совокупности могут пересекаться лишь по четному числу элементов. Поскольку запрещенное t – число нечетное, мы получаем необходимую оценку величины $m(n, k, t)$.

2. Рассмотрим пары $\{1, 2\}, \{3, 4\}, \dots, \{n-2, n-1\}$. Множества мощности k образуем как объединение некоторого набора из $(k-1)/2$ таких пар и элемента n . Понятно, что все множества имеют теперь нечетное число общих элементов, а значит, два множества никогда не пересекаются по t элементам.

Теорема доказана.

Приведем два стандартных рисунка. На рис. 16 изображен случай $k' = 0.5$, на рис. 17 – случай $k' = 0.1$. На них добавлены графики, полученные как результат теоремы 7 и замечания 1 (эти графики обозначены Parametric Family),

Рис. 16. Сравнение оценок из теорем 3–8 и оценки из теоремы 2 при $k' = 0.5$: ---- AKh; VG; ----- Glue; -.-.-.- Super Glue; — Upper; — Pairs; Parametric Family

Рис. 17. Сравнение оценок из теорем 3–8 и оценки из теоремы 2 при $k' = 0.1$: ---- AKh; VG; ----- Glue; -.-.-.- Super Glue; — Upper; — Pairs; Parametric Family

а также график оценки из теоремы 8 (он обозначен Pairs). Видно, что почти везде теорема 7 и замечание 1 превосходят все остальные результаты. Но есть крошечные участки, где лучше работает весьма специфичная теорема 8 (один из них в большем масштабе изображен на рис. 18), и это показывает, что скорее всего оптимальные границы находятся где-то еще выше. Некоторые неровности на графике теоремы 7 и замечания 1 связаны с недостаточной точностью вычислений.

Рис. 18. Сравнение оценок из теорем 3–8 и оценки из теоремы 2 при $k' = 0.5$ для $0.4 \leq t' \leq 0.44$: ---- AKh; VG; ----- Glue; Super Glue; — Upper; — Pairs; Parametric Family

§ 4. О верхних границах для равновесных кодов, исправляющих ошибки

В п. 3.2 мы уже говорили о нижней границе Варшавова–Гилберта для равновесных кодов, исправляющих ошибки. Там мы ввели обозначение $h(n, k, t)$. В терминах теории кодирования это наибольшее количество кодовых слов веса k , у которых попарные хэмминговы расстояния не меньше чем $2(k - t)$. В теории кодирования гораздо чаще используют обозначение $A(n, 2\delta, \omega)$: это максимальное число кодовых слов веса ω с попарными хэмминговыми расстояниями, не меньшими 2δ (см. [1]). Таким образом, $h(n, k, t) = A(n, 2(k - t), k)$.

В п. 3.3 мы осуществили “склейку”, а именно при данных n, k, t взяли произвольное число r из промежутка от 0 до $k - t$ и с помощью нижней границы Варшавова–Гилберта (теорема 4) нашли много $(t + 2r)$ -элементных множеств, у которых мощности взаимных пересечений не превосходят $t_1 = 3t + 2r - 2k$. Потом мы с каждым таким множеством связали

$$y = \sum_{i=r+1}^{\min\{2r, k-t\}} C_{t+2r}^{t+i} C_{n-t-2r}^{k-t-i}$$

k -элементных множеств, получив в итоге совокупность, мощность которой равна произведению границы Варшавова–Гилберта и числа y .

Представим себе, что граница Варшавова–Гилберта допускает усиление, скажем, до какой-то величины z . Ясно, однако, что произведение zy никак не может превзойти границы из теорем 1 и 2. Если попытаться оценить таким образом величину $A(n, 2\delta, \omega)$ сверху, то, очевидно, нужно положить $t + 2r = \omega$, $t_1 = \omega - \delta$. В итоге получается следующая теорема.

ТЕОРЕМА 9. Пусть даны числа ω и δ . Пусть, далее, k, t, r, t_1 – натуральные числа, удовлетворяющие соотношениям

$$\frac{\delta}{2} < k < \omega + \frac{\delta}{2}, \quad t = k - \frac{\delta}{2}, \quad r = \frac{\omega + \delta/2 - k}{2}, \\ 1 \leq r \leq k - t, \quad t_1 = 3t + 2r - 2k, \quad 2(t + 2r) - t_1 \leq n.$$

Выберем числа d, ρ : если $2t < k$, то положим $d = \rho = 0$; в противном случае

$$d = 2t - k + 1, \quad (k - d + 1) \left(2 + \frac{d - 1}{\rho + 1} \right) \leq n < (k - d + 1) \left(2 + \frac{d - 1}{\rho} \right).$$

Пусть, наконец, $k - t$ – степень простого числа.

Тогда выполнено неравенство

$$A(n, 2\delta, \omega) \leq \frac{C_n^{d+2\rho}}{C_k^{d+\rho} C_{n-k}^\rho} \left(\sum_{i=0}^{k-t-1} C_n^i \right) \cdot \frac{1}{\sum_{i=r+1}^{\min(2r, k-t)} C_{t+2r}^{t+i} C_{n-t-2r}^{k-t-i}}.$$

Выбор чисел d, ρ в теореме 9 связан с тем, какую из границ мы хотим применять – доказанную в теореме 1 или полученную в теореме 2. Оказалось, что оптимальный выбор всегда остается за теоремой 2, но это численный результат, и потому мы не посчитали правильным удалять из формулировки теоремы соответствующую альтернативу.

Видно, что теорема 9 работает не всегда, так как требуется условие “ $k - t$ – степень простого числа”. Однако она дает довольно сильный результат. Для того чтобы в этом убедиться, вспомним наилучшие известные границы для величины $A(n, 2\delta, \omega)$ в асимптотическом случае. Это границы Хэмминга (см. [1], [27] и теорему 10 ниже), границы Левенштейна (см. [24] и теорему 11 ниже) и границы линейного программирования, доказанные Мак-Элисом, Родемичем, Рамсеем и Велчем (см. [1], [28] и теорему 12 ниже). Известные границы Элайеса–Бассальяго (см. [1], [29]) мы не приводим, так как в случае равновесных кодов они доминируются остальными перечисленными границами.

ТЕОРЕМА 10. Имеет место неравенство

$$A(n, 2\delta, \omega) \leq \frac{C_n^\omega}{\sum_{i=0}^{\delta/2} C_{\omega-i}^{\omega-i} C_{n-\omega}^i}.$$

ТЕОРЕМА 11. Пусть r и j – такие целые числа, что число $t = (r - j)/2$ целое. Тогда если

$$0 \leq r - j \leq 2(n - \omega), \quad 0 \leq r + j \leq 2\omega, \quad \frac{(r - j)^2}{4(\omega - j)} + \frac{(r + j)^2}{4(n - \omega + j)} + \delta - r > 0,$$

то выполнено неравенство

$$A(n, 2\delta, \omega) \leq \frac{C_n^{\omega-j}}{C_{\omega^{(r+j)/2}}^{(r+j)/2} C_{n-\omega}^{(r-j)/2}} \left[\frac{\delta}{\frac{(r-j)^2}{4(\omega-j)} + \frac{(r+j)^2}{4(n-\omega+j)} + \delta - r} \right].$$

ТЕОРЕМА 12. При $0 \leq \delta \leq \omega \leq 1/2$ положим

$$R(\delta, \omega) = \lim_{n \rightarrow \infty} \frac{1}{n} \log_2 A(n, \delta n, \omega n)$$

и введем функции

$$H_2(x) = -x \log_2 x - (1-x) \log_2(1-x), \quad g(x) = H_2\left(\frac{1 - \sqrt{1-x}}{2}\right).$$

Тогда при $\delta^* \leq \omega$ имеем

$$R(\delta, \omega) \leq g(u^2),$$

где

$$\delta^* = \frac{1 - \sqrt{1 - 2\delta}}{2}, \quad u = -\delta + \sqrt{\delta^2 - 2\delta + 4\omega(1 - \omega)}.$$

На рис. 19 и рис. 20 показаны оценки из теорем 9–12 (здесь использованы обозначения: теорема 9 – New bound, теорема 10 – Hamming, теорема 11 – Levenstein, теорема 12 – LP). Видно, что граница Левенштейна (теорема 11)

Рис. 19. Оценки из теорем 9–12 при $\omega = 0.05n$: — New bound; ---- Hamming; Levenstein; -.-.- LP

Рис. 20. Оценки из теорем 9–12 при $\omega = 0.2n$: — New bound; ---- Hamming; Levenstein; -.-.- LP

слегка уточняет теорему 9, но есть значительные участки, на которых теорема 9 лучше границы линейного программирования (теорема 12).

ЗАМЕЧАНИЕ 2. Может возникнуть вопрос: почему мы не использовали более сложную склейку из теоремы 7, в которой эта склейка содержит два дополнительных параметра f, l (“выкидывание” не в счет)? Дело в том, что численные эксперименты показали, что оптимум всегда достигается при $f = n$. Поэтому мы не стали делать формулировку и без того громоздкой теоремы 9 еще более нагруженной параметрами.

§ 5. Несколько слов о проблеме Нельсона–Хадвигера

Одна из классических проблем комбинаторной геометрии – проблема Нельсона–Хадвигера – была поставлена Нельсоном в 1950 г. (Хадвигер занимался близкой проблемой в 1944 г.; см. [30]). Состоит она в отыскании величины $\chi(\mathbb{R}^n)$, называемой *хроматическим числом пространства* и равной наименьшему количеству цветов, в которые можно так покрасить все точки $\mathbb{R}^n$, чтобы между точками одного цвета не было евклидова расстояния 1.

Напомним также, что *хроматическое число графа* $G = (V, E)$ – это наименьшее число $\chi(G)$ цветов, в которые можно так покрасить все вершины графа, чтобы между вершинами одного цвета не было ребра. Ясно, что $\chi(\mathbb{R}^n) \geq \chi(G(n, k, t))$ (см. § 1). Более того, сейчас известно, что

$$(1.239 \dots + o(1))^n \leq \chi(\mathbb{R}^n) \leq (3 + o(1))^n$$

(нижняя оценка получена в [31], верхняя – в [32]), а чуть более слабая оценка $\chi(\mathbb{R}^n) \geq (1.207 \dots + o(1))^n$ доказана в той самой работе [15], которая послужила отправной точкой для текущего исследования. Эта более слабая оценка сделана за счет оптимизации неравенства $\chi(\mathbb{R}^n) \geq \chi(G(n, k, t))$ по t и k . Таким образом, задача отыскания хроматических чисел графов $G(n, k, t)$ исключительно важна для комбинаторной геометрии.

Хорошо известно, что для любого графа G выполнено $\chi(G) \geq |V|/\alpha(G)$ (это практически очевидно) и что для транзитивных графов $\chi(G) \leq c \frac{|V|}{\alpha(G)} \ln |V|$ (см. [33]). Для графов $G(n, k, t)$, которые транзитивны, это означает, что в асимптотическом случае задача сводится к отысканию такого числа $a(k', t')$, что

$$\frac{C_n^k}{\alpha(G(n, k, t))} = (a(k', t') + o(1))^n.$$

В итоге вопрос лишь в нашей стандартной асимптотической записи для числа независимости, которое и есть $m(n, k, t)$, подробно изученное нами выше. Если $2t < k$, то с учетом результата § 2 мы знаем величину $a(k', t')$. В противном случае мы получаем новые верхние оценки этой величины. Отметим, что при $2t < k$ есть чуть более аккуратные оценки для функций $o(1)$ в основаниях экспонент, которые являются частными случаями существенно более трудных границ для графов с вершинами в точках целочисленной решетки (см. [34]–[38]). При $2t \geq k$ нынешнее исследование первое.

Список литературы

- [1] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, *Теория кодов, исправляющих ошибки*, Части I, II, Связь, М., 1979, 744 с.; пер. с англ.: F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, Parts I, II, North-Holland Math. Library, **16**, North-Holland, Amsterdam–New York–Oxford, 1977, xv+ix+762 pp.
- [2] L. Bassalygo, G. Cohen, G. Zémor, “Codes with forbidden distances”, *Discrete Math.*, **213**:1-3 (2000), 3–11.
- [3] V. G. Boltyanski, H. Martini, P. S. Soltan, *Excursions into combinatorial geometry*, Universitext, Springer-Verlag, Berlin, 1997, xiv+418 pp.
- [4] А. М. Райгородский, “Three lectures on the Borsuk partition problem”, *Surveys in contemporary mathematics*, London Math. Soc. Lecture Note Ser., **347**, Cambridge Univ. Press, Cambridge, 2008, 202–247.
- [5] А. М. Райгородский, “Вокруг гипотезы Борсука”, *СМФН*, **23**, РУДН, М., 2007, 147–164; англ. пер.: А. М. Raigorodskii, “Around Borsuk’s hypothesis”, *J. Math. Sci. (N. Y.)*, **154**:4 (2008), 604–623.
- [6] А. М. Raigorodskii, “Cliques and cycles in distance graphs and graphs of diameters”, *Discrete geometry and algebraic combinatorics*, Contemp. Math., **625**, Amer. Math. Soc., Providence, RI, 2014, 93–109.
- [7] А. М. Raigorodskii, “Coloring distance graphs and graphs of diameters”, *Thirty essays on geometric graph theory*, Springer-Verlag, New York, 2013, 429–460.
- [8] А. М. Райгородский, “Проблема Борсука и хроматические числа некоторых метрических пространств”, *УМН*, **56**:1(337) (2001), 107–146; англ. пер.: А. М. Raigorodskii, “Borsuk’s problem and the chromatic numbers of some metric spaces”, *Russian Math. Surveys*, **56**:1 (2001), 103–139.
- [9] А. М. Райгородский, “О хроматических числах сфер в евклидовых пространствах”, *Докл. РАН*, **432**:2 (2010), 174–177; англ. пер.: А. М. Raigorodskii, “On the chromatic numbers of spheres in Euclidean spaces”, *Dokl. Math.*, **81**:3 (2010), 379–382.
- [10] А. М. Raigorodskii, “On the chromatic numbers of spheres in $\mathbb{R}^n$ ”, *Combinatorica*, **32**:1 (2012), 111–123.
- [11] P. K. Agarwal, J. Pach, *Combinatorial geometry*, Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1995, xiv+354 pp.
- [12] L. A. Székely, “Erdős on unit distances and the Szemerédi–Trotter theorems”, *Paul Erdős and his mathematics*, v. II (Budapest, 1999), Bolyai Soc. Math. Stud., **11**, János Bolyai Math. Soc., Budapest, 2002, 649–666.
- [13] A. Soifer, *The mathematical coloring book. Mathematics of coloring and the colorful life of its creators*, Springer-Verlag, New York, 2009, xxx+607 pp.
- [14] V. Klee, S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, Dolciani Math. Exp., **11**, Math. Assoc. America, Washington, DC, 1991, xvi+333 pp.
- [15] P. Frankl, R. M. Wilson, “Intersection theorems with geometric consequences”, *Combinatorica*, **1**:4 (1981), 357–368.
- [16] А. В. Бобу, О. А. Костина, А. Э. Куприянов, “Числа независимости и хроматические числа некоторых дистанционных графов”, *Пробл. передачи информ.*, **51**:2 (2015), 86–98; англ. пер.: A. V. Bobu, O. A. Kostina, A. E. Kupriyanov, “Independence numbers and chromatic numbers of some distance graphs”, *Problems Inform. Transmission*, **51**:2 (2015), 165–176.
- [17] Е. И. Пономаренко, А. М. Райгородский, “Улучшение теоремы Франкла–Уилсона о числе ребер гиперграфа с запретами на пересечения”, *Докл. РАН*, **454**:3 (2014), 268–269; англ. пер.: E. I. Ponomarenko, A. M. Raigorodskii, “An improvement of

- the Frankl–Wilson theorem on the number of edges in a hypergraph with forbidden intersections of edges”, *Dokl. Math.*, **89**:1 (2014), 59–60.
- [18] Е. И. Пономаренко, А. М. Райгородский, “Новые оценки в задаче о числе ребер гиперграфа с запретами на пересечения”, *Пробл. передачи информ.*, **49**:4 (2013), 98–104; англ. пер.: Е. I. Ponomarenko, A. M. Raigorodskii, “New estimates in the problem of the number of edges in a hypergraph with forbidden intersections”, *Problems Inform. Transmission*, **49**:4 (2013), 384–390.
 - [19] R. Ahlswede, L. H. Khachatrian, “The complete nontrivial-intersection theorem for systems of finite sets”, *J. Combin. Theory Ser. A*, **76**:1 (1996), 121–138.
 - [20] R. Ahlswede, L. H. Khachatrian, “The complete intersection theorem for systems of finite sets”, *European J. Combin.*, **18**:2 (1997), 125–136.
 - [21] R. Ahlswede, V. Blinovsky, *Lectures on advances in combinatorics*, Universitext, Springer-Verlag, Berlin, 2008, xiv+314 pp.
 - [22] Р. Р. Варшамов, “Оценка числа сигналов в кодах с коррекцией ошибок”, *Докл. АН СССР*, **117**:5 (1957), 739–741.
 - [23] E. N. Gilbert, “A comparison of signalling alphabets”, *Bell Syst. Tech. J.*, **31**:3 (1952), 504–522.
 - [24] В. И. Левенштейн, “О верхних оценках для кодов с фиксированным весом векторов”, *Пробл. передачи информ.*, **7**:4 (1971), 3–12; англ. пер.: V. I. Levenshtein, “Upper-bound estimates for fixed-weight codes”, *Problems Inform. Transmission*, **7**:4 (1971), 281–287.
 - [25] В. А. Зиновьев, Т. Эрикссон, “О каскадных равновесных кодах, превышающих границу Варшамова–Гилберта”, *Пробл. передачи информ.*, **23**:1 (1987), 110–111; англ. пер.: V. A. Zinov’ev, T. Ericson, “On concatenated constant-weight codes beyond the Varshamov–Gilbert bound”, *Problems Inform. Transmission*, **23**:1 (1987), 110–111.
 - [26] V. Rödl, “On a packing and covering problem”, *European J. Combin.*, **6**:1 (1985), 69–78.
 - [27] R. W. Hamming, “Error detecting and error correcting codes”, *Bell System Tech. J.*, **29**:2 (1950), 147–160.
 - [28] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., L. R. Welch, “New upper bounds on the rate of a code via the Delsarte–MacWilliams inequalities”, *IEEE Trans. Information Theory*, **23**:2 (1977), 157–166.
 - [29] Л. А. Бассальго, “Новые верхние границы для кодов, исправляющих ошибки”, *Пробл. передачи информ.*, **1**:4 (1965), 41–44; англ. пер.: L. A. Bassalygo, “New upper bounds for error correcting codes”, *Problems Inform. Transmission*, **1**:4 (1965), 32–35.
 - [30] H. Hadwiger, “Ein Überdeckungssatz für den Euklidischen Raum”, *Portugaliae Math.*, **4** (1944), 140–144.
 - [31] А. М. Райгородский, “О хроматическом числе пространства”, *УМН*, **55**:2(332) (2000), 147–148; англ. пер.: A. M. Raigorodskii, “On the chromatic number of a space”, *Russian Math. Surveys*, **55**:2 (2000), 351–352.
 - [32] D. G. Larman, C. A. Rogers, “The realization of distances within sets in Euclidean space”, *Mathematika*, **19** (1972), 1–24.
 - [33] R. L. Graham, B. L. Rothschild, J. H. Spencer, *Ramsey theory*, 2nd ed., Wiley-Intersci. Ser. Discrete Math. Optim., Wiley, New York, 1990, xii+196 pp.
 - [34] А. М. Райгородский, “Проблема Борсука для $(0, 1)$ -многогранников и кросс-политопов”, *Докл. РАН*, **371**:5 (2000), 600–603; англ. пер.: A. M. Raigorodskii, “The Borsuk problem for $(0, 1)$ -polyhedra and cross polytopes”, *Dokl. Math.*, **61** (2000), 256–259.

- [35] А. М. Райгородский, “Проблема Борсука для $(0, 1)$ -многогранников и кросс-политопов”, *Докл. РАН*, **384**:5 (2002), 593–597; англ. пер.: А. М. Raigorodskii, “Borsuk’s problem for $(0, 1)$ -polytopes and cross-polytopes”, *Dokl. Math.*, **65**:3 (2002), 413–416.
- [36] А. М. Райгородский, “Проблема Борсука для целочисленных многогранников”, *Матем. сб.*, **193**:10 (2002), 139–160; англ. пер.: А. М. Raigorodskii, “The Borsuk problem for integral polytopes”, *Sb. Math.*, **193**:10 (2002), 1535–1556.
- [37] А. М. Райгородский, “Проблемы Борсука, Хадвигера и Грюнбаума для некоторых классов многогранников и графов”, *Докл. РАН*, **388**:6 (2003), 738–742; англ. пер.: А. М. Raigorodskii, “The problem of Borsuk, Hadwiger, and Grünbaum for some classes of polytopes and graphs”, *Dokl. Math.*, **67**:1 (2003), 85–89.
- [38] А. М. Райгородский, “Проблемы Борсука и Грюнбаума для решетчатых многогранников”, *Изв. РАН. Сер. матем.*, **69**:3 (2005), 81–108; англ. пер.: А. М. Raigorodskii, “The problems of Borsuk and Grünbaum on lattice polytopes”, *Izv. Math.*, **69**:3 (2005), 513–537.

Андрей Викторович Бобу
(**Andrei V. Bobu**)

Механико-математический факультет,
Московский государственный университет
имени М.В.Ломоносова
E-mail: a.v.bobu@gmail.com

Поступила в редакцию
12.01.2015 и 18.01.2016

Александр Эдуардович Куприянов
(**Aleksandr E. Kupriyanov**)

Механико-математический факультет,
Московский государственный университет
имени М.В.Ломоносова
E-mail: yashik-cuso4a@yandex.ru

Андрей Михайлович Райгородский
(**Andrei M. Raigorodskii**)

Механико-математический факультет,
Московский государственный университет
имени М.В.Ломоносова;
Факультет инноваций и высоких технологий,
Московский физико-технический институт
(государственный университет),
г. Долгопрудный Московской обл.;
Институт математики и информатики,
Бурятский государственный университет,
г. Улан-Удэ
E-mail: mraigor@yandex.ru