УДК 519.174
DOI: 10.53815/20726759_2021_13_3_29

А. В. Бердников

Московский физико-технический институт (национальный исследовательский университет)

Числа Борсука множеств специального вида на сферах малого радиуса

В 1933 году К. Борсук сформулировал классическую гипотезу о том, что любое множество диаметра 1 в d-мерном евклидовом пространстве может быть разбито на $d+1$ частей меньшего диаметра. В 1993 году гипотеза Борсука была опровергнута. Более того, в 2012 году было доказано, что контрпримеры к гипотезе могут быть найдены на сферах любого радиуса больше $1/2$. В данной статье с помощью $(-1,1)$-векторов и $(-1,0,1)$-векторов строятся новые контрпримеры на сферах малого радиуса в $\mathbb{R}^d$.

Ключевые слова: проблема Борсука, разбиения, $(-1,1)$-векторы, $(-1,0,1)$-векторы, дистанционные графы, графы диаметров, раскраски.

A. V. Berdnikov

Moscow Institute of Physics and Technology

Borsuk number of special sets on spheres of small radii

In 1933 K. Borsuk stated his classical conjecture that any set of diameter 1 in the d-dimensional Euclidean space can be divided into $d+1$ parts of smaller diameters. In 1993 Borsuk's conjecture was disproved. Moreover, in 2012 it was proved that counterexamples to the conjecture can be found on spheres of any radii greater than $1/2$. In this paper we build using $(-1,1)$-vectors and $(-1,0,1)$-vectors new counterexamples to Borsuk's conjecture on spheres of small radii in $\mathbb{R}^d$.

Key words: Borsuk's problem, partitions, $(-1,1)$-vectors, $(-1,0,1)$-vectors, distance graphs, diameter graphs, colourings.

1. Введение

В данной статье будут доказаны результаты, тесно связанные с классической задачей Борсука о разбиении множества на части меньшего диаметра. Напомним, что для евклидова d-мерного пространства $\mathbb{R}^d$ *числом Борсука* называется наименьшее такое $f(d)$, что любое множество точек диаметра 1 в $\mathbb{R}^d$ возможно разбить на $f(d)$ частей меньшего диаметра. Очевидно, что $f(1)=2$. В 30-х годах прошлого века К. Борсук доказал, что $f(d)$ всегда больше d, причем $f(2)=3$, и выдвинул гипотезу, что $f(d)=d+1$ для всех размерностей d [1]. В 1993 году гипотеза Борсука была опровергнута Дж. Каном и Г. Калаи [2], и в настоящее время известно, что, хотя гипотеза верна для $d \leqslant 3$, $f(64)$ уже строго больше 65 (см. [3]). Кроме того, асимптотический рост величины $f(d)$ быстрее, чем линейный:

$$\left(\left(\frac{2}{\sqrt{3}}\right)^{\sqrt{2}}+o(1)\right)^{\sqrt{d}} \leqslant f(d) \leqslant \left(\sqrt{\frac{3}{2}}+o(1)\right)^{d} \tag{1}$$

(нижняя оценка принадлежит А. М. Райгородскому [4], верхняя — О. Шрамму [5]). В данной работе нас будут интересовать асимптотические нижние оценки $f(d)$ при $d \to \infty$.

Напомним, что *дистанционным графом*, или *графом расстояний*, в пространстве $\mathbb{R}^d$ называется такой граф $G = (V, E)$, вершины которого лежат в данном пространстве (т. е. $V \subset \mathbb{R}^d$), а ребра соединяют те и только те пары вершин, расстояние между которыми равно некоторому наперед заданному числу (будем называть его *запрещенным расстоянием*). Частным случаем дистанционного графа является *граф диаметров* — такой граф $G = (\Omega, E)$, что $\Omega \subset \mathbb{R}^d$ и ребрами являются все пары вершин, расстояние между которыми равно диаметру множества $\operatorname{diam}\Omega$ (мы будем рассматривать только случаи, когда Ω конечно). Ясно, что разбиение множества Ω на f частей равносильно правильной раскраске графа диаметров G в f цветов, то есть раскраске вершин графа таким образом, что каждое ребро будет соединять вершины разного цвета. Напомним, что наименьшее возможное число цветов в правильной раскраске графа G называется его *хроматическим числом* и обозначается $\chi(G)$. Таким образом, хроматическое число любого графа диаметров в $\mathbb{R}^d$ является нижней оценкой числа Борсука $f(d)$.

Нижняя оценка в (1) получается следующим образом. Рассматривается дистанционный граф G в пространстве $\mathbb{R}^n$, вершины которого являются $(-1, 0, 1)$-векторами, причем фиксированная доля всех координат равна -1, столько же координат равны 1, а остальные координаты равны 0. Этот граф оказывается изоморфен некоторому графу диаметров H (с диаметром 1) в пространстве $\mathbb{R}^d$, где $d = n(n+1)/2$. Далее оценивается снизу хроматическоое число графа G:

$$\chi(G) \geqslant \left(\frac{2}{\sqrt{3}} + o(1)\right)^n,$$

и это даёт нужную оценку, поскольку $f(d) \geqslant \chi(H) = \chi(G)$ и $n \sim \sqrt{2d}$.

В статье [6] доказывается, что целый класс таких конструкций может давать подобные контрпримеры к гипотезе Борсука. А именно, можно расматривать $(-1, 0, 1)$-векторы в $\mathbb{R}^n$, у которых некоторая фиксированная доля координат равна -1 и некоторая другая фиксированная доля координат равна 1. При правильном выборе запрещенного расстояния можно построить на этих вершинах дистанционный граф G с экспоненциально растущим хроматическим числом (при $n \to \infty$), изоморфный некоторому графу диаметров с диаметром 1 в пространстве размерности $d = n(n+1)/2$. Каждая такая конструкция дает нижнюю оценку $f(d) \geqslant (c + o(1))^{\sqrt{d}}$, хотя это и не позволяет превзойти результат (1).

У всех упомянутых выше конструкций есть общая черта: множество вершин построенного графа единичных диаметров в пространстве $\mathbb{R}^d$ всегда лежит на сфере, радиус которой асимптотически равен $1/\sqrt{2}$. Интуитивно это кажется естественным, ведь любое множество диаметра 1 в пространстве $\mathbb{R}^d$ можно накрыть шаром радиуса $\sqrt{d/(2d+2)} \sim 1/\sqrt{2}$, и для построения контрпримера к гипотезе Борсука хочется взять множество с как можно большим накрывающим шаром. Однако в 2012 году А. М. Райгородский и А. Б. Купавский доказали [7], что для любого наперед заданного $r \in (1/2, 1/\sqrt{2})$ на сфере радиуса r в $\mathbb{R}^d$ существует множество диаметра 1, дающее контрпример к гипотезе Борсука.

Райгородский и Купавский для доказательства указанного выше результата использовали $(-1, 1)$-векторы с равным числом положительных и отрицательных координат. В данной статье доказывается, что аналогичные контрпримеры к гипотезе Борсука на сферах малых радиусов можно строить с помощью довольно произвольных конфигураций $(-1, 1)$-векторов и $(-1, 0, 1)$-векторов.

Пусть $\mathcal{V}(n_-, n_+)$ — множество векторов в $\mathbb{R}^n$ $(n = n_+ + n_-)$, у которых n_+ координат равны 1 и n_- координат равны -1. Пусть $\mathcal{G}(n_-, n_+; k, r)$ — множество всех таких дистанционных графов с вершинами $\mathcal{V}(n_-, n_+)$, что для каждого из них найдется изоморфный ему граф диаметров в пространстве $\mathbb{R}^d$ с вершинами, лежащими на сфере радиуса не более r, причем $d \leqslant \overline{C}_n^{2k} + n$ (здесь $\overline{C}_n^m = C_{n+m-1}^m$ — число сочетаний из n по m с повторениями).

Аналогично, пусть $\mathcal{V}(n_-, n_0, n_+)$ — множество векторов в $\mathbb{R}^n$ $(n = n_- + n_0 + n_+)$, у которых n_+ координат равны 1, n_0 координат равны 0 и n_- координат равны -1. В множество

$\mathcal{G}(n_-, n_0, n_+; k, r)$ включим каждый дистанционный граф с вершинами $\mathcal{V}(n_-, n_0, n_+)$, который изоморфен какому-нибудь графу диаметров с вершинами на сфере радиуса не более r в пространстве $\mathbb{R}^d$, $d \leqslant \overline{C}_n^{2k} + n$.

Наконец, определим $\chi(n_-, n_+; k, r)$ и $\chi(n_-, n_0, n_+; k, r)$ как максимум хроматических чисел графов, лежащих соответственно в множествах $\mathcal{G}(n_-, n_+; k, r)$ и $\mathcal{G}(n_-, n_0, n_+; k, r)$. Мы докажем следующие две теоремы.

Теорема 1. *Пусть фиксированы* $r \in (1/2, 1/\sqrt{2})$ *и* $\nu_+ \in [1/2, 3/4)$. *Пусть* $n_+(l) + n_-(l) = n(l) = 4l$ *и* $n_+ \sim \nu_+ n$ *при* $l \to \infty$. *Пусть выбраны натуральное число* k, *такое, что* $r^2 > (2k+1)/(8k)$, *и действительное число* α, *такое, что* $0 \leqslant \alpha < 1 - 2\zeta$ *и*

$$\frac{1}{2} \cdot \frac{(1-\zeta^{4k}) + 2(1-\zeta^2)k\alpha^{2k-1}}{1 + 2k\alpha^{2k-1} + (2k-1)\alpha^{2k}} < r^2,$$

где $\zeta := 2\nu_+ - 1$. *Тогда*

$$\chi(n_-, n_+; k, r) \geqslant \left(\frac{\rho^\rho (1-\rho)^{(1-\rho)}}{{\nu_+}^{\nu_+}(1-\nu_+)^{1-\nu_+}} + o(1) \right)^n,$$

где $\rho := (\alpha + 1)/4$.

Теорема 2. *Пусть фиксированы* $r \in (1/2, 1/\sqrt{2})$, $\nu_+ > 0$ *и* $\nu_- > 0$, *причем* $\nu_+ \geqslant \nu_-$ *и* $\nu_+ + \nu_- \leqslant 1/2$. *Пусть* $n_+(n) + n_0(n) + n_-(n) = n$, $n_+ \sim \nu_+ n$ *и* $n_- \sim \nu_- n$ *при* $n \to \infty$. *Пусть выбраны натуральное число* k *и действительные числа* α *и* ρ *таким образом, что* $r^2 > (2k+1)/(8k)$, $0 < \alpha \leqslant \min\{2\nu_-, 1/2 - \eta\} + \zeta^2$, $\alpha + \eta - \zeta^2 \leqslant \rho < \min\{\eta + 2\nu_-, 1/2\}$ *и*

$$\frac{1}{2} \frac{(\rho-\alpha)^{2k} - (\rho - \alpha - (\eta - \zeta^2))^{2k} + 2k\alpha^{2k-1}(\eta - \zeta^2)}{(\rho-\alpha)^{2k} + 2k\alpha^{2k-1}(\rho - \alpha) + (2k-1)\alpha^{2k}} < r^2,$$

где $\zeta := \nu_+ - \nu_-$ *и* $\eta := \nu_+ + \nu_-$. *Тогда*

$$\chi(n_-, n_0, n_+; k, r) \geqslant \left(\frac{\kappa^\kappa (\rho - 2\kappa)^{\rho - 2\kappa} (1 + \kappa - \rho)^{1+\kappa-\rho}}{{\nu_+}^{\nu_+} {\nu_-}^{\nu_-} (1-\eta)^{1-\eta}} + o(1) \right)^n,$$

где κ *— меньший корень уравнения* $(\rho - 2\kappa)^2 = \kappa(1 - \rho + \kappa)$.

Таблица 1

Основания экспоненты в оценке $\chi(n_-, n_+; k, r)$ (теорема 1)

ν_+	0,50	0,52	0,54	0,56	0,58	0,60	0,64	0,68	0,74
$r^2 = 0{,}50; k = 1$	1,1397	1,1388	1,1361	1,1315	1,1251	1,1170	1,0953	1,0666	1,0107
$r^2 = 0{,}48; k = 1$	1,0747	1,0742	1,0729	1,0708	1,0678	1,0641	1,0545	1,0425	1,0107
$r^2 = 0{,}46; k = 1$	1,0476	1,0472	1,0457	1,0434	1,0402	1,0362	1,0259	1,0132	
$r^2 = 0{,}44; k = 1$	1,0282	1,0277	1,0261	1,0236	1,0201	1,0156	1,0044		
$r^2 = 0{,}42; k = 1$	1,0140	1,0134	1,0117	1,0088	1,0049				
$r^2 = 0{,}40; k = 1$	1,0045	1,0039	1,0019						
$r^2 = 0{,}38; k = 1$	1,0001								
$r^2 = 0{,}38; k = 2$	1,0104	1,0097	1,0075	1,0039					
$r^2 = 0{,}36; k = 2$	1,0057	1,0050	1,0028						
$r^2 = 0{,}34; k = 2$	1,0021	1,0014							
$r^2 = 0{,}32; k = 2$	1,0001								

В табл. 1 приведены наибольшие основания экспоненты, которые можно получить для некоторых значений r, k и ν_+, подобрав оптимальное значение α. Оценка вида $\chi(n_-, n_0, n_+; k, r) \geqslant (C + o(1))^n$ при $n \to \infty$ $(C > 1)$ означает, что для каждого $d \in \mathbb{N}$

найдется конечное множество диаметра 1, расположенное на сфере радиуса не более r в пространстве $\mathbb{R}^d$ таким образом, что эти множества не разбиваются на $(C+o(1))^{\sqrt[2k]{(2k)!d}}$ частей меньшего диаметра. В частности, если $f_r(d)$ — наименьшее такое число, что любое подмножество диаметра 1 сферы радиуса r в $\mathbb{R}^d$ разбивается на $f_r(d)$ частей меньшего диаметра, то мы имеем асимптотическую оценку

$$f_r(d) \geqslant (C+o(1))^{\sqrt[2k]{(2k)!d}}.$$

Таблица 2

Основания экспоненты в теореме 2 при $r^2 = 0{,}5$

$\nu_- \downarrow\ \nu_+ \rightarrow$	0,05	0,10	0,15	0,20	0,25	0,30	0,35	0,40	0,45
0,05	1,0619	1,0835	1,0994	1,1120	1,1216	1,1280	1,1308	1,1297	1,1242
0,10		1,1090	1,1253	1,1364	1,1430	1,1451	1,1423	1,1342	
0,15			1,1403	1,1488	1,1519	1,1496	1,1415		
0,20				1,1541	1,1534	1,1466			
0,25					1,1485				

Таблица 3

Основания экспоненты в теореме 2 при $r^2 = 0{,}48$

$\nu_- \downarrow\ \nu_+ \rightarrow$	0,10	0,15	0,20	0,25	0,30	0,35	0,40	0,45
0,02			1,0015	1,0067	1,0115	1,0151	1,0167	1,0159
0,06	1,0135	1,0199	1,0256	1,0303	1,0332	1,0334	1,0304	
0,10	1,0230	1,0311	1,0371	1,0409	1,0419	1,0393		
0,14		1,0385	1,0442	1,0470				
0,18			1,0488					

Таблица 4

Константа C в оценке $f_r(d) \geqslant (C+o(1))^{\sqrt{2d}}$

r^2	0,500	0,499	0,498	0,497	0,496	0,495
Теорема 1	1,1397	1,1255	1,1196	1,1150	**1,1111**	**1,1077**
Теорема 2	**1,1547**	**1,1324**	**1,1231**	**1,1158**	1,1097	1,1042

В то время как теорема 1 дает некоторые нетривиальные результаты для всех радиусов больше $1/2$, теорема 2 позволяет получить экспоненциальные оценки роста $\chi(n_-, n_0, n_+; k, r)$ лишь для радиусов, близких к $1/\sqrt{2}$. В табл. 2 приведены оптимальные основания экспонент при $r^2 = 0{,}5$, в табл. 3 — при $r^2 = 0{,}48$ ($k = 1$). Для значений радиуса r около $1/\sqrt{2}$ и $k = 1$ обе теоремы дают оценку вида

$$f_r(d) \geqslant (C+o(1))^{\sqrt{2d}},$$

причем иногда теорема 2 позволяет получить большее основание экспоненты C. Оптимальные значения C для некоторых радиусов приведены в табл. 4. При меньших радиусах теорема 1 дает лучший результат.

2. Доказательство теоремы 1

Пусть a — наименьшее число, такое, что $a \geqslant \alpha n$ и отношение $(a+n)/4$ является целым простым числом (далее мы будем обозначать это простое буквой p). Легко видеть, что при этом a окажется целым числом, делящимся на четыре. Также известно, что простые

числа в натуральном ряду расположены достаточно плотно (при достаточно большом x отрезок $[x - x^{0{,}525}, x]$ заведомо содержит простое число [8]), поэтому $a = (\alpha + o(1))n$ и $p \sim (\alpha + 1)n/4 = \rho n$.

Определим на множестве вершин $\mathcal{V}(n_-, n_+)$ дистанционный граф G с запрещенным скалярным произведением $-a$, т. е. соединим ребрами вершины, расстояние между которыми равно $\sqrt{2n + 2a}$. При достаточно большом n граф заведомо будет непустым, так как между векторами из множества $\mathcal{V}(n_-, n_+)$ достигаются любые скалярные произведения, делящиеся на 4, в пределах от наибольшего до наименьшего, а число $-a = -(\alpha + o(1))n$ убывает асимптотически медленнее, чем наименьшее скалярное произведение $n - 4n_- \sim -(1 - 2\zeta)n$ (это следует из условия на α в формулировке теоремы). Докажем, что G принадлежит множеству $\mathcal{G}(n_+, n_-; k, r)$, то есть граф G изоморфен графу диаметров некоторого множества диаметра 1 на сфере малого радиуса (не больше r) в пространстве размерности $\overline{C}_n^{2k} + n$.

Определим величину $c = \sqrt{2ka^{2k-1}}$. Для каждого вектора $\boldsymbol{x} = (x_1, \ldots, x_n)$ из множества $\mathcal{V}(n_-, n_+)$ определим вектор $\boldsymbol{x}^{*2k}$, у которого первые n^{2k} координат предсталяют собой всевозможные произведения упорядоченных наборов из $2k$ координат исходного вектора, а последние n координат — это вектор $\boldsymbol{x}$, умноженный на константу c:

$$\boldsymbol{x}^{*2k} = (x_1 \cdots x_1 x_1, x_1 \cdots x_1 x_2, \ldots, x_n \cdots x_n x_n, cx_1, \ldots, cx_n).$$

Пусть $\mathcal{W}' \subset \mathbb{R}^{n^{2k}+n}$ — множество всех таких векторов. Сразу отметим, что некоторые координаты вектора $\boldsymbol{x}^{*2k}$ заведомо равны друг другу (независимо от выбора $\boldsymbol{x}$). Произведение не зависит от порядка множителей, поэтому множество $\mathcal{W}'$ лежит в некотором подпространстве размерности $\overline{C}_n^{2k} + n$. Исследуем граф диаметров на этом множестве.

Заметим, что для любых двух векторов $\boldsymbol{x} = (x_1, \ldots, x_n)$ и $\boldsymbol{y} = (y_1, \ldots, y_n)$ из $\mathcal{V}(n_-, n_+)$

$$(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k}) = \sum_{i_1=1}^{2k} \ldots \sum_{i_{2k}=1}^{2k} x_{i_1} y_{i_1} \cdots x_{i_{2k}} y_{i_{2k}} + c^2(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{x}, \boldsymbol{y})^{2k} + 2ka^{2k-1}(\boldsymbol{x}, \boldsymbol{y}). \qquad (2)$$

Нетрудно видеть, что наимньшее скалярное произведение $(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k})$ достигается ровно в том случае, когда $(\boldsymbol{x}, \boldsymbol{y}) = -a$. Таким образом, граф G оказался изоморфен графу диаметров множества $\mathcal{W}'$.

Рассмотрим векторы $\boldsymbol{x}^{*2k}$ и $\boldsymbol{y}^{*2k}$, на которых достигается диаметр множества $\mathcal{W}'$ (то есть $(\boldsymbol{x}, \boldsymbol{y}) = -a$). Из формулы (2) следует, что

$$\begin{aligned}(\operatorname{diam} \mathcal{W}')^2 &= |\boldsymbol{x}^{*2k} - \boldsymbol{y}^{*2k}|^2 = (\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) + (\boldsymbol{y}^{*2k}, \boldsymbol{y}^{*2k}) - 2(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k}) = \\ &= 2(n^{2k} + c^2 n) - 2(\boldsymbol{x}, \boldsymbol{y})^{2k} - 4ka^{2k-1}(\boldsymbol{x}, \boldsymbol{y}) = 2(n^{2k} + 2ka^{2k-1}n + (2k-1)a^{2k}).\end{aligned}$$

Поскольку $a = (\alpha + o(1))n$, получаем

$$(\operatorname{diam} \mathcal{W}')^2 \sim 2\left(1 + 2k\alpha^{2k-1} + (2k-1)\alpha^{2k}\right) n^{2k}. \qquad (3)$$

Теперь рассмотрим гомотетичную копию множества $\mathcal{W}'$, имеющую диаметр 1:

$$\mathcal{W} = \{(\operatorname{diam} \mathcal{W}')^{-1} \cdot \boldsymbol{x}^{*2k} \mid \boldsymbol{x}^{*2k} \in \mathcal{W}'\}.$$

Граф G изоморфен графу диаметров множества $\mathcal{W}'$, и, следовательно, графу диаметров множества $\mathcal{W}$, которое расположено в пространстве размерности $\overline{C}_n^{2k} + n$, причем $\operatorname{diam} \mathcal{W} = 1$. Чтобы установить, что $G \in \mathcal{G}(n_+, n_-; k, r)$, осталось доказать, что $\mathcal{W}$ лежит на сфере радиуса r (или меньше).

Определим величину $z = (n_+ - n_-)/n$, то есть среднее арифметическое координат любого вектора $\boldsymbol{x} \in \mathcal{V}(n_-, n_+)$. Сразу же заметим, что

$$z = \frac{2n_+ - n}{n} = 2\nu_+ - 1 + o(1) = \zeta + o(1) \qquad (4)$$

(см. определение ζ в формулировке теоремы). Рассмотрим точку

$$\boldsymbol{o} = (z^{2k}, \ldots, z^{2k}, cz, \ldots, cz),$$

у которой первые n^{2k} координат равны z^{2k}, а последние n координат равны cz. Квадрат расстояния от точки $\boldsymbol{o}$ до произвольной точки $\boldsymbol{x}^{*2k} \in \mathcal{W}'$ равен

$$|\boldsymbol{x}^{*2k} - \boldsymbol{o}|^2 = (\boldsymbol{x}^{*2k} - \boldsymbol{o}, \boldsymbol{x}^{*2k} - \boldsymbol{o}) = (\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) - 2(\boldsymbol{x}^{*2k}, \boldsymbol{o}) + (\boldsymbol{o}, \boldsymbol{o}).$$

Ясно, что $(\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) = n^{2k} + c^2 n$ и $(\boldsymbol{o}, \boldsymbol{o}) = z^{4k} n^{2k} + c^2 z^2 n$. Найдем $(\boldsymbol{x}^{*2k}, \boldsymbol{o})$, учитывая, что сумма всех координат вектора $\boldsymbol{x} \in \mathcal{V}(n_-, n_+)$ равна zn:

$$(\boldsymbol{x}^{*2k}, \boldsymbol{o}) = z^{2k} \left(\sum_{i=1}^{n} x_i \right)^{2k} + c^2 z \sum_{i=1}^{n} x_i = z^{2k} (zn)^{2k} + c^2 z^2 n = z^{4k} n^{2k} + c^2 z^2 n.$$

Выходит, что величина $|\boldsymbol{x}^{*2k} - \boldsymbol{o}|^2$ не зависит от выбора точки $\boldsymbol{x}^{*2k}$, то есть все точки множества $\mathcal{W}'$ располагаются на сфере с центром в точке $\boldsymbol{o}$ и радиусом r', где

$$\begin{aligned}(r')^2 = |\boldsymbol{x}^{*2k} - \boldsymbol{o}|^2 = n^{2k} + c^2 n - 2(z^{4k} n^{2k} + c^2 z^2 n) + z^{4k} n^{2k} + c^2 z^2 n = \\ = (1 - z^{4k}) n^{2k} + (1 - z^2) c^2 n = (1 - z^{4k}) n^{2k} + 2(1 - z^2) k a^{2k-1} n.\end{aligned}$$

Поскольку $z = \zeta + o(1)$ (см. (4)) и $a = (\alpha + o(1))n$, получаем

$$(r')^2 \sim \left((1 - \zeta^{4k}) + 2(1 - \zeta^2) k \alpha^{2k-1} \right) n^{2k}. \tag{5}$$

Множество $\mathcal{W}$ является гомотетичной копией множества $\mathcal{W}'$, поэтому $\mathcal{W}$ лежит на сфере радиуса $r'/\operatorname{diam} \mathcal{W}'$. Найдем асимптотику квадрата этой величины, используя формулы (3) и (5):

$$\left(\frac{r'}{\operatorname{diam} \mathcal{W}'} \right)^2 \sim \frac{\left((1 - \zeta^{4k}) + 2(1 - \zeta^2) k \alpha^{2k-1} \right) n^{2k}}{2\left(1 + 2k\alpha^{2k-1} + (2k-1)\alpha^{2k}\right) n^{2k}} = \frac{1}{2} \cdot \frac{(1 - \zeta^{4k}) + 2(1 - \zeta^2) k \alpha^{2k-1}}{1 + 2k\alpha^{2k-1} + (2k-1)\alpha^{2k}}.$$

По условию теоремы это число меньше, чем r^2, поэтому при достаточно большом n все точки множества $\mathcal{W}$ действительно будут лежать на сфере радиуса меньше r^2.

Итак, мы убедились, что $G \in \mathcal{G}(n_+, n_-; k, r)$. Осталось оценить снизу хроматическое число графа G. Из элементарной теории графов известно, что

$$\chi(G) \geqslant \frac{\operatorname{card} \mathcal{V}(n_-, n_+)}{\alpha(G)}, \tag{6}$$

где $\mathcal{V}(n_-, n_+)$ — это множество вершин нашего графа, а $\alpha(G)$ — это *число независимости* графа G, то есть максимальная мощность такого множества вершин графа, что никакие две из них не соединены в графе ребром (сами такие множества вершин называются *независимыми*). В нашем графе, как легко видеть,

$$\operatorname{card} \mathcal{V}(n_-, n_+) = C_n^{n_+} = \left(\frac{1}{\nu_+^{\nu_+} (1 - \nu_+)^{1 - \nu_+}} + o(1) \right)^n.$$

Из формулировки теоремы и неравенства (6) видно, что для завершения доказательства достаточно асимптотически оценить число независимости графа G следующим образом:

$$\alpha(G) \leqslant \left(\frac{1}{\rho^{\rho} (1 - \rho)^{(1-\rho)}} + o(1) \right)^n.$$

Пусть $U = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s\} \subset \mathcal{V}(n_-, n_+)$ — произвольное независимое множество вершин в графе G (то есть скалярное произведение любых двух векторов из U не равно $-a$). Мы

хотим оценить сверху его мощность s, и для этого применим линейно-алгебраический метод в комбинаторике. Каждому вектору $\boldsymbol{x}_i \in U$ поставим в соответствие многочлен $P_{\boldsymbol{x}_i}$ от n переменных над полем $\mathbb{Z}_p$ вычетов по модулю p следующим образом:

$$P_{\boldsymbol{x}_i}(\boldsymbol{y}) = \prod_{\substack{j=0 \\ j \not\equiv -a \,(\mathrm{mod}\, p)}}^{p-1} (j - (\boldsymbol{x}_i, \boldsymbol{y})). \tag{7}$$

Здесь мы берем произведение по всем целым j от 0 до p кроме единственного значения $j \equiv -a \pmod p$. (Напомним, что число p простое, причем $n - 4p = -a$ — запрещенное скалярное произведение в нашем дистанционном графе G.)

Построенные многочлены обладают следующим свойством: для любых двух $\boldsymbol{x}_i, \boldsymbol{x}_j$ вычет $P_{\boldsymbol{x}_i}(\boldsymbol{x}_j) \not\equiv 0 \pmod p$ тогда и только тогда, когда $(\boldsymbol{x}_i, \boldsymbol{x}_j) \equiv -a \pmod p$. Выясним, когда это условие выполняется. Легко видеть, что скалярное произведение любых двух векторов из $\mathcal{V}(n_-, n_+)$, в том числе и число $-a$, делится на 4. Значит, величина $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ должна отличаться от $-a$ на число, кратное $4p$. Произведение $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ не может в точности равняться $-a$, т. к. векторы взяты из независимого множества U. Также $4p = n + a > n$, поэтому $-a - 4p$ меньше $-n$ и уж тем более меньше наименьшего возможного скалярного произведения векторов из $\mathcal{V}(n_-, n_+)$. Наконец, $-a + 4p = n$ — наибольшее скалярное произведение, достижимое только при умножении вектора на самого себя. Таким образом, $P_{\boldsymbol{x}_i}(\boldsymbol{x}_j) \not\equiv 0 \pmod p$ тогда и только тогда, когда $i = j$.

Преобразуем каждый многочлен $P_{\boldsymbol{x}_i}$ следующим образом. Раскрыв скобки в определении (7), представим $P_{\boldsymbol{x}_i}$ в виде линейной комбинации одночленов вида $y_{i_1}^{\alpha_1} \cdots y_{i_q}^{\alpha_q}$, где $q \leqslant p - 1$. Заменив в каждом таком таком одночлене четные степени α_t на нули, а нечетные степени α_t на единицы, получим новый многочлен $P'_{\boldsymbol{x}_i} \in \mathbb{Z}_p[y_1, \ldots, y_n]$, являющийся линейной комбинацией одночленов вида $y_{i_1} \cdots y_{i_q}$, где $q \leqslant p - 1$. Это означает, что многочлены $P'_{\boldsymbol{x}_1}, \ldots, P'_{\boldsymbol{x}_s}$ расположены в линейном подпространстве пространства $\mathbb{Z}_p[y_1, \ldots, y_n]$ размерности

$$C_n^0 + C_n^1 + \ldots + C_n^{p-1}. \tag{8}$$

Кроме того, из построения $P'_{\boldsymbol{x}_i}$ видно, что $P'_{\boldsymbol{x}_i}(\boldsymbol{y}) = P_{\boldsymbol{x}_i}(\boldsymbol{y})$ для любого $\boldsymbol{y} \in \mathcal{V}(n_-, n_+)$, поэтому новые многочлены обладают тем же свойством, что было отмечено в предыдущем абзаце для старых многочленов: $P'_{\boldsymbol{x}_i}(\boldsymbol{x}_j) \not\equiv 0 \pmod p$ тогда и только тогда, когда $i = j$.

Теперь докажем, что многочлены $P'_{\boldsymbol{x}_1}, \ldots, P'_{\boldsymbol{x}_s}$ линейно независимы. Предположим, что

$$c_1 P'_{\boldsymbol{x}_1} + \ldots + c_s P'_{\boldsymbol{x}_s} \equiv 0 \pmod p \tag{9}$$

для некоторых целых коэффициентов c_i. Подставим вместо $\boldsymbol{y}$ произвольный $\boldsymbol{x}_j$. В силу указанных выше свойств все слагаемые $P'_{\boldsymbol{x}_i}(\boldsymbol{x}_j)$, $i \neq j$, обнулятся (по модулю p) и останется сравнение

$$c_j P'_{\boldsymbol{x}_j}(\boldsymbol{x}_j) \equiv 0 \pmod p.$$

Но $P'_{\boldsymbol{x}_j}(\boldsymbol{x}_j) \not\equiv 0 \pmod p$, значит, $c_j \equiv 0 \pmod p$. Это верно для каждого $j = 1, \ldots, s$, то есть линейная комбинация (9) была тривиальной.

Итак, многочлены $P'_{\boldsymbol{x}_1}, \ldots, P'_{\boldsymbol{x}_s}$ оказались линейно независимыми, значит их количество s не превышает размерности пространства (8). Но s — мощность произвольного независимого множества U, то есть мы нашли верхнюю оценку числа независимости $\alpha(G)$. Учитывая, что $p \sim \rho n$, с помощью формулы Стирлинга получаем

$$\alpha(G) \leqslant C_n^0 + C_n^1 + \ldots + C_n^{p-1} = \left(\frac{1}{\rho^\rho (1-\rho)^{(1-\rho)}} + o(1) \right)^n,$$

что и завершает наше доказательство.

3. Доказательство теоремы 2

Определим $a := \alpha n$. Далее, пусть p — наименьшее простое число, такое, что $p \geqslant \rho n$ и $p \geqslant a + n_+ + n_- - (n_+ - n_-)^2/n$. Про последнюю величину мы знаем, что

$$a + n_+ + n_- - \frac{(n_+ - n_-)^2}{n} \sim \left(\alpha + \nu_+ + \nu_- - (\nu_+ - \nu_-)^2\right) n = (\alpha + \eta - \zeta^2)n,$$

причем по условию $\alpha + \eta - \zeta^2 \leqslant \rho$, поэтому $p \sim \rho n$.

Также сразу докажем, что

$$n_+ + n_- - 2p < -2n_-. \tag{10}$$

Действительно, нам достаточно убедиться, что $n_+ + n_- - p < (n_+ - n_-)/2$, то есть $p > n_+ + n_- - (n_+ - n_-)/2$, а последнее неравенство следует из определения числа p и неравенства $n_+ - n_- < n/2$ (по условию теоремы $n_+ - n_- \sim (\nu_+ - \nu_-)n$ и $\nu_+ - \nu_- < 1/2$):

$$p \geqslant a + n_+ + n_- - \frac{(n_+ - n_-)^2}{n} > n_+ + n_- - \frac{(n_+ - n_-)^2}{n} \geqslant n_+ + n_- - \frac{n_+ - n_-}{2}.$$

Определим на множестве $\mathcal{V}(n_-, n_0, n_+)$ дистанционный граф G с запрещенным расстоянием $\sqrt{2p}$. Ребрами окажутся соединены те и только те пары вершин $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{V}(n_-, n_0, n_+)$, для которых $(\boldsymbol{x}, \boldsymbol{y}) = n_+ + n_- - p$. Заметим, что

$$n_+ + n_- - p = (\nu_+ + \nu_- - \rho + o(1))n = (\eta - \rho + o(1))n.$$

Из условия на ρ в формулировке теоремы следует, что $\eta - \rho > -2\nu_-$, то есть при достаточно больших n запрещенное скалярное произведение $n_+ + n_- - p$ будет больше числа $-2n_-$. При этом между векторами из $\mathcal{V}(n_-, n_0, n_+)$ достигается любое целое скалярное произведение от $-2n_-$ до $n_+ + n_-$, что означает, что граф G не будет пустым. Докажем, что $G \in \mathcal{G}(n_+, n_0, n_-; k, r)$, то есть наш граф изоморфен некоторому графу диаметров в пространстве размерности $\overline{C}_n^{2k} + n$ с вершинами на сфере малого радиуса.

Определим λ как корень уравнения

$$\lambda^2 n - 2\lambda(n_+ - n_-) + n_+ + n_- + a - p = 0 \tag{11}$$

(мы определили p таким образом, чтобы дискриминант оказался положительным). Для определенности возьмем наибольший корень, то есть

$$\lambda := z + \sqrt{z^2 - \frac{n_+ + n_- + a - p}{n}},$$

где $z := (n_+ - n_-)/n$ — среднее арифметическое всех координат любого вектора $\boldsymbol{x} \in \mathcal{V}(n_-, n_0, n_+)$. Также положим $c := \sqrt{2ka^{2k-1}}$. Для каждого $\boldsymbol{x} \in \mathcal{V}(n_-, n_0, n_+)$ определим вектор $\boldsymbol{x}^{*2k} \in \mathbb{R}^{n^{2k}+n}$ следующим образом:

$$\boldsymbol{x}^{*2k} = ((x_1 - \lambda)\cdots(x_1 - \lambda)(x_1 - \lambda), (x_1 - \lambda)\cdots(x_1 - \lambda)(x_2 - \lambda), \ldots, \\ (x_n - \lambda)\cdots(x_n - \lambda)(x_n - \lambda), c(x_1 - \lambda), \ldots, c(x_n - \lambda)),$$

то есть первые n^{2k} координат имеют вид $(x_{i_1} - \lambda)\cdots(x_{i_{2k}} - \lambda)$ для всевозможных упорядоченных наборов индексов $i_1, \ldots, i_{2k}$. Пусть $\mathcal{W}'$ — множество всех векторов $\boldsymbol{x}^{*2k}$. В силу коммутативности умножения некоторые координаты вектора $\boldsymbol{x}^{*2k}$ заведомо совпадают, поэтому $\mathcal{W}'$ лежит в подпространстве размерности $\overline{C}_n^{2k} + n$.

Теперь исследуем граф диаметров на $\mathcal{W}'$. Рассмотрим две вершины $\boldsymbol{x}^{*2k}$ и $\boldsymbol{y}^{*2k}$ из $\mathcal{W}'$. Их скалярное произведение равно

$$(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k}) = \sum_{i_1=1}^{n} \ldots \sum_{i_{2k}=1}^{n} (x_{i_1} - \lambda)(y_{i_1} - \lambda)\cdots(x_{i_{2k}} - \lambda)(y_{i_{2k}} - \lambda)) + \\ + c^2 \sum_{i=1}^{n} (x_i - \lambda)(y_i - \lambda) = (\boldsymbol{x} - \boldsymbol{\lambda}, \boldsymbol{y} - \boldsymbol{\lambda})^{2k} + c^2(\boldsymbol{x} - \boldsymbol{\lambda}, \boldsymbol{y} - \boldsymbol{\lambda}),$$

где $\boldsymbol{\lambda} = (\lambda, \ldots, \lambda) \in \mathbb{R}^n$. Заметим, что $(\boldsymbol{x}, \boldsymbol{\lambda}) = (\boldsymbol{y}, \boldsymbol{\lambda}) = \lambda(n_+ - n_-)$, поэтому, с учетом равенства (11),

$$(\boldsymbol{x} - \boldsymbol{\lambda}, \boldsymbol{y} - \boldsymbol{\lambda}) = (\boldsymbol{x}, \boldsymbol{y}) - (\boldsymbol{x}, \boldsymbol{\lambda}) - (\boldsymbol{y}, \boldsymbol{\lambda}) + (\boldsymbol{\lambda}, \boldsymbol{\lambda}) = (\boldsymbol{x}, \boldsymbol{y}) - 2\lambda(n_+ - n_-) + \lambda^2 n = \\ = (\boldsymbol{x}, \boldsymbol{y}) + p - a - n_+ - n_-,$$

то есть

$$(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k}) = ((\boldsymbol{x}, \boldsymbol{y}) + p - a - n_+ - n_-)^{2k} + c^2((\boldsymbol{x}, \boldsymbol{y}) + p - a - n_+ - n_-). \quad (12)$$

Расстояние между $\boldsymbol{x}^{*2k}$ и $\boldsymbol{y}^{*2k}$ максимально тогда и только тогда, когда минимально их скалярное произведение. Величина $s^{2k} + c^2 s$ минимизируется при $s = -\sqrt[2k-1]{\frac{c^2}{2k}} = -a$, поэтому минимум скалярного произведения (12) достигается при $(\boldsymbol{x}, \boldsymbol{y}) + p - a - n_+ - n_- = -a$, то есть когда $(\boldsymbol{x}, \boldsymbol{y}) = n_+ + n_- - p$, а это как раз запрещенное скалярное произведение в дистанционном графе G. Итак, между $\boldsymbol{x}^{*2k}$ и $\boldsymbol{y}^{*2k}$ достигается диаметр множества $\mathcal{W}'$ тогда и только тогда, когда $\boldsymbol{x}$ и $\boldsymbol{y}$ соединены ребром в G. Иными словами, граф диаметров множества $\mathcal{W}'$ изоморфен графу G.

Теперь мы можем найти сам диаметр $\mathcal{W}'$. Пусть $\boldsymbol{x}^{*2k}$ и $\boldsymbol{y}^{*2k}$ — две наиболее удаленные друг от друга точки из $\mathcal{W}'$. Тогда

$$(\operatorname{diam} \mathcal{W}')^2 = (\boldsymbol{x}^{*2k} - \boldsymbol{y}^{*2k}, \boldsymbol{x}^{*2k} - \boldsymbol{y}^{*2k}) = (\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) + (\boldsymbol{y}^{*2k}, \boldsymbol{y}^{*2k}) - 2(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k}).$$

Из предыдущего абзаца мы уже знаем, что

$$(\boldsymbol{x}^{*2k}, \boldsymbol{y}^{*2k}) = (-a)^{2k} + c^2(-a) = -(2k-1)a^{2k}.$$

Выразим $(\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k})$, используя формулу (12) и равенство $(\boldsymbol{x}, \boldsymbol{x}) = n_+ + n_-$:

$$(\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) = ((\boldsymbol{x}, \boldsymbol{x}) + p - a - n_+ - n_-)^{2k} + c^2((\boldsymbol{x}, \boldsymbol{x}) + p - a - n_+ - n_-) = (p-a)^{2k} + c^2(p-a).$$

Ясно, что произведение $(\boldsymbol{y}^{*2k}, \boldsymbol{y}^{*2k})$ будет точно таким же. Получаем

$$(\operatorname{diam} \mathcal{W}')^2 = 2\left((p-a)^{2k} + c^2(p-a) + (2k-1)a^{2k}\right) \sim \\ \sim 2\left((\rho-\alpha)^{2k} + 2k\alpha^{2k-1}(\rho-\alpha) + (2k-1)\alpha^{2k}\right) n^{2k}. \quad (13)$$

Докажем, что все точки множества $\mathcal{W}'$ равноудалены от центра

$$\boldsymbol{o} = ((z-\lambda)^{2k}, \ldots, (z-\lambda)^{2k}, c(z-\lambda), \ldots, c(z-\lambda))$$

(здесь первые n^{2k} координат равны $(z-\lambda)^{2k}$, а оставшиеся n равны $c(z-\lambda)$). Найдем квадрат расстояния от произвольного $\boldsymbol{x}^{*2k} \in \mathcal{W}'$ до $\boldsymbol{o}$:

$$|\boldsymbol{x}^{*2k} - \boldsymbol{o}|^2 = (\boldsymbol{x}^{*2k} - \boldsymbol{o}, \boldsymbol{x}^{*2k} - \boldsymbol{o}) = (\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) - 2(\boldsymbol{x}^{*2k}, \boldsymbol{o}) + (\boldsymbol{o}, \boldsymbol{o}).$$

Мы уже знаем, что $(\boldsymbol{x}^{*2k}, \boldsymbol{x}^{*2k}) = (p-a)^{2k} + c^2(p-a)$. Найдем остальные слагаемые, пользуясь тем, что сумма всех координат вектора $\boldsymbol{x} \in \mathcal{V}(n_-, n_0, n_+)$ равна zn:

$$(\boldsymbol{x}^{*2k}, \boldsymbol{o}) = (z-\lambda)^{2k}\left(\sum_{i=1}^{n}(x_i - \lambda)\right)^{2k} + c^2(z-\lambda)\sum_{i=1}^{n}(x_i - \lambda) = \\ = (z-\lambda)^{2k}(zn - \lambda n)^{2k} + c^2(z-\lambda)(zn - \lambda n) = ((z-\lambda)^2 n)^{2k} + c^2(z-\lambda)^2 n,$$

$$(\boldsymbol{o}, \boldsymbol{o}) = (z-\lambda)^{4k} n^{2k} + c^2(z-\lambda)^2 n = ((z-\lambda)^2 n)^{2k} + c^2(z-\lambda)^2 n.$$

Получается, что величина $|\boldsymbol{x}^{*2k} - \boldsymbol{o}|^2$ одинакова для всех $\boldsymbol{x}^{*2k} \in \mathcal{W}'$, то есть $\mathcal{W}'$ является подмножеством сферы, квадрат радиуса которой равен

$$(r')^2 = (p-a)^{2k} - (z-\lambda)^{4k} n^{2k} + c^2(p - a - (z-\lambda)^2 n).$$

Из определения числа λ напрямую следует, что $(z-\lambda)^2 n = p - a - (n_+ + n_- - z^2 n)$, поэтому

$$(r')^2 = (p-a)^{2k} - (p - a - (n_+ + n_- - z^2 n))^{2k} + c^2(n_+ + n_- - z^2 n). \tag{14}$$

Рассмотрим множество

$$\mathcal{W} = \{(\operatorname{diam} \mathcal{W}')^{-1} \cdot \boldsymbol{x}^{*2k} \mid \boldsymbol{x}^{*2k} \in \mathcal{W}'\}.$$

Его диаметр, очевидно, равен 1. Граф диаметров, построенный на множестве точек $\mathcal{W}$, изоморфен графу диаметров на $\mathcal{W}'$, который, как мы знаем, изоморфен графу G. Все точки $\mathcal{W}'$ лежат на сфере радиуса r', значит $\mathcal{W}$ лежит на сфере радиуса $r'/\operatorname{diam} \mathcal{W}'$. Мы хотим доказать, что $G \in \mathcal{G}(n_-, n_0, n_+; k, r)$, то есть осталось установить, что радиус $r'/\operatorname{diam} \mathcal{W}'$ не превышает r. Найдем асимптотику квадрата этой величины, используя равенства (13) и (14), учитывая также, что $c^2 = 2k\alpha^{2k-1} n^{2k-1}$ и $n_+ + n_- \sim \eta n$:

$$\left(\frac{r'}{\operatorname{diam} \mathcal{W}'}\right)^2 = \frac{1}{2} \frac{(p-a)^{2k} - (p - a - (n_+ + n_- - z^2 n))^{2k} + c^2(n_+ + n_- - z^2 n)}{(p-a)^{2k} + c^2(p-a) + (2k-1)a^{2k}} \sim$$
$$\sim \frac{1}{2} \frac{(\rho-\alpha)^{2k} - (\rho - \alpha - (\eta - \zeta^2))^{2k} + 2k\alpha^{2k-1}(\eta - \zeta^2)}{(\rho-\alpha)^{2k} + 2k\alpha^{2k-1}(\rho - \alpha) + (2k-1)\alpha^{2k}}.$$

По условию это число меньше r^2, значит, при достаточно больших n радиус $r'/\operatorname{diam} \mathcal{W}'$ будет действительно меньше r.

Итак, граф G в самом деле принадлежит множеству $\mathcal{G}(n_-, n_0, n_+; k, r)$, и теперь мы хотим оценить его хроматическое число. Мы знаем, что

$$\chi(G) \geqslant \frac{\operatorname{card} \mathcal{V}(n_-, n_0, n_+)}{\alpha(G)},$$

причем

$$\operatorname{card} \mathcal{V}(n_-, n_0, n_+) = C_n^{n_+} C_{n-n_+}^{n_-} = \left(\frac{1}{{\nu_+}^{\nu_+} {\nu_-}^{\nu_-} (1-\eta)^{1-\eta}} + o(1)\right)^n.$$

Для завершения доказательства достаточно доказать оценку числа независимости $\alpha(G)$ вида

$$\alpha(G) < \left(\frac{1}{\kappa^\kappa (\rho - 2\kappa)^{\rho - 2\kappa} (1 + \kappa - \rho)^{1+\kappa-\rho}} + o(1)\right)^n. \tag{15}$$

Рассмотрим произвольное независимое множество $U = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_s\} \subset \mathcal{V}(n_-, n_0, n_+)$ в графе G (то есть $(\boldsymbol{x}_i, \boldsymbol{x}_j) \neq n_+ + n_- - p$ для любых $i, j = 1, \ldots, s$) и сопоставим каждому вектору $\boldsymbol{x}_i$ многочлен $P_{\boldsymbol{x}_i}$ от n переменных над полем $\mathbb{Z}_p$:

$$P_{\boldsymbol{x}_i}(\boldsymbol{y}) = \prod_{\substack{j=0 \\ j \not\equiv n_+ + n_- \pmod p}}^{p-1} (j - (\boldsymbol{x}_i, \boldsymbol{y})).$$

Докажем, что для любых двух векторов $\boldsymbol{x}_i, \boldsymbol{x}_j \in U$ условие $P_{\boldsymbol{x}_i}(\boldsymbol{x}_j) \not\equiv 0 \pmod p$ эквивалентно равенству $i = j$. Действительно, многочлен определен таким образом, что $P_{\boldsymbol{x}_i}(\boldsymbol{x}_j)$ не делится на простое p ровно в тех случаях, когда $(\boldsymbol{x}_i, \boldsymbol{x}_j) \equiv n_+ + n_- \pmod p$. Но, как уже было замечено выше, скалярное произведение $(\boldsymbol{x}_i, \boldsymbol{x}_j)$ — это целое число в пределах от $-2n_-$ до $n_+ + n_-$, причем оно не может равняться $n_+ + n_- - p$, а число $n_+ + n_- - 2p$ уже не попадает в указанный диапазон в силу неравенства (10). Таким образом, сравнение $(\boldsymbol{x}_i, \boldsymbol{x}_j) \equiv n_+ + n_- \pmod p$ равносильно равенству векторов $\boldsymbol{x}_i$ и $\boldsymbol{x}_j$.

Каждый многочлен $P_{\boldsymbol{x}_i}$ представи́м в виде линейной комбинации одночленов вида $y_{i_1}^{\alpha_1}\cdots y_{i_q}^{\alpha_q}$, степень которых $\alpha_1+\ldots+\alpha_q$ не превышает $p-1$. Заменив в каждом таком одночлене все нечетные α_t на 1 и все четные α_t на 2, получим новый многочлен $P'_{\boldsymbol{x}_i}$, значение которого совпадает с $P_{\boldsymbol{x}_i}$ на всех $\boldsymbol{y}\in\mathcal{V}(n_-,n_0,n_+)$, то есть, опять же, $P'_{\boldsymbol{x}_i}(\boldsymbol{x}_j)\not\equiv 0 \pmod p$ тогда и только тогда, когда $i=j$. По построению многочлены $P'_{\boldsymbol{x}_i}$ состоят из мономов вида $y_{i_1}^{\alpha_1}\cdots y_{i_q}^{\alpha_q}$, где

$$q<p,\quad \alpha_1,\ldots,\alpha_q\in\{1,2\},\quad \alpha_1+\ldots+\alpha_q\leqslant p-1.$$

Мономы такого вида порождают в $\mathbb{Z}_p[y_1,\ldots,y_n]$ подпространство размерности

$$\sum_{\substack{i,j\in\mathbb{N}\cup\{0\}\\ i+2j\leqslant p-1}} C_n^i C_{n-i}^j$$

(здесь i — количество переменных, входящих в моном со степенью 1, а j — количество переменных, входящих со степенью 2).

Аналогично доказательству предыдущей теоремы убеждаемся, что многочлены $P'_{\boldsymbol{x}_1},\ldots,P'_{\boldsymbol{x}_s}$ линейно неависимы: предположив, что

$$c_1P'_{\boldsymbol{x}_1}+\ldots+c_sP'_{\boldsymbol{x}_s}\equiv 0 \pmod p,$$

вычислем значение левой части в точке $\boldsymbol{x}_i$ и получаем, что $c_iP'_{\boldsymbol{x}_i}(\boldsymbol{x}_i)\equiv 0 \pmod p$, то есть $c_i\equiv 0 \pmod p$ — линейная комбинация была тривиальной. Значит, количество наших многочленов s (равное мощности независимого множества U) не превышает разерности подпространства, которому принадлежат все многочлены $P'_{\boldsymbol{x}_i}$. Мы оценили сверху мощность произвольного независимого множества, а значит и число независимости графа G:

$$\alpha(G)\leqslant \sum_{\substack{i,j\in\mathbb{N}\cup\{0\}\\ i+2j\leqslant p-1}} C_n^i C_{n-i}^j.$$

Для получения оценки (15) остается доказать, что

$$\sum_{\substack{i,j\in\mathbb{N}\cup\{0\}\\ i+2j\leqslant p-1}} C_n^i C_{n-i}^j = \left(\frac{1}{\kappa^\kappa(\rho-2\kappa)^{\rho-2\kappa}(1+\kappa-\rho)^{1+\kappa-\rho}}+o(1)\right)^n.$$

Это достаточно рутинная выкладка, и мы не будем вдаваться в подробности. Идея заключается в том, что наибольшее слагаемое в нашей сумме экспоненциально (то есть асиптотически равно $(C+o(1))^n$ для некоторого $C>1$), а общее число слагаемых полиномиально, поэтому вся сумма тоже представима в виде $(C+o(1))^n$. Осталось найти асимптотику наибольшего слагаемого в сумме. Ясно, что в этом слагаемом $i+2j=p-1$ (т. к. $p\sim\rho n$ и $\rho<1/2$), поэтому оно имеет вид $C_n^iC_{n-i}^{p-1-2i}$. Можно доказать, что искомый параметр i асимптотически эквивалентен κn для некоторой константы κ, поэтому (с учетом $p\sim\rho n$)

$$C_n^iC_{n-i}^{p-1-2i} = \left(\frac{1}{\kappa^\kappa(\rho-2\kappa)^{\rho-2\kappa}(1-\rho+\kappa)^{1-\rho+\kappa}}+o(1)\right)^n.$$

Стандартными методами анализа проверяем, что κ из условия теоремы максимизирует константу в скобках, что и завершает наше доказательство.

Литература

1. *Borsuk K.* Drei Sätze über die n-dimensionale euklidische Sphäre // Fundamenta Mathematicae. 1933. Jg. 20. S. 177–190.

2. *Kahn J., Kalai G.* A counterexample to Borsuk's conjecture // Bulletin (new series) of the AMS. 1993. V. 29. P. 60–62.

3. *Райгородский А.М.* Вокруг гипотезы Борсука // Современная математика. Фундаментальные направления. 2007. Т. 23. С. 147—164.

4. *Райгородский А. М.* Об одной оценке в проблеме Борсука // Успехи математических наук. 1999. Т. 54, вып. 2(326). С. 185—186.

5. *Schramm O.* Illuminating sets of constant width // Mathematika. 1988. V. 35. P. 180–189.

6. *Бердников А.В., Райгородский А.М.* Оценки чисел Борсука по дистанционным графам специального вида // Пробл. передачи информ. 2021. Т. 57, вып. 2. С. 44—50.

7. *Kupavskii A., Raigorodskii A.* A counterexample to Borsuk's conjecture // Moscow Journal of Combinatorics and Number Theory. 2012. V. 2. P. 27–48.

8. *Baker R. C., Harman G., Pintz J.* The Difference Between Consecutive Primes, II // Proceedings of the London Mathematical Society. 2001. V. 83, I. 3. P. 532–562.

References

1. *Borsuk K.* Three theorems on the n-dimensional Euclidean sphere. Fundamenta Mathematicae. 1933. V. 20. P. 177–190. (in German).

2. *Kahn J., Kalai G.* A counterexample to Borsuk's conjecture. Bulletin (new series) of the AMS. 1993. V. 29. P. 60–62.

3. *Raigorodskii A. M.* Around Borsuk's Hypothesis. Journal of Mathematical Sciences. 2008. V. 154, I. 4. P. 604–623.

4. *Raigorodskii A. M.* On a bound in Borsuk's problem. Russian Mathematical Surveys. 1999. V. 54, I. 2. P. 453–454.

5. *Schramm O.* Illuminating sets of constant width. Mathematika. 1988. V. 35. P. 180–189.

6. *Berdnikov A. V., Raigorodskii A. M.* Bounds on Borsuk numbers in distance graphs of a special type. Problems of Information Transmission. 2021. V. 57. P. 136–142.

7. *Kupavskii A., Raigorodskii A.* A counterexample to Borsuk's conjecture. Moscow Journal of Combinatorics and Number Theory. 2012. V. 2. P. 27–48.

8. *Baker R. C., Harman G., Pintz J.* The Difference Between Consecutive Primes, II. Proceedings of the London Mathematical Society. 2001. V 83, I. 3. P. 532–562.

Поступила в редакцию 29.08.2021