Ф.Ю. Воробьев

О СТРУКТУРЕ МНОЖЕСТВА ВЫПОЛНЯЮЩИХ НАБОРОВ СЛУЧАЙНОЙ k-КНФ [1]

1 Введение

Пусть $x_1, \dots, x_n$ – множество из n булевых переменных. Назовем k-буквенной скобкой дизъюнкцию вида $(x_{i_1}^{\sigma_1} \vee x_{i_2}^{\sigma_2} \vee \dots \vee x_{i_k}^{\sigma_k})$. Построим случайную k-КНФ $F_k(n,m)$ путем случайного, равновероятного и независимого выбора m скобок из числа $2^k C_n^k$ всех скобок. Многие исследования посвящены изучению структуры $N_{F_k(n,rn)}$ – множества выполняющих наборов $F_k(n,rn)$, где r – константа, а n стремится к бесконечности. Пусть $S_k(n,r)$ – вероятность того, что $F_k(n,rn)$ выполнима. Определим

$$r_k \equiv \sup\{r : \lim_{n\to\infty} S_k(n,r) = 1\},$$

$$r_k^* \equiv \inf\{r : \lim_{n\to\infty} S_k(n,r) = 0\},$$

то есть r_k – точная верхняя грань таких r, что вероятность выполнимости формулы все еще стремится к единице, r_k^* – точная нижняя грань таких r, что вероятность выполнимости формулы стремится к нулю. Ясно, что $r_k \le r_k^*$. Существует предположение, что $r_k = r_k^*$, то есть при увеличении r в определенный момент происходит скачок предела вероятности выполнимости от единицы к нулю. Такое число r_k называется *порогом выполнимости.*

Существование порога не доказано, но известно следующее утверждение:

Теорема 1. *(Friedgut [4]) Для любого $k \ge 2$ существует такая последовательность $r_k(n)$, что для любого $\varepsilon > 0$*

$$\lim_{n\to\infty} S_k\left(n, (1-\varepsilon) r_k(n)\right) = 1,$$

$$\lim_{n\to\infty} S_k\left(n, (1+\varepsilon) r_k(n)\right) = 0.$$

[1]Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант 07-01-00444А

Следствие 1. *Зафиксируем $k \geq 2$. Если $F_k(n, rn)$ выполнима с вероятностью $P_n > C > 0$, то $r_k > r$.*

В работах [1], [2], [3] были получены нижние оценки порога выполнимости для различных k с помощью метода вторых моментов в следующем виде.

Лемма 1. *(Метод вторых моментов) Пусть X – неотрицательная случайная величина. Тогда*

$$P(X > 0) \geq \frac{M^2(X)}{M(X^2)}.$$

В 2005 году в работе [7] было доказано, что при определенных значениях r с высокой вероятностью ($P \to 1$) множество выполняющих наборов разбивается на „кластеры`` – подмножества, расстояния между которыми существенно больше, чем диаметры самих подмножеств.

В настоящей работе исследуется вероятность присутствия в множестве выполняющих наборов $F_k(n, rn)$ граней различных размерностей.

2 Общие соображения

Из элементарных соображений получается следующий результат.

Теорема 2. *Пусть $r < r_k$, $t(n) = o(n)$. Тогда с высокой вероятностью ($P \to 1$ при $n \to \infty$) множество $N_{F_k(n,rn)}$ состоит из граней размерности не меньше $t(n)$.*

Чтобы доказать это, заметим, что с высокой вероятностью не менее $t(n)$ из переменных $x_1, \ldots, x_n$ не попадут в формулу.

Лемма 2. *Если $t(n) = o(n)$, то с высокой вероятностью не менее $t(n)$ из переменных $x_1, \ldots, x_n$ не входят в формулу $F_k(n, rn)$.*

Доказательство. Построим случайную формулу $F_k(n, rn)$ с помощью выбора rn скобок из числа $2^k C_n^k$ всех k-буквенных скобок. Пусть X – случайная величина, равная числу переменных, не вошедших в формулу, а V – множество переменных, вошедших в формулу. Тогда

$$X = \sum_i 1_{x_i \notin V}.$$

Пусть V_j – множество переменных из j-й скобки формулы.

$$M(X) = \sum_{i=1}^{n} P(x_i \notin V) = nP(x_i \notin V) = n \prod_{j=1}^{rn} P(x_i \notin V_j) = nP(x_i \notin V_j)^{rn}.$$

Заметим, что переменная входит в скобку с вероятностью k/n, а значит,

$$M(X) = n\left(1 - \frac{k}{n}\right)^{rn} \sim ne^{-kr}. \qquad (1)$$

Для того, чтобы применить неравенство Пэли-Зигмунда в виде

$$P(X \geq t) \geq \frac{(M(X) - t)^2}{M(X^2)}$$

при $t \leq M(X)$, нам потребуется найти $M(X^2)$.

$$M(X^2) = M\left(\left(\sum_i 1_{x_i \notin V}\right)^2\right) = M\left(\sum_{i_1, i_2 = 1}^{n} 1_{x_{i_1}, x_{i_2} \notin V}\right) =$$

$$= \sum_{i_1, i_2 = 1}^{n} P(x_{i_1}, x_{i_2} \notin V) = \sum_{i=1}^{n} P(x_i \notin V) + \sum_{i_1 \neq i_2} P(x_{i_1}, x_{i_2} \notin V) =$$

$$= nP(x_i \notin V) + (n^2 - n)P(x_{i_1}, x_{i_2} \notin V). \qquad (2)$$

Вероятность $P(x_i \notin V)$ уже посчитана и равна $\left(1 - \frac{k}{n}\right)^{rn} \to e^{-kr}$. Вероятность $P(x_{i_1}, x_{i_2} \notin V)$ равна $P(x_{i_1}, x_{i_2} \notin V_j)^{rn}$. В то же время

$$P(x_{i_1}, x_{i_2} \notin V_j) = 1 - P(x_{i_1} \in V_j \cup x_{i_2} \in V_j) =$$
$$= 1 - (P(x_{i_1} \in V_j) + P(x_{i_2} \in V_j) - P(x_{i_1} \in V_j \cap x_{i_2} \in V_j)).$$

Вероятность того, что две заданные переменные входят в случайную скобку, равна $\frac{k}{n}\frac{k-1}{n-1}$, так как всего есть C_n^2 способов выбрать две переменные из $\{x_1, \ldots, x_n\}$ и C_k^2 способов выбрать две переменные из V_j. Следовательно,

$$1-(P(x_{i_1} \in V_j) + P(x_{i_2} \in V_j) - P(x_{i_1} \in V_j \cap x_{i_2} \in V_j)) = 1 - \frac{2k}{n} + \frac{k}{n}\frac{k-1}{n-1},$$

а значит,

$$P(x_{i_1}, x_{i_2} \notin V) = \left(1 - \frac{2k}{n} + \frac{k}{n}\frac{k-1}{n-1}\right)^{rn} \to e^{-2kr}.$$

Подставляя это в (2), получим

$$M(X^2) = n\left(1-\frac{k}{n}\right)^{rn} + (n^2-n)\left(1-\frac{2k}{n}+\frac{k}{n}\frac{k-1}{n-1}\right)^{rn}. \qquad (3)$$

Пусть $t(n) = o(n)$. По неравенству Пэли-Зигмунда,

$$P(X > t(n)) \geq \frac{(M(X)-t(n))^2}{M(X^2)}.$$

Подставляя (1) и (3), получим

$$\frac{(M(X)-t(n))^2}{M(X^2)} = \frac{\left(n\left(1-\frac{k}{n}\right)^{rn}-t(n)\right)^2}{n\left(1-\frac{k}{n}\right)^{rn}+(n^2-n)\left(1-\frac{2k}{n}+\frac{k}{n}\frac{k-1}{n-1}\right)^{rn}} =$$

$$= \frac{\left(\left(1-\frac{k}{n}\right)^{rn}-\frac{t(n)}{n}\right)^2}{\frac{1}{n}\left(1-\frac{k}{n}\right)^{rn}+\left(1-\frac{1}{n}\right)\left(1-\frac{2k}{n}+\frac{k}{n}\frac{k-1}{n-1}\right)^{rn}}. \qquad (4)$$

Так как $\left(1-\frac{k}{n}\right)^{rn} \to e^{-kr}$, $\left(1-\frac{2k}{n}+\frac{k}{n}\frac{k-1}{n-1}\right)^{rn} \to e^{-2kr}$, а $t(n) = o(n)$,

$$\lim_{n\to\infty}\frac{(M(X)-t(n))^2}{M(X^2)} = \frac{(e^{-kr})^2}{e^{-2kr}} = 1.$$

Следовательно, $P(X > t(n)) \to 1$, что и требовалось доказать. ■

Таким образом, с высокой вероятностью в $F_k(n, rn)$ не войдут $t(n)$ переменных. Если $r < r_k$, то формула $F_k(n, rn)$ выполнима с высокой вероятностью. Пусть σ – ее выполняющий набор. Ясно, что изменяя координаты, соответствующие переменным, не вошедшим в формулу, мы получим грань размерности $t(n)$, состоящую из выполняющих наборов. ■

Из доказательства леммы 2 понятно, что даже при $t(n)/n = const < e^{-kr}$ можно оценить снизу предел вероятности $P(X > t(n))$.

Теорема 3. *Пусть* $r < r_k$, $t(n) = cn$, *где* c *– константа,* $c < e^{-kr}$. *Тогда вероятность того, что множество* $N_{F_k(n,rn)}$ *состоит из граней размерности не меньше* $t(n)$, *ограничена снизу величиной, стремящейся к* $(1-ce^{kr})^2$.

Доказательство. Подставляя $t(n) = c/n$ в (4), получим

$$P(X > t(n)) \geq \frac{\left(\left(1-\frac{k}{n}\right)^{rn}-c\right)^2}{\frac{1}{n}\left(1-\frac{k}{n}\right)^{rn}+\left(1-\frac{1}{n}\right)\left(1-\frac{2k}{n}+\frac{k}{n}\frac{k-1}{n-1}\right)^{rn}}.$$

Но

$$\frac{\left(\left(1-\frac{k}{n}\right)^{rn}-c\right)^2}{\frac{1}{n}\left(1-\frac{k}{n}\right)^{rn}+\left(1-\frac{1}{n}\right)\left(1-\frac{2k}{n}+\frac{k}{n}\frac{k-1}{n-1}\right)^{rn}} \to \frac{(e^{-kr}-c)^2}{e^{-2kr}} = (1-ce^{kr})^2.$$

■

Исследуем поведение вероятности присутствия грани размерности ns в множестве выполняющих наборов случайной формулы. Напомним, что были сделаны следующие предположения о множестве выполняющих наборов случайной формулы.

Предположение 1. *(О пороге выполнимости, Chvatal, Reed, [6]) Для любого $k \geq 2$ существует такое r_k, что*

если $r < r_k$, то $F_k(n, rn)$ выполнима с высокой вероятностью,

если $r > r_k$, то $F_k(n, rn)$ не выполнима с высокой вероятностью.

Предположение 2. *(О пороге x-выполнимости, Mezard, Mora, Zecchina, [7]) Будем называть формулу x-выполнимой, если у нее есть два выполняющих набора с расстоянием nx. Тогда для любого $k \geq 2$ и для любого x, $0 < x < 1$, существует такое $r_k(x)$, что*

если $r < r_k(x)$, то $F_k(n, rn)$ x-выполнима с высокой вероятностью,

если $r > r_k(x)$, то $F_k(n, rn)$ не x-выполнима с высокой вероятностью.

(Заметим, что x-выполнимость эквивалентна выполнимости при $x = 0$.)

Более слабые результаты были позднее экспериментально проверены и доказаны.

Сделаем аналогичное предположение о присутствии граней размерности ns в множестве $N_{F_k(n,rn)}$.

Предположение 3. *(О пороге присутствия граней) Для любого $k \geq 2$ и для любого s, $0 < s < 1$, существует такое $r_k(s)$, что*

если $r < r_k(s)$, то с высокой вероятностью в $N_{F_k(n,rn)}$ найдется грань размерности ns,

если $r > r_k(s)$, то с высокой вероятностью в $N_{F_k(n,rn)}$ отсутствуют грани размерности ns.

3 Порог присутствия граней

Следующая теорема – аналог теоремы 1 для граней размерности ns.

Теорема 4. *Для всех* $k \geq 2$ *и* $s \in (0,1)$ *существует такая последовательность* $r_{k,s}(n)$, *что для любого* $\epsilon > 0$

$$\lim_{n\to\infty} P(\exists\sigma \in G_{ns}^n : \sigma \subset N_{F_k(n,rn)}) = \begin{cases} 1, & \text{\textit{если} } r = (1-\epsilon)r_{k,s}(n) \\ 0, & \text{\textit{если} } r = (1+\epsilon)r_{k,s}(n). \end{cases} \tag{5}$$

Для доказательства этой теоремы мы применим подход, использованный в работе [4] для выполнимости и в работе [7] для x-выполнимости. Прежде всего, требуется ввести новую вероятностную меру для формул. Число скобок в случайной формуле $F_k(n,rn)$ зафиксировано и равно rn. Пусть $G_k(n,rn)$ – случайная формула, полученная следующим образом. Выберем независимо каждую из $\mathcal{N} = 2^k C_n^k$ скобок с вероятностью $p = rn/\mathcal{N}$, и составим формулу из конъюнкции выбранных скобок. Число скобок формулы $G_k(n,rn)$ распределено согласно биномиальному распределению $\mathrm{Bin}(\mathcal{N}, rn/\mathcal{N})$, максимум функции вероятности достигается в точке математического ожидания, rn. Доказательство теоремы опирается на следующую лемму.

Лемма 3. *Для всех* $k \geq 2$ *и* $s \in (0,1)$ *существует такая последовательность* $r_{k,s}(n)$, *что для любого* $\epsilon > 0$

$$\lim_{n\to\infty} P(\exists\sigma \in G_{ns}^n : \sigma \subset N_{G_k(n,rn)}) = \begin{cases} 1, & \text{\textit{если} } r = (1-\epsilon)r_{k,s}(n) \\ 0, & \text{\textit{если} } r = (1+\epsilon)r_{k,s}(n). \end{cases} \tag{6}$$

Перед тем, как доказывать лемму, убедимся, что из нее следует теорема 4, аналогично тому, как это было сделано в работах [4] и [7] для выполнимости и x-выполнимости. Пусть выполнено (6). Обозначим $P(\exists\sigma \in G_{ns}^n : \sigma \subset N_{F_k(n,rn)})$ через $f_k(n,rn)$, $P(\exists\sigma \in G_{ns}^n : \sigma \subset N_{G_k(n,rn)})$ через $g_k(n,rn)$. Пусть $\epsilon > 0$, $0 < s < 1$ и $k \geq 2$. Заметим, что для любой k-КНФ F условная вероятность $P\left(G_k(n,rn) = F \middle| |G_k(n,rn)| = |F|\right)$ равна вероятности $P(F_k(n,|F|) = F)$ (где $|F|$ – число скобок в формуле F). А значит, по формуле полной вероятности

$$g_k(n,(r-\epsilon/2)n) = \sum_m f_k(n,m)\mathrm{Bin}(\mathcal{N},(r-\epsilon/2)n/\mathcal{N})(m). \tag{7}$$

Здесь $\mathrm{Bin}(\mathcal{N},(r-\epsilon/2)n/\mathcal{N})(m)$ – вероятность того, что случайная величина с распределением $\mathrm{Bin}(\mathcal{N},(r-\epsilon/2)n/\mathcal{N})$ равна m.

Воспользуемся тем фактом, что основной вклад в сумму дают слагаемые в окрестности математического ожидания числа скобок, $(r-\epsilon/2)n$.

$$g_k(n,(r-\epsilon/2)n) = \sum_{(r-\epsilon)n<m<rn} f_k(n,m)\mathrm{Bin}(\mathcal{N},(r-\epsilon/2)n/\mathcal{N})(m) + o(1). \tag{8}$$

Функция $f_k(n,rn)$ убывает по r. А значит,

$$g_k(n,(r-\epsilon/2)n) \le f_k(n,(r-\epsilon)n) + o(1). \tag{9}$$

Подставляя $r = r_{k,s}(n)$, получим первую часть теоремы:

$$\lim_{n\to\infty} f_k(n,(r_{k,s}(n)-\epsilon)n) = 1.$$

Вторая часть получается аналогично.

Докажем лемму 3, следуя рассуждениям, приведенным в [4] и [7]. В работе [4] Friedgut получил условия наличия „размытого порога`` для свойств случайных формул. В приложении к работе [4] Bourgain получил немного другое условие, которое было использовано в работе [7] и лучше подойдет для наших целей. Для того, чтобы применить это условие, нам потребуются следующие обозначения.

Подмножество („свойство``) A множества $\{0,1\}^{\mathcal{N}}$ ($\mathcal{N} = 2^k C_n^k$) называется монотонным, если для любых $F, F' \in \{0,1\}^{\mathcal{N}}$ из $F \le F'$ и $F \in A$ следует $F' \in A$. Пусть вероятностная мера на $\{0,1\}^{\mathcal{N}}$, μ_p, задана как произведение мер: вероятность единицы равна p, вероятность нуля равна $1-p$. Построим взаимно однозначное соответствие между множеством всех k-КНФ на n переменных и множеством $\{0,1\}^{\mathcal{N}}$ (1 соответствует вхождению скобки в формулу, 0 соответствует отсутствию скобки, всего есть $\mathcal{N} = 2^k C_n^k$ возможных скобок). В нашем случае свойство A означает отсутствие в $N_{G_k(n,rn)}$ граней размерности ns. Ясно, что это свойство монотонно. Кроме того,

$$\mu_p(A) = 1 - g_k(n,rn) \quad \text{при } p = rn/\mathcal{N}.$$

Теорема 5. *[Bourgain] Пусть $A \subset \{0,1\}^{\mathcal{N}}$ – монотонное свойство, и пусть*

$$\mu_p(A) = \frac{1}{2}, \tag{10}$$

$$p\,\frac{d\mu_p(A)}{dp} < C, \tag{11}$$

$$p = o(1). \tag{12}$$

Тогда существует такое $\delta = \delta(C)$, *что либо*

$$\mu_p(F \in \{0,1\}^{\mathcal{N}} \textit{ содержит } F' \in A \textit{ размера } |F'| \leq 10C) > \delta, \tag{13}$$

либо существует такая формула $F' \notin A$ *размера* $|F'| \leq 10C$, *что условная вероятность*

$$\mu_p(F \textit{ принадлежит } A | F \textit{ содержит } F') > \frac{1}{2} + \delta. \tag{14}$$

Кроме того, в (10) *и* (14) *можно заменить* $1/2$ *на любое* $\alpha \in (0,1)$.

Ясно, что $\mu_0(A) = 0$. С помощью неравенства Маркова нетрудно показать, что $\mu_{p^*}(A) = 1 + o(1)$, где $p^* = 2^k n \ln 2/\mathcal{N}$. Значение $\mu_p(A)$ непрерывно возрастает с ростом p. Следовательно, существует такое $p \leq p^* = o(1)$, что $\mu_p(A) = 1/2$. Таким образом, условия (10) и (12) выполнены. Условие (11) выполнено для всех достаточно больших n (при C, не зависящем от n) тогда и только тогда, когда порог для свойства A „размыт`` и лемма 3 не верна. А значит, для доказательства леммы 3 надо доказать, что для любых C и $\delta(C)$ при достаточно больших n утверждения (13) и (14) всегда ложны.

Докажем невозможность (13). Пусть свойство $B \subset \{0,1\}^{\mathcal{N}}$ соответствует множеству невыполнимых формул. Ясно, что $\mu_p(B) \leq \mu_p(A)$ (так как если в множестве выполняющих наборов формулы есть грань размерности ns, то формула выполнима). В [4] было доказано, что при $\mu_p(B) \leq 1/2$ в F с высокой вероятностью нет невыполнимых подформул размера не больше $10C$. Заметим, что в подформулу $F', |F'| \leq 10C$, не входят как минимум $n - 10Ck$ из n переменных, а значит если F' выполнима, то выбрав выполняющий набор и присваивая переменным, не вошедшим в F', произвольные значения, получим грань размерности не менее $n - 10Ck$, что больше ns при достаточно большом n. Следовательно, с высокой вероятностью в F не существует подформулы F', принадлежащей A, размера не более $10C$, и неравенство (13) не выполняется.

Остается доказать невозможность (14), то есть доказать, что не существует „маленькой`` формулы (размера не более $10C$), присутствие которой увеличивает вероятность того, что F принадлежит множеству A, на константу. Предположим, что такая формула F' существует. Пусть V' – множество переменных, входящих в F', $|V'| \leq 10Ck$. Нам понадобится множество переменных V, такое, что $V' \subset V$ и $|V| = v(n)$, где $v(n) = n^{\frac{1}{16(k+1)}}$ (такой выбор функции $v(n)$ будет объяснен при доказательстве леммы 6). Пусть каждая из $\mathcal{N}$ скобок входит в F независимо с вероятностью p (а значит, $\mu_p(F \in A) = 1/2$). Представим формулу F в виде конъюнкции формул F_1 и F_2, где в F_1 входят скобки из F, содержащие хотя бы одну переменную из V, а в F_2 – остальные скобки из F.

Сначала оценим размер F_1.

Лемма 4. *Существует такая константа C_1, что с высокой вероятностью $|F_1| \leq C_1 v(n)$.*

Доказательство. Заметим, что случайная величина $|F_1|$ распределена по биномиальному закону $\mathrm{Bin}(2^k C_n^k - 2^k C_{n-v(n)}^k, p)$, так как число скобок, содержащих хотя бы одну переменную из V, равно $2^k C_n^k - 2^k C_{n-v(n)}^k$. А значит,

$$M(|F_1|) = p2^k(C_n^k - C_{n-v(n)}^k).$$

Поскольку $p \leq 2^k n \ln 2/\mathcal{N} = n \ln 2/C_n^k$,

$$M(|F_1|) \leq 2^k n \ln 2 \left(1 - \frac{C_{n-v(n)}^k}{C_n^k}\right) \leq$$

$$\leq 2^k n \ln 2 \left(1 - \left(\frac{n-k-v(n)+1}{n-k+1}\right)^k\right) =$$

$$= 2^k n \ln 2 \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k\right). \tag{15}$$

Вычислим предел

$$\lim_{n\to\infty} \frac{n}{v(n)} \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k\right).$$

Обозначим $-\frac{v(n)}{n-k+1}$ через x. Известно, что

$$\lim_{x\to 0} \frac{(1+x)^k - 1}{x} = k,$$

а значит

$$\lim_{n\to\infty} \frac{n-k+1}{v(n)} \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k\right) = k,$$

и

$$\lim_{n\to\infty}\frac{n}{v(n)}\left(1-\left(1-\frac{v(n)}{n-k+1}\right)^k\right)=k.$$

Следовательно, существует такая константа c_2, что при достаточно большом n

$$n\left(1-\left(1-\frac{v(n)}{n-k+1}\right)^k\right)\leq c_2kv(n).$$

Тогда из (15) следует, что

$$M(|F_1|)\leq 2^k\ln 2c_2kv(n)=c_3v(n).$$

Кроме того, из свойств биномиального распределения следует, что

$$D(|F_1|)=(1-p)M(|F_1|)\leq M(|F_1|).$$

Тогда по неравенству Чебышева

$$P(|F_1|\geq 2M(|F_1|))\leq\frac{D(|F_1|)}{M(|F_1|)^2}\leq\frac{1}{M(|F_1|)}\to 0 \text{ при } n\to\infty.$$

А значит, с высокой вероятностью $|F_1|<2M(|F_1|)\leq 2c_3v(n)=C_1v(n)$ (где $C_1=2c_3$), что и требовалось доказать. ■

Лемма 5. *С высокой вероятностью, каждая из скобок F_1 содержит ровно одну переменную из V.*

Доказательство. Обозначим множество скобок из F_1, содержащих хотя бы две переменные из V, через F_1''. Общее число возможных скобок, содержащих ровно одну переменную из V, равно $2^kv(n)C_{n-v(n)}^{k-1}$, а значит, случайная величина $|F_1''|$ распределена по биномиальному закону $\mathrm{Bin}(2^kC_n^k-2^kC_{n-v(n)}^k-2^kv(n)C_{n-v(n)}^{k-1},p)$. Оценим вероятность $|F_1''|>0$ с помощью неравенства Маркова.

$$M(|F_1''|)=p2^k(C_n^k-C_{n-v(n)}^k-v(n)C_{n-v(n)}^{k-1}).$$

Поскольку $p\leq 2^kn\ln 2/\mathcal{N}=n\ln 2/C_n^k$, а $C_{n-v(n)}^{k-1}=C_{n-v(n)}^k\frac{k}{n-v(n)-k+1}$,

$$M(|F_1''|)\leq 2^kn\ln 2\left(1-\frac{C_{n-v(n)}^k}{C_n^k}\left(1+\frac{kv(n)}{n-v(n)-k+1}\right)\right)\leq$$

$$\leq 2^kn\ln 2\left(1-\left(\frac{n-k-v(n)+1}{n-k+1}\right)^k\left(1+\frac{kv(n)}{n-k+1}\right)\right)=$$

$$= 2^k n \ln 2 \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k \left(1 + \frac{kv(n)}{n-k+1}\right)\right). \qquad (16)$$

Обозначим $\frac{v(n)}{n-k+1}$ через x и заметим, что

$$\lim_{x \to 0} \frac{1-(1-x)^k(1+kx)}{x^2} = \frac{1}{2}k(1-k).$$

(Это нетрудно показать например дважды применив правило Лопиталя). Тогда

$$\lim_{n \to \infty} \frac{(n-k+1)^2}{v(n)^2} \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k \left(1 + \frac{kv(n)}{n-k+1}\right)\right) = \frac{1}{2}k(1-k),$$

а значит ---

$$\lim_{n \to \infty} \frac{n^2}{v(n)^2} \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k \left(1 + \frac{kv(n)}{n-k+1}\right)\right) = \frac{1}{2}k(1-k),$$

и существует такая константа c_4, что при достаточно большом n

$$n \left(1 - \left(1 - \frac{v(n)}{n-k+1}\right)^k \left(1 + \frac{kv(n)}{n-k+1}\right)\right) \leq c_4 \frac{v(n)^2}{n}.$$

Из (16) следует, что

$$M(|F_1''|) \leq 2^k \ln 2 c_4 \frac{v(n)^2}{n} \to 0 \text{ при } v(n) = o(\sqrt{n}).$$

По неравенству Маркова, с высокой вероятностью $|F_1''| = 0$, что и требовалось доказать. ■

Будем говорить, что в формуле присутствует грань размерности ns, если такая грань найдется в множестве выполняющих наборов формулы. Рассмотрим формулу G_1, полученную с помощью случайного, равновероятного и независимого выбора $C_1 v(n)$ скобок размера $k-1$. Позднее мы заменим F_1 на G_1. Пока что докажем, что добавление G_1 в формулу не может увеличить вероятность отсутствия в формуле грани размерности ns более чем на $\delta/2$. Фактически мы докажем более сильное утверждение: даже если G_1 состоит из $C_1 v(n)$ однобуквенных скобок, добавление G_1 в формулу не может увеличить вероятность отсутствия в формуле грани размерности ns более чем на $\delta/2$.

Пусть $f(n)$ стремится к бесконечности при n, стремящемся к бесконечности, но $f(n) = o(\sqrt{n})$. Для определенности выберем $f(n) = n^{1/4}$. Согласно лемме 5.6 из [4], добавление $f(n)$ скобок длины k в формулу не может увеличить вероятность выполнения какого-либо монотонного свойства более чем на $\delta/2$. Следовательно, добавление $f(n)$ скобок длины k в формулу не может увеличить вероятность отсутствия в формуле грани размерности ns более чем на $\delta/2$. Докажем, что добавление $C_1v(n)$ однобуквенных скобок не может увеличить эту вероятность больше, чем добавление $f(n)$ скобок длины k. Аналогичные утверждения были доказаны для выполнимости (лемма 5.7 из [4]) и для x-выполнимости (лемма 4 из [7]).

Лемма 6. *Пусть $S \subset G^n_{ns}$. Будем говорить, что формула F покрывает множество S, если все грани из S отсутствуют в N_F. Будем говорить, что S является (d, k, ϵ)-покрываемым, если случайная k-КНФ с d скобками покрывает S с вероятностью по крайней мере ϵ. Пусть $f(n) = n^{1/4}$. Тогда для любых фиксированных k и ϵ при достаточно большом n любое множество $S \subset G^n_{ns}$, являющееся $(C_1v(n), 1, \epsilon)$-покрываемым, является также $(f(n), k, \epsilon)$-покрываемым.*

Доказательство. Пусть S является $(C_1v(n), 1, \epsilon)$-покрываемым. Это значит, что случайная формула, полученная последовательным выбором $C_1v(n)$ однобуквенных скобок, покрывает S с вероятностью по крайней мере ϵ. Мы докажем, что если заменить последнюю однобуквенную скобку на $\sqrt{f(n)}/C_1v(n)$ скобок длины k, то вероятность покрытия S не может уменьшиться более чем на $\epsilon/2C_1v(n)$. От порядка добавления скобок в формулу вероятность покрытия не меняется, а значит, можно сначала выбрать $\sqrt{f(n)}/C_1v(n)$ скобок длины k, а затем – $C_1v(n) - 1$ однобуквенных скобок. Повторив замену однобуквенной скобки на $\sqrt{f(n)}/C_1v(n)$ скобок длины k $C_1v(n)$ раз, получим $\sqrt{f(n)}$ скобок длины k, при этом вероятность покрытия S не может уменьшиться более чем на $C_1v(n)\epsilon/2C_1v(n) = \epsilon/2$. Таким образом, множество S является $(\sqrt{f(n)}, k, \epsilon/2)$-покрываемым. Тогда построим случайную формулу, $\sqrt{f(n)}$ раз выбрав $\sqrt{f(n)}$ скобок длины k. Вероятность того, что такая формула покрывает S, не меньше $1 - (1 - \epsilon/2)^{\sqrt{f(n)}} \geq \epsilon$ (при достаточно большом n). Следовательно, S является $(f(n), k, \epsilon)$-покрываемым.

Осталось доказать, что при замене последней однобуквенной скобки на $\sqrt{f(n)}/C_1v(n)$ скобок длины k вероятность покрытия не может уменьшиться более чем на $\epsilon/2C_1v(n)$. В случае, если до замены вероятность покрытия была не больше $\epsilon/2C_1v(n)$, доказывать нечего (даже если после замены вероятность покрытия станет равна нулю, она уменьшится не более чем на $\epsilon/2C_1v(n)$). Рассмотрим случай, когда вероятность покрытия до замены равна $\alpha(n) > \epsilon/2C_1v(n)$. Достаточно доказать, что если множество S' является $(1,1,\alpha(n))$-покрываемым, то оно является $(\sqrt{f(n)}/C_1v(n), k, \alpha(n))$-покрываемым (а значит, при замене вероятность покрытия вообще не уменьшится).

Заметим, что однобуквенная скобка x_i^σ покрывает множество S' тогда и только тогда, когда в коде каждой грани из S' координата с номером i не равна σ. Следовательно, для того, чтобы скобка x_i^σ могла покрыть множество S', необходимо, чтобы в кодах граней из S' координаты с номером i принадлежали множеству $\{\bar{\sigma}, -\}$ (т.е. или $\{0,-\}$ или $\{1,-\}$). Для того, чтобы S' было $(1,1,\alpha(n))$-покрываемым, необходимо, чтобы число таких i было не меньше $n\alpha(n)$. Но тогда k-буквенная скобка покрывает S' с вероятностью не меньше $2^{-k}C^k_{n\alpha(n)}/C^k_n \geq c \times \alpha(n)^k$, где c – константа, не зависящая от n. Значит, вероятность того, что $\sqrt{f(n)}/C_1v(n)$ скобок длины k покрывают S', не меньше

$$1 - \left(1 - c\alpha(n)^k\right)^{\frac{\sqrt{f(n)}}{C_1v(n)}} > 1 - \left(1 - c\left(\frac{\epsilon}{2C_1v(n)}\right)^k\right)^{\frac{\sqrt{f(n)}}{C_1v(n)}},$$

а это выражение стремится к единице, если $v(n)^k = o(\sqrt{f(n)}/v(n))$, т.е. если $v(n)^{k+1} = o(\sqrt{f(n)})$, или, что то же самое, $v(n) = o(f(n)^{\frac{1}{2(k+1)}})$. Это условие выполнено при $v(n) = n^{\frac{1}{16(k+1)}}$ и $f(n) = n^{1/4}$. ∎

Напомним, что в формулу F каждая из $\mathcal{N}$ скобок входит независимо с вероятностью p, а значит, согласно (10), $\mu_p(F$ принадлежит $A) = 1/2$. Из леммы 6 следует, что добавление в F $C_1v(n)$ случайных однобуквенных скобок не может увеличить вероятность отсутствия в формуле грани размерности ns сильнее, чем добавление $f(n)$ скобок длины k. При этом добавление $f(n)$ скобок длины k в формулу не может увеличить вероятность отсутствия в формуле грани размерности ns более чем на $\delta/2$. Следовательно, добавление в F $C_1v(n)$ однобуквенных скобок может увеличить эту вероятность не более чем на $\delta/2$. Ясно, что если заменить однобуквенные скобки на скобки длины $k-1$, то вероятность не может увеличиться. Следовательно, вероятность присутствия в формуле $F \wedge G_1$ грани размерности ns не меньше $1/2 - \delta/2$. Рассмотрим случай, когда такие грани присутствуют в $F \wedge G_1$. Выберем одну такую грань случайно и равновероятно. Нетрудно видеть, что выбор грани не зависит от выбора множества V.

Лемма 7. *Рассмотрим случай, когда в $F \wedge G_1$ присутствуют грани размерности ns. Выберем одну такую грань τ случайно и равновероятно. Пусть $T(\tau)$ – число прочерков в коде грани τ, соответствующих переменным из V ($T(\tau) = \sum_{i=1}^{n} 1_{\tau_i=-,x_i\in V}$). Тогда с высокой вероятностью $T(\tau) \le v(n) - 10Ck$.*

Доказательство. Так как выбор грани не зависит от выбора множества V, каждая грань из множества G^n_{ns} может быть выбрана с равной вероятностью. Таким образом, грань τ получена в результате случайного равновероятного выбора из множества G^n_{ns}.

Найдем число граней σ из G^n_{ns}, таких, что $T(\sigma) = t$. Есть $C^t_{v(n)} C^{ns-t}_{n-v(n)}$ способов выбрать ns координат, равных $-$, и $2^{(1-s)n}$ способов зафиксировать остальные координаты. Тогда число таких граней, что $T(\sigma) = t$, равно $2^{(1-s)n} C^t_{v(n)} C^{ns-t}_{n-v(n)}$, и

$$P(T(\tau) = t) = \frac{2^{(1-s)n} C^t_{v(n)} C^{ns-t}_{n-v(n)}}{2^{(1-s)n} C^{ns}_n} = \frac{C^t_{v(n)} C^{ns-t}_{n-v(n)}}{C^{ns}_n}.$$

Обозначим $10Ck$ через K. Требуется доказать, что $P(T(\tau) > v(n) - K) = o(n)$. Ясно, что

$$P(T(\tau) > v(n) - K) = \sum_{t=v(n)-K+1}^{v(n)} P(T(\tau) = t).$$

Так как при достаточно большом n вероятность $P(T(\tau) = t)$ убывает на $[v(n) - K + 1, v(n)]$,

$$\sum_{t=v(n)-K+1}^{v(n)} P(T(\tau) = t) \le KP(T(\tau) = v(n) - K + 1) =$$

$$= K \frac{C^{v(n)-K+1}_{v(n)} C^{ns-v(n)+K-1}_{n-v(n)}}{C^{ns}_n} \le$$

$$\le K \frac{v(n)^K}{K!} \frac{(n - v(n))!}{n!} \frac{(ns)!}{(ns - v(n) + K)!} \frac{(n - ns)!}{(n - ns - K)!} \le$$

$$\leq K\frac{v(n)^K}{K!}\frac{1}{(n-v(n))^{v(n)}}(ns)^{v(n)-K}(n-ns)^K =$$

$$= \frac{v(n)^K}{(K-1)!}\left(\frac{n}{n-v(n)}\right)^{v(n)} s^{v(n)-K}(1-s)^K.$$

При n, стремящемся к бесконечности, $v(n)^K s^{v(n)-K}$ стремится к нулю, а $\left(\frac{n}{n-v(n)}\right)^{v(n)}$ стремится к единице. Следовательно,

$$\frac{v(n)^K}{(K-1)!}\left(\frac{n}{n-v(n)}\right)^{v(n)} s^{v(n)-K}(1-s)^K = o(n),$$

и $P(T(\tau) > v(n) - K) = o(n)$, а значит, с высокой вероятностью $T(\tau) \leq v(n) - 10Ck$, что и требовалось доказать. ■

Итак, в $F \wedge G_1$ присутствуют грани размерности ns с вероятностью по крайней мере $1/2 - \delta/2$. Если такие грани присутствуют, то с высокой вероятностью хотя бы в одной из граней менее $v(n) - 10Ck$ прочерков попадают в множество V (то есть более $ns - v(n) + 10Ck$ прочерков не попадут в это множество). Удалим из $F \wedge G_1$ подформулу F_1, то есть все скобки F, содержащие переменные из V. Останется формула $F_2 \wedge G_1$, в которой с высокой вероятностью нет переменных из V. Тогда если грань σ содержится в $F_2 \wedge G_1$, то заменяя в коде σ все координаты, соответствующие множеству V, на прочерки, получим грань σ' размерности по крайней мере $ns + 10Ck$, содержащуюся в $F_2 \wedge G_1$. Добавим подформулу F'. Все ее переменные содержатся в V, F' выполнима и содержит не более $10Ck$ переменных. Заменим в коде грани σ' прочерки, соответствующие переменным из F', на нули и единицы таким образом, чтобы получившаяся грань σ'' содержалась в F'. Это можно сделать, так как F' выполнима. Размерность грани при этом уменьшится не более чем на $10Ck$, а значит, размерность σ'' не меньше ns. Грань σ'' содержится в F' и в $F_2 \wedge G_1$, а значит, σ'' содержится и в $F' \wedge F_2 \wedge G_1$. Итак, при достаточно больших n в $F' \wedge F_2 \wedge G_1$ есть грань размерности ns с вероятностью не меньше $1/2 - 3\delta/4$. Заметим, что формула $F' \wedge F_2 \wedge G_1$ получена из формулы $F' \wedge F$ заменой подформулы F_1 на G_1. Для того, чтобы применить теорему 5, осталось доказать, что при такой замене вероятность присутствия в формуле грани размерности ns не могла вырасти на $\delta/4$.

Пусть U – событие „каждая скобка из F_1 содержит ровно одну переменную из V, все скобки из G_1 не содержат переменных из V и

$|F_1| \leq C_1 v(n)$``. Согласно леммам 4 и 5, $U$ выполнено с высокой вероятностью. Пусть $A_F$ – событие „в $F' \wedge F$ есть грань размерности $ns$``, A_G – событие „в $F' \wedge F_2 \wedge G_1$ есть грань размерности ns``. По формуле полной вероятности

$$P(A_F) = P(A_F|U)P(U) + P(A_F|\bar{U})P(\bar{U}), \tag{17}$$

$$P(A_G) = P(A_G|U)P(U) + P(A_G|\bar{U})P(\bar{U}). \tag{18}$$

Пусть B_t – событие „$|F_1| = t$``. Тогда по формуле полной вероятности

$$P(A_F|U) = \sum_{t=0}^{C_1 v(n)} P(A_F|U \cap B_t)P(B_t|U).$$

Нетрудно видеть, что при увеличении числа скобок вероятность присутствия в формуле грани размерности ns уменьшается, а значит

$$P(A_F|U) \geq \sum_{t=0}^{C_1 v(n)} P(A_F|U \cap B_{C_1 v(n)})P(B_t|U) = P(A_F|U \cap B_{C_1 v(n)}). \tag{19}$$

Сравним вероятности $P(A_F|U \cap B_{C_1 v(n)})$ и $P(A_G|U)$. Выбор G_1 при условии U равнозначен равновероятному выбору формулы из $C_1 v(n)$ скобок размера $k-1$, не содержащих переменных из V. Выбор F_1 при условии $U \cap B_{C_1 v(n)}$ равнозначен равновероятному выбору формулы из $C_1 v(n)$ скобок размера $k-1$, не содержащих переменных из V, и добавлению в каждую скобку случайной буквы из V. Поскольку добавление букв в скобку может только увеличить вероятность отсутствия граней, $P(A_F|U \cap B_{C_1 v(n)}) \geq P(A_G|U)$, и из (19) следует, что $P(A_F|U) \geq P(A_G|U)$. Заметим, что поскольку вероятность события U стремится к единице, $P(\bar{U}) < \delta/16$ при достаточно больших n. Но тогда из (17) и (18) следует, что $P(A_F) > P(A_G) - \delta/8$. Так как $P(A_G) \geq 1/2 - 3\delta/4$, это означает, что $P(A_F) > 1/2 - 7\delta/8$, и условие (14) не может быть выполнено. Из теоремы 5 следует, что условие (11) не выполнено ни при каких C. Согласно [4], это эквивалентно наличию у монотонного свойства A „четкого`` порога, а значит лемма 3 доказана. Как было показано выше, из леммы 3 следует теорема 4.

Теорема 4 в частности означает, что верен аналог следствия 1 для граней.

Следствие 2. *Зафиксируем $s \in (0,1)$, $r > 0$, $k \geq 3$. Если существует такая константа C, что вероятность присутствия в $N_{F_k(n,rn)}$ грани размерности ns больше C при любом n, то эта вероятность стремится к единице при n, стремящемся к бесконечности.*

Но по теореме 3 при $s < e^{-kr}$ и $r < r_k$ вероятность присутствия грани размерности ns ограничена снизу величиной, стремящейся к $(1 - se^{kr})^2 > 0$.

Следствие 3. *При $s < e^{-kr}$ и $r < r_k$ в $N_{F_k(n,rn)}$ с высокой вероятностью присутствует грань размерности ns.*

Для того, чтобы оценить вероятность присутствия в $N_{F_k(n,rn)}$ грани размерности s при $s \geq e^{-kr}$, воспользуемся методом вторых моментов. Это будет обобщением подхода, примененного в работе [3].

4 Метод вторых моментов напрямую неприменим

Естественно начать исследование применимости метода вторых моментов с рассмотрения случайной величины, равной числу граней размерности ns в $N_{F_k(n,rn)}$.

$$X = \sum_{\sigma \in G^n_{ns}} 1_{\sigma \subset N_{F_k(n,rn)}},$$

где G^n_{ns} – множество граней размерности ns n-мерного куба. Мы будем использовать метод вторых моментов в виде леммы 1. Из леммы следует, что если для некоторого r существует такая положительная константа C, что для всех n выполняется неравенство $M^2(X)/M(X^2) > C$, то вероятность присутствия грани размерности ns в $N_{F_k(n,rn)}$ не меньше C. В этом случае согласно следствию 2 в $N_{F_k(n,rn)}$ с высокой вероятностью присутствует грань размерности ns. Аналогичный подход был рассмотрен, например, в работе [2] для случайной величины $|N_{F_k(n,rn)}|$.

Из независимости скобок и линейности математического ожидания следует, что

$$M(X) = \sum_{\sigma \in G^n_{ns}} P(\sigma \subset N_{F_k(n,rn)}) = 2^{(1-s)n} C_n^{ns} P(\sigma \subset N_{F_k(n,rn)}) =$$

$$= 2^{(1-s)n} C_n^{ns} (P(\sigma \subset N_c))^{rn}, \tag{20}$$

где N_c – множество выполняющих наборов некоторой k-буквенной скобки c.

Пусть $A = \{0, 1, -\}^k$ – множество векторов, σ – некоторая грань размерности ns. Пусть $c = x_{i_1}^{\delta_1} \vee x_{i_2}^{\delta_2} \vee \ldots \vee x_{i_k}^{\delta_k}$ – случайная скобка. Определим вектор $u \in A$ следующим образом: если $\sigma_{i_j} = -$, то $u_j = -$, если $\sigma_{i_j} \neq -$, то $u_j = \sigma_{i_j}^{\delta_j}$. Тогда вектор u описывает поведение скобки c на множестве наборов из грани σ. В частности, $\sigma \subset N_c$ тогда и только тогда, когда в u есть хотя бы одна единица. Обозначим число единиц в u через $|u|$. Тогда

$$P(\sigma \subset N_c) = 1 - P(\sigma \not\subset N_c) = 1 - P(|u| = 0) = 1 - (P(u_j \neq 1))^k.$$

$u_j \neq 1$ тогда и только тогда, когда $\sigma_{i_j} = -$ или $\sigma_{i_j} \neq \delta_j$. Вероятность такого события равна $s + \frac{1-s}{2} = \frac{1+s}{2}$. Следовательно,

$$P(\sigma \subset N_c) = 1 - \left(\frac{1+s}{2}\right)^k,$$

и из (20) получаем

$$M(X) = 2^{(1-s)n} C_n^{ns} \left(1 - \left(\frac{1+s}{2}\right)^k\right)^{rn}. \tag{21}$$

Для применения метода вторых моментов необходимо оценить $M(X^2)$.

$$M(X^2) = M\left(\left(\sum_{\sigma \in G_{ns}^n} 1_{\sigma \subset N_{F_k(n,rn)}}\right)^2\right) = M\left(\sum_{\sigma,\tau \in G_{ns}^n} 1_{\sigma,\tau \subset N_{F_k(n,rn)}}\right) =$$

$$= \sum_{\sigma,\tau \in G_{ns}^n} P(\sigma, \tau \subset N_{F_k(n,rn)}) = \sum_{\sigma,\tau \in G_{ns}^n} P(\sigma, \tau \subset N_c)^{rn}. \tag{22}$$

Рассмотрим пару граней σ и τ размерности ns. Исследуем вероятность того, что они обе принадлежат множеству N_c (или, что то же самое, они не пересекаются с гранью, соответствующей скобке c). Без ограничения общности, пусть код грани σ имеет вид $(00\ldots0--\ldots-)$. Пусть $z_1, z_2, z_3, z_3', z_3'', z_4$ – количество пар (σ_i, τ_i) различных типов, как указано в таблице:

	z_1	z_2	z_3	z_3'	z_3''	z_4
σ	0	0	0	–	–	–
τ	0	1	–	0	1	–

(Соответственно, если σ имеет другой вид, то z_1 – число таких пар (σ_i, τ_i), что $\sigma_i = \tau_i \neq -$, и так далее.) Заметим, что выполнены следующие условия:

$$\begin{cases} z_3 = z_3' + z_3'' \\ z_3 + z_4 = ns \\ z_1 + z_2 + z_3 + z_3' + z_3'' + z_4 = n. \end{cases}$$

Решив эту систему относительно z_2 и z_4, получим

$$\begin{cases} z_4 = ns - z_3 \\ z_2 = n - ns - z_1 - z_3. \end{cases} \tag{23}$$

Построим вектор u для σ так, как это было сделано выше. Построим вектор v для τ аналогичным образом. Заметим, что $\sigma, \tau \subset N_c$ тогда и только тогда, когда $|u| \geq 1$ и $|v| \geq 1$. Следовательно,

$$P(\sigma, \tau \subset N_c) = P(|u| \geq 1 \cap |v| \geq 1) = 1 - P(|u| = 0 \cup |v| = 0) =$$

$$= 1 - 2P(|u| = 0) + P(|u| = 0 \cap |v| = 0). \tag{24}$$

Значение $P(|u| = 0)$ получено выше и равно $\left(\frac{1+s}{2}\right)^k$.

Найдем значение $P(|u| = 0 \cap |v| = 0)$. Ясно, что

$$P(|u| = 0 \cap |v| = 0) = P(u_j \neq 1 \cap v_j \neq 1)^k. \tag{25}$$

Пусть $\alpha_1 = z_1/n, \alpha_2 = z_2/n, \alpha_3 = z_3/n, \alpha_4 = z_4/n$. Из (23) следует, что

$$\begin{cases} \alpha_2 = 1 - s - \alpha_1 - \alpha_3 \\ \alpha_4 = s - \alpha_3. \end{cases}$$

Обозначим событие $(u_j \neq 1 \cap v_j \neq 1)$ через B и вычислим его вероятность.

Рассмотрим следующие события:

- $A_1 = (\sigma_{i_j} = 0, \tau_{i_j} = 0)$. $P(A_1) = \alpha_1$. $P(B|A_1) = 1/2$.
- $A_2 = (\sigma_{i_j} = 0, \tau_{i_j} = 1)$. Нетрудно видеть, что $P(B|A_2) = 0$.
- $A_3 = (\sigma_{i_j} = 0, \tau_{i_j} = -) \cap (\sigma_{i_j} = -, \tau_{i_j} \neq -)$. $P(A_3) = 2\alpha_3$, $P(B|A_3) = 1/2$.

- $A_4 = (\sigma_{i_j} = -, \tau_{i_j} = -)$. $P(A_4) = \alpha_4$, $P(B|A_4) = 1$.

По формуле полной вероятности,

$$P(B) =$$

$$= P(B|A_1)P(A_1) + P(B|A_2)P(A_2) + P(B|A_3)P(A_3) + P(B|A_4)P(A_4) =$$

$$= \frac{\alpha_1}{2} + \alpha_3 + \alpha_4 = \frac{\alpha_1}{2} + s. \tag{26}$$

Сопоставляя (22), (24), (25) и (26), получим

$$M(X^2) = \sum_{\sigma,\tau \in G^n_{ns}} \left(1 - 2\left(\frac{1+s}{2}\right)^k + \left(\frac{\alpha_1}{2} + s\right)^k\right)^{rn}.$$

Обозначим

$$P(\sigma, \tau \subset N_c) = 1 - 2\left(\frac{1+s}{2}\right)^k + \left(\frac{\alpha_1}{2} + s\right)^k$$

через $f(\alpha_1)$. Тогда

$$M(X^2) = \sum_{\sigma,\tau \in G^n_{ns}} f(z_1/n)^{rn}.$$

Пусть заданы параметры z_1 и z_3, код грани σ имеет вид $(00\ldots0--\ldots-)$. Найдем число способов выбрать $\tau \in G^n_{ns}$. Сначала выберем, какие из пар (σ_i, τ_i) равны $(0, -)$. $n(1-s)$ координат кода σ равны 0, из их числа надо выбрать z_3 координат, всего $C^{z_3}_{n(1-s)}$ способов. Затем выберем, какие из пар (σ_i, τ_i) равны $(0,0)$. Для этого надо выбрать z_1 из $n(1-s) - z_3$ координат, всего $C^{z_1}_{n(1-s)-z_3}$ способов. Далее выберем, какие из пар (σ_i, τ_i) равны $(-,-)$. ns координат кода σ равны $-$, из их числа надо выбрать $z_4 = ns - z_3$ координат, всего $C^{ns-z_3}_{ns} = C^{z_3}_{ns}$ способов. Наконец для тех пар (σ_i, τ_i), в которых $\sigma_i = -, \tau_i \neq -$, надо выбрать значение τ_i. Число таких координат равно $z_3' + z_3'' = z_3$, каждая может принимать два значения, всего 2^{z_3} способов. Перемножая, получим $2^{z_3} C^{z_3}_{n(1-s)} C^{z_3}_{ns} C^{z_1}_{n(1-s)-z_3}$ способов выбора грани τ.

Таким образом,

$$M(X^2) = 2^{(1-s)n} C^{ns}_n \sum_{z_3=0}^{ns} 2^{z_3} C^{z_3}_{n(1-s)} C^{z_3}_{ns} \sum_{z_1=0}^{n(1-s)-z_3} C^{z_1}_{n(1-s)-z_3} f(z_1/n)^{rn}. \tag{27}$$

Известно, что $C_n^{\alpha n} = 2^{nH(\alpha)} \times \mathrm{poly}(n)$, где $H(\alpha) = -\alpha\log_2(\alpha) - (1-\alpha)\log_2(1-\alpha)$, а запись $p(n) = \mathrm{poly}(n)$ означает, что существуют такие константы $c_1, c_2 > 0$ и действительные константы d_1, d_2, что при достаточно больших n выполняется $c_1 n^{d_1} < p(n) < c_2 n^{d_2}$. Тогда

$$2^{(1-s)n} C_n^{ms} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f(z_1/n)^{rn} =$$
$$= 2^{(1-s)n} 2^{nH(s)} 2^{n\alpha_3} 2^{n(1-s)H\left(\frac{\alpha_3}{1-s}\right)} 2^{nsH\left(\frac{\alpha_3}{s}\right)} 2^{n(1-s-\alpha_3)H\left(\frac{\alpha_1}{1-s-\alpha_3}\right)} f(\alpha_1)^{rn} \times$$
$$\times \mathrm{poly}(n) =$$
$$= \left(2^{(1-s)} 2^{H(s)} 2^{\alpha_3} 2^{(1-s)H\left(\frac{\alpha_3}{1-s}\right)} 2^{sH\left(\frac{\alpha_3}{s}\right)} 2^{(1-s-\alpha_3)H\left(\frac{\alpha_1}{1-s-\alpha_3}\right)} f(\alpha_1)^r\right)^n \times$$
$$\times \mathrm{poly}(n) =$$
$$= (h(\alpha_1, \alpha_3) f(\alpha_1)^r)^n \times \mathrm{poly}(n),$$

где

$$h(\alpha_1, \alpha_3) \equiv 2^{(1-s)} 2^{H(s)} 2^{\alpha_3} 2^{(1-s)H\left(\frac{\alpha_3}{1-s}\right)} 2^{sH\left(\frac{\alpha_3}{s}\right)} 2^{(1-s-\alpha_3)H\left(\frac{\alpha_1}{1-s-\alpha_3}\right)}.$$

Из (27) следует, что

$$M(X^2) \geq \left(\max_{z_3 \in [0, ns], z_1 \in [0, n(1-s)-z_3]} h(\alpha_1, \alpha_3) f(\alpha_1)^r\right)^n \times \mathrm{poly}(n). \tag{28}$$

Заметим, что

$$f\left(\frac{(1-s)^2}{2}\right) = 1 - 2\left(\frac{1+s}{2}\right)^k + \left(\frac{(1-s)^2}{4} + s\right)^k =$$
$$= 1 - 2\left(\frac{1+s}{2}\right)^k + \left(\frac{(1+s)^2}{4}\right)^k = \left(1 - \left(\frac{1+s}{2}\right)^k\right)^2.$$

Тогда из (21) следует, что

$$M(X) = 2^{(1-s)n} C_n^{ms} f\left(\frac{(1-s)^2}{2}\right)^{\frac{rn}{2}} =$$
$$= 2^{(1-s)n} 2^{nH(s)} f\left(\frac{(1-s)^2}{2}\right)^{\frac{rn}{2}} \times \mathrm{poly}(n),$$

$$M(X)^2 = 2^{2(1-s)n}2^{2nH(s)}f\left(\frac{(1-s)^2}{2}\right)^{rn} \times \mathrm{poly}(n).$$

Но

$$h\left(\frac{(1-s)^2}{2}, s(1-s)\right) =$$

$$= 2^{(1-s)+H(s)+s(1-s)+(1-s)H(s)+sH(1-s)+(1-s-s(1-s))H(1/2)} = 2^{2(1-s)+2H(s)},$$

и

$$M(X)^2 = \left(h\left(\frac{(1-s)^2}{2}, s(1-s)\right)f\left(\frac{(1-s)^2}{2}\right)^r\right)^n \times \mathrm{poly}(n).$$

С учетом (28), это означает, что для применения метода вторых моментов необходимо, чтобы функция $h(\alpha_1, \alpha_3)f(\alpha_1)^r$ достигала максимума в точке $((1-s)^2/2, s(1-s))$. Для этого необходимо, чтобы производная функции $h(\alpha_1, s(1-s))f(\alpha_1)^r$ равнялась нулю при $\alpha_1 = (1-s)^2/2$.

Лемма 8. *Производная функции* $h(\alpha_1, s(1-s))$ *равна нулю при* $\alpha_1 = (1-s)^2/2$.

Доказательство.

$$h(\alpha_1, s(1-s)) = 2^{(1-s-s(1-s))H\left(\frac{\alpha_1}{1-s-s(1-s)}\right)} \times C_h = 2^{(1-s)^2H\left(\frac{\alpha_1}{(1-s)^2}\right)} \times C_h,$$

где C_h – константа, не зависящая от α_1. Поскольку максимум $H(\alpha)$ достигается при $\alpha = 1/2$, максимум функции $h(\alpha_1, s(1-s))$ достигается при $\alpha_1 = (1-s)^2/2$. Следовательно, производная функции $h(\alpha_1, s(1-s))$ равна нулю при $\alpha_1 = (1-s)^2/2$, что и требовалось доказать. ■

Следовательно, для применения метода вторых моментов необходимо, чтобы производная функции $f(\alpha_1)^r$ равнялась нулю при $\alpha_1 = (1-s)^2/2$. Но нетрудно видеть, что производная функции $f(\alpha_1)^r$ строго положительна на $[0, 1]$, а значит, метод вторых моментов напрямую неприменим.

5 Сбалансированная случайная величина

Пусть W – множество действительнозначных функций вида $w(\sigma, c)$, где $\sigma \in G^n_{ns}$ – грань размерности ns n-мерного куба, а c – некоторая скобка. Рассмотрим класс случайных величин

$$X = \sum_{\sigma}\prod_{c} w(\sigma, c),$$

где сумма берется по всем $\sigma \in G_{ns}^n$, а произведение --- по всем скобкам случайной формулы, и $w(\sigma, c) \in W$. Ясно, что при $w(\sigma, c) = 1_{\sigma \subset N_c}$ случайная величина X равна $\sum_\sigma 1_{\sigma \subset N_{F_k(n,rn)}}$, этот случай был рассмотрен в предыдущем разделе. Выясним, какие условия следует наложить на $w(\sigma, c)$ для применимости метода вторых моментов, а также для упрощения вычислений.

Из независимости скобок и линейности математического ожидания следует, что

$$M(X) = \sum_{\sigma \in G_{ns}^n} M\left(\prod_c w(\sigma, c)\right) = 2^{(1-s)n} C_n^{ns} \prod_c M(w(\sigma, c)) =$$

$$= 2^{(1-s)n} C_n^{ns} M(w(\sigma, c))^{rn}, \qquad (29)$$

$$M(X^2) = M\left(\left(\sum_{\sigma \in G_{ns}^n} \prod_c w(\sigma, c)\right)^2\right) = M\left(\sum_{\sigma, \tau \in G_{ns}^n} \prod_c w(\sigma, c) w(\tau, c)\right) =$$

$$= \sum_{\sigma, \tau \in G_{ns}^n} M(w(\sigma, c), w(\tau, c))^{rn}. \qquad (30)$$

Как и в работе [3], будем рассматривать функции вида $w(\sigma, c) = w(u) = w(|u|) = w_{|u|}$ (u и $|u|$ были определены в предыдущем разделе). Зафиксируем σ и τ. Без ограничения общности, пусть код σ имеет вид $(00\ldots 0 - - \ldots -)$. Как и в предыдущем разделе, выбор τ определяет четыре параметра, $\alpha_1, \alpha_2, \alpha_3$ и α_4, причем

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = 1 - s \\ \alpha_3 + \alpha_4 = s. \end{cases}$$

Найдем $M(w(\sigma, c), w(\tau, c))$. Обозначим вероятность того, что $|u| = i$, а $|v| = j$, через $P_{i,j}$. Тогда

$$M(w(\sigma, c) w(\tau, c)) = \sum_{i,j} w_i w_j P_{i,j}.$$

Пусть $\gamma(u, v)$ – число координат, в которых u и v совпадают и равны единице, т.е. $\gamma(u, v) = |\{t : u_t = v_t = 1\}|$. Обозначим вероятность события „$|u| = i$, $|v| = j$, $\gamma(u,v) = \gamma$`` через $P_{i,j,\gamma}$. Тогда

$$M(w(\sigma,c)w(\tau,c)) = \sum_{i,j} w_i w_j \sum_{\gamma} P_{i,j,\gamma}.$$

Для того, чтобы найти $P_{i,j,\gamma}$, найдем число способов выбрать, какие из координат векторов u и v равны единице. Есть C_k^i способов выбрать единицы в u, C_i^γ способов выбрать единицы в v, соответствующие единицам в u, $C_{k-i}^{j-\gamma}$ способов выбрать единицы в v, не соответствующие единицам в u. Всего $C_k^i C_i^\gamma C_{k-i}^{j-\gamma}$ способов. Пусть выбрано, какие из координат векторов u и v равны единице. Найдем вероятность такой конфигурации. Нетрудно видеть, что вероятность события „$u_t = v_t = 1$`` равна $\alpha_1/2$ (число таких $t$ равно $\gamma$), вероятности событий „$u_t = 1, v_t \neq 1$`` и „$u_t \neq 1, v_t = 1$`` равны $\alpha_2/2+\alpha_3/2$ (число таких $t$ равно $(i-\gamma)+(j-\gamma)$), вероятность события „$u_t \neq 1, v_t \neq 1$`` равна $\alpha_1/2 + \alpha_3 + \alpha_4 = \alpha_1/2 + s$ (число таких t равно $k-i-j+\gamma$). Следовательно, вероятность конкретной конфигурации равна

$$\left(\frac{\alpha_1}{2}\right)^\gamma \left(\frac{\alpha_2+\alpha_3}{2}\right)^{(i-\gamma)+(j-\gamma)} \left(\frac{\alpha_1}{2}+s\right)^{k-i-j+\gamma}.$$

Умножая эту вероятность на число конфигураций, получим

$$P_{i,j,\gamma} = C_k^i C_i^\gamma C_{k-i}^{j-\gamma} \left(\frac{\alpha_1}{2}\right)^\gamma \left(\frac{\alpha_2+\alpha_3}{2}\right)^{(i-\gamma)+(j-\gamma)} \left(\frac{\alpha_1}{2}+s\right)^{k-i-j+\gamma}.$$

При этом s – константа, а $\alpha_2 + \alpha_3 = 1 - s - \alpha_1$. Таким образом, значение $M(w(\sigma,c)w(\tau,c))$ определяется выбором α_1. Обозначим $M(w(\sigma,c)w(\tau,c))$ через $f_w(\alpha_1)$.

Докажем, что как и в предыдущем разделе при $\alpha_1 = (1-s)^2/2$ достигается „независимость`` граней, т.е. $M(w(\sigma,c)w(\tau,c)) = M(w(\sigma,c))M(w(\tau,c))$. Построим векторы u и $v \in A = \{0,1,-\}^k$ так, как это было сделано в предыдущем разделе. Ясно, что

$$M(w(\sigma,c)) = \sum_{u\in A} w(u)P(u).$$

Тогда

$$M(w(\sigma,c))M(w(\tau,c)) = \sum_{u,v\in A} w(u)w(v)P(u)P(v).$$

Но

$$M(w(\sigma,c)(w(\tau,c)) = \sum_{u,v\in A} w(u)w(v)P(u\cap v),$$

и нетрудно видеть, что для „независимости`` граней достаточно, чтобы для всех $u,v\in A$ выполнялось равенство $P(u\cap v) = P(u)P(v)$ (т.е. все события вида „грани $\sigma$ соответствует вектор $u'\in A$`` попарно независимы). При этом

$$P(u) = \prod_{j=1}^{k} s^{(1_{u_j=-})}\left(\frac{1-s}{2}\right)^{(1_{u_j\neq -})},$$

а значит, если $1^j_{u_0v_0}$ – индикатор события „$u_j = u_0, v_j = v_0$``, то

$$P(u)P(v) = \prod_{j=1}^{k} (s^2)^{1^j_{--}} \left(\left(\frac{1-s}{2}\right)^2\right)^{1^j_{00}+1^j_{01}+1^j_{10}+1^j_{11}} \times$$

$$\times\left(s\frac{1-s}{2}\right)^{1^j_{0-}+1^j_{1-}+1^j_{-0}+1^j_{-1}}, \tag{31}$$

$$P(u\cap v) = \prod_{j=1}^{k}\left(\frac{\alpha_1}{2}\right)^{1^j_{00}+1^j_{11}}\left(\frac{1-s-\alpha_1-\alpha_3}{2}\right)^{1^j_{01}+1^j_{10}} \times$$

$$\times\left(\frac{\alpha_3}{2}\right)^{1^j_{0-}+1^j_{1-}+1^j_{-0}+1^j_{-1}}(s-\alpha_3)^{1^j_{--}}. \tag{32}$$

При $\alpha_1 = (1-s)^2/2, \alpha_3 = s(1-s)$

$$\frac{\alpha_1}{2} = \frac{1-s-\alpha_1-\alpha_3}{2} = \left(\frac{1-s}{2}\right)^2,$$

$$\frac{\alpha_3}{2} = s\frac{1-s}{2}, s-\alpha_3 = s^2,$$

и из (31) и (32) следует, что $P(u)P(v) = P(u\cap v)$ для всех u и v из A. Тогда при $\alpha_1 = \frac{(1-s)^2}{2}, \alpha_3 = s(1-s)$ выполняется равенство $M(w(\sigma,c)w(\tau,c)) = M(w(\sigma,c))M(w(\tau,c))$, но $M(w(\sigma,c)w(\tau,c))$ однозначно определяется выбором α_1, следовательно это равенство выполняется при любых α_3.

$$M(X^2) = \sum_{\sigma,\tau\in G^n_{ns}} M(w(\sigma,c),w(\tau,c))^{rn} = \sum_{\sigma,\tau\in G^n_{ns}} f_w(z_1/n)^{rn} =$$

$$= 2^{(1-s)n} C_n^{ns} \sum_{z_3=0}^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} \sum_{z_1=0}^{n(1-s)-z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn} = \tag{33}$$

$$= \sum_{z_3=0}^{ns} \sum_{z_1=0}^{n(1-s)-z_3} h(z_1/n, z_3/n)^n f_w(z_1/n)^{rn} \times \mathrm{poly}(n),$$

где

$$h(\alpha_1, \alpha_3) = 2^{(1-s)} 2^{H(s)} 2^{\alpha_3} 2^{(1-s)H\left(\frac{\alpha_3}{1-s}\right)} 2^{sH\left(\frac{\alpha_3}{s}\right)} 2^{(1-s-\alpha_3)H\left(\frac{\alpha_1}{1-s-\alpha_3}\right)}.$$

В то же время, нетрудно показать (аналогично тому, как это было сделано в предыдущем разделе), что

$$M(X)^2 = \left(h\left(\frac{(1-s)^2}{2}, s(1-s) \right) f_w\left(\frac{(1-s)^2}{2} \right)^r \right)^n \times \mathrm{poly}(n).$$

Следовательно, для применения метода вторых моментов необходимо, чтобы функция $h(\alpha_1, \alpha_3) f_w(\alpha_1)^r$ достигала максимума в точке $((1-s)^2/2, s(1-s))$. Для этого необходимо, чтобы производная функции $h(\alpha_1, s(1-s)) f(\alpha_1)^r$ равнялась нулю при $\alpha_1 = (1-s)^2/2$. Согласно лемме 8, производная функции $h(\alpha_1, s(1-s))$ равна нулю в $(1-s)^2/2$. Следовательно, для применения метода вторых моментов необходимо, чтобы производная функции $f_w(\alpha_1)$ также равнялась нулю в $(1-s)^2/2$. Вычислим производную функции $f_w(\alpha_1)$ в $(1-s)^2/2$.

Лемма 9. *Производная функции $f_w(\alpha_1)$ в точке $(1-s)^2/2$ равна*

$$c\left(\sum_i w_i p_i \right)^2,$$

где $p_i = C_k^i \left(\frac{1-s}{1+s}\right)^i (k(1-s) - 2i)$, а c зависит только от k и s, $c > 0$.

Доказательство. Сначала найдем производную функции $\Phi_{i,j,\gamma}(\alpha_1) \equiv$

$$\equiv \left(\frac{\alpha_1}{2}\right)^\gamma \left(\frac{\alpha_2 + \alpha_3}{2}\right)^{(i-\gamma)+(j-\gamma)} \left(\frac{\alpha_1}{2} + s\right)^{k-i-j+\gamma} =$$

$$= \left(\frac{\alpha_1}{2}\right)^\gamma \left(\frac{1 - s - \alpha_1}{2}\right)^{(i-\gamma)+(j-\gamma)} \left(\frac{\alpha_1}{2} + s\right)^{k-i-j+\gamma}.$$

Нетрудно видеть, что

$$\Phi'_{i,j,\gamma}(\alpha_1) = \Phi_{i,j,\gamma}(\alpha_1) \ln(\Phi_{i,j,\gamma}(\alpha_1))' =$$

$$= \Phi_{i,j,\gamma}(\alpha_1)\left(\frac{\gamma}{\alpha_1} - \frac{i+j-2\gamma}{1-s-\alpha_1} + \frac{k+\gamma-i-j}{2s+\alpha_1}\right).$$

Подставляя $\alpha_1 = (1-s)^2/2$, получим

$$\Phi'_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right) =$$

$$= 2\Phi_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right)\left(\frac{\gamma}{(1-s)^2} - \frac{i+j-2\gamma}{(1-s)(1+s)} + \frac{k+\gamma-i-j}{(1+s)^2}\right) =$$

$$= 2\Phi_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right) \times$$

$$\times \frac{\gamma(1+s)^2 - (i+j-2\gamma)(1-s)(1+s) + (k+\gamma-i-j)(1-s)^2}{(1-s)^2(1+s)^2} =$$

$$= 2\Phi_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right) \times$$

$$\times\Bigg(\frac{\gamma\left((1+s)^2 + 2(1-s)(1+s) + (1-s)^2\right) + k(1-s)^2}{(1-s)^2(1+s)^2} -$$

$$- \frac{(i+j)(1-s)\left((1+s)+(1-s)\right)}{(1-s)^2(1+s)^2}\Bigg) =$$

$$= 2\Phi_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right)\frac{4\gamma + k(1-s)^2 - 2(i+j)(1-s)}{(1-s)^2(1+s)^2}. \qquad (34)$$

Ясно, что

$$\Phi_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right) =$$

$$= \left(\frac{1-s}{2}\right)^{2\gamma}\left(\frac{(1-s)}{2}\frac{(1+s)}{2}\right)^{(i-\gamma)+(j-\gamma)}\left(\frac{1+s}{2}\right)^{2(k-i-j+\gamma)} =$$

$$= \left(\frac{1-s}{2}\right)^{i+j}\left(\frac{1+s}{2}\right)^{2k-i-j}. \qquad (35)$$

Подставляя (35) в (34), получим

$$\Phi'_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right)=$$

$$=2\left(\frac{1-s}{2}\right)^{i+j}\left(\frac{1+s}{2}\right)^{2k-i-j}\frac{4\gamma+k(1-s)^2-2(i+j)(1-s)}{(1-s)^2(1+s)^2}=$$

$$=2^{1-2k}(1-s)^{i+j-2}(1+s)^{2k-i-j}\left(4\gamma+k(1-s)^2-2(i+j)(1-s)\right).$$

Заметим, что

$$P_{i,j}=P_{i,j}(\alpha_1)=\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}\Phi_{i,j,\gamma}(\alpha_1).$$

А значит,

$$P'_{i,j}\left(\frac{(1-s)^2}{2}\right)=\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}\Phi'_{i,j,\gamma}\left(\frac{(1-s)^2}{2}\right)=$$

$$=\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}2^{1-2k}(1-s)^{i+j-2}(1+s)^{2k-i-j}\times$$

$$\times\left(4\gamma+k(1-s)^2-2(i+j)(1-s)\right)=$$

$$=2^{1-2k}(1-s)^{i+j-2}(1+s)^{2k-i-j}\Big(\big(4\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}\gamma\big)+$$

$$+\left(k(1-s)^2-2(i+j)(1-s)\right)\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}\Big). \qquad (36)$$

Нетрудно видеть, что

$$\sum_\gamma C_i^\gamma C_{k-i}^{j-\gamma}=C_k^j,$$

$$\sum_\gamma C_i^\gamma C_{k-i}^{j-\gamma}\frac{\gamma}{i}=\sum_\gamma C_{i-1}^{\gamma-1}C_{k-i}^{j-\gamma}=C_{k-1}^{j-1}=\frac{j}{k}C_k^j.$$

Отсюда

$$\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}=C_k^iC_k^j,$$

$$\sum_\gamma C_k^iC_i^\gamma C_{k-i}^{j-\gamma}\gamma=\frac{ij}{k}C_k^iC_k^j.$$

Тогда из (36) следует, что

$$P'_{i,j}\left(\frac{(1-s)^2}{2}\right) = 2^{1-2k}(1-s)^{i+j-2}(1+s)^{2k-i-j}\times$$

$$\times\left(4\frac{ij}{k}C_k^iC_k^j + \left(k(1-s)^2 - 2(i+j)(1-s)\right)C_k^iC_k^j\right) =$$

$$= 2^{1-2k}(1-s)^{i+j-2}(1+s)^{2k-i-j}C_k^iC_k^j\left(k(1-s)^2 - 2(i+j)(1-s) + 4\frac{ij}{k}\right).$$

Но

$$k(1-s)^2 - 2(i+j)(1-s) + 4\frac{ij}{k} = \frac{1}{k}\left(k(1-s) - 2i\right)\left(k(1-s) - 2j\right).$$

А значит,

$$P'_{i,j}\left(\frac{(1-s)^2}{2}\right) = 2^{1-2k}(1-s)^{-2}(1+s)^{2k}\frac{1}{k}p_ip_j, \qquad (37)$$

где $p_i = C_k^i\left(\frac{1-s}{1+s}\right)^i(k(1-s) - 2i)$. Поскольку

$$f_w(\alpha_1) = \sum_{i,j} w_iw_jP_{i,j}(\alpha_1),$$

выполняется равенство

$$f'_w\left(\frac{(1-s)^2}{2}\right) = \sum_{i,j} w_iw_jP'_{i,j}\left(\frac{(1-s)^2}{2}\right),$$

и из (37) следует, что

$$f'_w\left(\frac{(1-s)^2}{2}\right) = 2^{1-2k}(1-s)^{-2}(1+s)^{2k}\frac{1}{k}\sum_{i,j} w_iw_jp_ip_j =$$

$$= 2^{1-2k}(1-s)^{-2}(1+s)^{2k}\frac{1}{k}\left(\sum_i w_ip_i\right)^2. \blacksquare$$

Таким образом, $f'_w\left(\frac{(1-s)^2}{2}\right) \geq 0$, причем равенство достигается тогда и только тогда, когда выполняется равенство

$$\sum_{i=1}^{k} w_iC_k^i\left(\frac{1-s}{1+s}\right)^i(k(1-s) - 2i) = 0.$$

Ранее функция $H(\alpha)$ была определена как $H(\alpha) = -\alpha\log_2(\alpha) - (1-\alpha)\log_2(1-\alpha)$ при $\alpha \in (0,1)$. Доопределим $H(0) \equiv H(1) \equiv 0$. При этом функция останется непрерывной. Обозначим $h(\alpha_1, \alpha_3) f_w(\alpha_1)^r$ через $g(\alpha_1, \alpha_3)$. Следующая теорема представляет собой достаточное условие применимости метода вторых моментов.

Теорема 6. *Если* $g\left(\frac{(1-s)^2}{2}, s(1-s)\right) > g(\alpha_1, \alpha_3)$ *при всех* $(\alpha_1, \alpha_3) \neq \left(\frac{(1-s)^2}{2}, s(1-s)\right)$, *то в* $N_{F_k(n,rn)}$ *с высокой вероятностью найдется грань размерности* ns.

Доказательство.

Согласно (33),

$$M(X^2) = 2^{(1-s)n} C_n^{ns} \sum_{z_3=0}^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} \sum_{z_1=0}^{n(1-s)-z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn},$$

$$M(X) = 2^{(1-s)n} C_n^{ns} f_w\left(\frac{(1-s)^2}{2}\right)^{\frac{rn}{2}}.$$

Докажем, что для всех $z_3 \in [0, ns]$ и $z_1 \in [0, n(1-s)-z_3]$ выполняется неравенство

$$2^{(1-s)n} C_n^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn} \leq c_1 n^2 g(\alpha_1, \alpha_3), \tag{38}$$

где c_1 – константа, не зависящая от n, z_1 и z_3. Прежде всего, заметим, что

$$C_n^{\alpha n} = 2^{nH(\alpha)} = 1 \tag{39}$$

при $\alpha = 0$ и $\alpha = 1$,

$$C_n^{\alpha n} < \frac{1}{\sqrt{2\pi n}} \frac{1}{\sqrt{\alpha(1-\alpha)}} \left(\frac{1}{\alpha^\alpha (1-\alpha)^{1-\alpha}}\right)^n = \frac{1}{\sqrt{2\pi n}} \frac{1}{\sqrt{\alpha(1-\alpha)}} 2^{nH(\alpha)}$$

при $\alpha \in (0,1)$. В этом случае $\alpha n \geq 1$, а значит, $\alpha \geq 1/n$ и

$$\frac{1}{\sqrt{\alpha(1-\alpha)}} \leq \left(\frac{1}{\sqrt{1/n}}\right)^2 = n.$$

Следовательно,

$$C_n^{\alpha n} < \frac{\sqrt{n}}{2\pi} 2^{nH(\alpha)}. \tag{40}$$

Из (39) и (40) следует, что при всех возможных значениях α

$$C_n^{\alpha n} < c_2\sqrt{n}2^{nH(\alpha)},$$

где c_2 – константа, не зависящая от n и α. А значит,

$$2^{(1-s)n}C_n^{ns}2^{z_3}C_{n(1-s)}^{z_3}C_{ns}^{z_3}C_{n(1-s)-z_3}^{z_1}f_w(z_1/n)^{rn} <$$

$$< 2^{(1-s)n}c_2\sqrt{n}2^{nH(s)}2^{z_3}c_2\sqrt{n(1-s)}2^{n(1-s)H\left(\frac{\alpha_3}{1-s}\right)}c_2\sqrt{ns}2^{nsH\left(\frac{\alpha_3}{s}\right)}\times$$

$$\times c_2\sqrt{n(1-s-\alpha_3)}2^{n(1-s-\alpha_3)H\left(\frac{\alpha_1}{1-s-\alpha_3}\right)}f_w(z_1/n)^{rn} <$$

$$< c_1n^2g(\alpha_1,\alpha_3)^n,$$

где $c_1 = c_2^4$. Неравенство (38) доказано.

Следовательно, если мы рассмотрим произвольное множество $Z_* \subset \mathbb{Z}^2 \cap [0, n(1-s)] \times [0, ns]$, то

$$\sum_{(z_1,z_3)\in Z_*} 2^{(1-s)n}C_n^{ns}2^{z_3}C_{n(1-s)}^{z_3}C_{ns}^{z_3}C_{n(1-s)-z_3}^{z_1}f_w(z_1/n)^{rn} \le c_1n^4g_*^n,$$

где g_* – максимальное значение функции $g(z_1/n, z_3/n)$ на Z_*. Разделим сумму (33) на две части следующим образом. Ясно, что поскольку $g\left(\frac{(1-s)^2}{2}, s(1-s)\right) > g(\alpha_1,\alpha_3)$ при $(\alpha_1,\alpha_3) \ne \left(\frac{(1-s)^2}{2}, s(1-s)\right)$, если мы рассмотрим прямоугольную область вокруг точки максимума $U_{\max} = ((1-s)^2/2-\epsilon, (1-s)^2/2+\epsilon) \times (s(1-s)-\epsilon, s(1-s)+\epsilon)$, то $g_* = \max\limits_{(\alpha_1,\alpha_3)\notin U_{\max}} g(\alpha_1,\alpha_3) < g_{\max}$. Определим

$$Z = \{(z_1,z_3) \in \mathbb{Z}^2 | 0 \le z_3 \le ns, 0 \le z_1 \le n(1-s)-z_3\},$$

$$Z_{\max} = \{(z_1,z_3) \in Z | (z_1/n, z_3/n) \in U_{\max}\}, Z_* = Z \setminus Z_{\max}.$$

Тогда

$$M(X^2) = \sum_{(z_1,z_3)\in Z} 2^{(1-s)n}C_n^{ns}2^{z_3}C_{n(1-s)}^{z_3}C_{ns}^{z_3}C_{n(1-s)-z_3}^{z_1}f_w(z_1/n)^{rn} =$$

$$= \sum_{(z_1,z_3)\in Z_*} 2^{(1-s)n}C_n^{ns}2^{z_3}C_{n(1-s)}^{z_3}C_{ns}^{z_3}C_{n(1-s)-z_3}^{z_1}f_w(z_1/n)^{rn}+$$

$$+ \sum_{(z_1,z_3)\in Z_{\max}} 2^{(1-s)n}C_n^{ns}2^{z_3}C_{n(1-s)}^{z_3}C_{ns}^{z_3}C_{n(1-s)-z_3}^{z_1}f_w(z_1/n)^{rn} \le$$

$$\leq \sum_{(z_1,z_3)\in Z_{\max}} 2^{(1-s)n} C_n^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn} + c_1 n^4 g_*^n. \quad (41)$$

Оценим сверху сумму

$$\sum_{(z_1,z_3)\in Z_{\max}} 2^{(1-s)n} C_n^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn} \leq$$

$$\leq \sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} 2^{(1-s)n} C_n^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn},$$

где $(\alpha_1', \alpha_1'') \times (\alpha_3', \alpha_3'') = U_{\max}$. Так как

$$C_n^{\alpha n} < \frac{1}{\sqrt{2\pi n}} \frac{1}{\sqrt{\alpha(1-\alpha)}} 2^{nH(\alpha)},$$

$$\sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} 2^{(1-s)n} C_n^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn} <$$

$$< \sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} 2^{(1-s)n} \frac{1}{\sqrt{2\pi n}} \frac{1}{\sqrt{s(1-s)}} 2^{nH(s)} 2^{n\alpha_3} \times$$

$$\times \frac{1}{\sqrt{2\pi n(1-s)}} \frac{1}{\sqrt{\frac{\alpha_3}{1-s}\left(1-\frac{\alpha_3}{1-s}\right)}} 2^{n(1-s)H\left(\frac{\alpha_3}{1-s}\right)} \times$$

$$\times \frac{1}{\sqrt{2\pi n s}} \frac{1}{\sqrt{\frac{\alpha_3}{s}\left(1-\frac{\alpha_3}{s}\right)}} 2^{nsH\left(\frac{\alpha_3}{s}\right)} \frac{1}{\sqrt{2\pi n(1-s-\alpha_3)}} \times$$

$$\times \frac{1}{\sqrt{\frac{\alpha_1}{1-s-\alpha_3}\left(1-\frac{\alpha_1}{1-s-\alpha_3}\right)}} 2^{n(1-s-\alpha_3)H\left(\frac{\alpha_1}{1-s-\alpha_3}\right)} f_w(z_1/n)^{rn} \leq$$

$$\leq \frac{c_3}{n^2} \sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} h(z_1/n, z_3/n)^n \times$$

$$\times \frac{1}{\sqrt{\frac{\alpha_3}{1-s}\left(1-\frac{\alpha_3}{1-s}\right)}} \frac{1}{\sqrt{\frac{\alpha_3}{s}\left(1-\frac{\alpha_3}{s}\right)}} \frac{1}{\sqrt{\frac{\alpha_1}{1-s-\alpha_3}\left(1-\frac{\alpha_1}{1-s-\alpha_3}\right)}} f_w(z_1/n)^{rn}. \quad (42)$$

Воспользуемся тем, что значение выражения $\frac{1}{\sqrt{x(1-x)}}$ ограничено сверху константой при $x \in [x_0, x_1]$, где $x_0 > 0$ и $x_1 < 1$. Из (42) следует, что

$$\sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} 2^{(1-s)n} C_n^{ns} 2^{z_3} C_{n(1-s)}^{z_3} C_{ns}^{z_3} C_{n(1-s)-z_3}^{z_1} f_w(z_1/n)^{rn} <$$

$$< \frac{c_4}{n^2} \sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} h(z_1/n, z_3/n)^n f_w(z_1/n)^{rn} =$$

$$= \frac{c_4}{n^2} \sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} g(\alpha_1, \alpha_3)^n, \tag{43}$$

где c_3 и c_4 – константы, не зависящие от n.

Но из свойств $g(\alpha_1, \alpha_3)$ следует, что существуют такие константы c_5 и c_6, что

$$\sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} g(\alpha_1, \alpha_3)^n \leq c_5 n^2 \int_{\alpha_1'}^{\alpha_1''} \int_{\alpha_3'}^{\alpha_3''} g(\alpha_1, \alpha_3)^n d\alpha_1 d\alpha_3 + c_6 n g_{\max}^n,$$

а значит,

$$\frac{c_4}{n^2} \sum_{z_1=\alpha_1' n}^{\alpha_1'' n} \sum_{z_3=\alpha_3' n}^{\alpha_3'' n} g(\alpha_1, \alpha_3)^n \leq c_4 c_5 \int_{\alpha_1'}^{\alpha_1''} \int_{\alpha_3'}^{\alpha_3''} g(\alpha_1, \alpha_3)^n d\alpha_1 d\alpha_3 + \frac{c_4 c_6}{n} g_{\max}^n. \tag{44}$$

Интеграл

$$\int_{\alpha_1'}^{\alpha_1''} \int_{\alpha_3'}^{\alpha_3''} g(\alpha_1, \alpha_3)^n d\alpha_1 d\alpha_3$$

может быть оценен с помощью метода Лапласа для кратных интегралов ([5], §4.6):

$$\int_{\alpha_1'}^{\alpha_1''} \int_{\alpha_3'}^{\alpha_3''} g(\alpha_1, \alpha_3)^n d\alpha_1 d\alpha_3 = \int_{\alpha_1'}^{\alpha_1''} \int_{\alpha_3'}^{\alpha_3''} e^{n \ln g(\alpha_1, \alpha_3)} d\alpha_1 d\alpha_3 \sim \frac{A}{n} g_{\max}^n,$$

где A – константа, не зависящая от n. Следовательно, при достаточно больших n

$$\int_{\alpha_1'}^{\alpha_1''} \int_{\alpha_3'}^{\alpha_3''} g(\alpha_1, \alpha_3)^n d\alpha_1 d\alpha_3 \leq \frac{2A}{n} g_{\max}^n. \tag{45}$$

Совмещая (41), (43), (44) и (45), получим

$$M(X^2) \le c_4c_5\frac{2A}{n}g_{\max}^n + \frac{c_4c_6}{n}g_{\max}^n + c_1n^4g_*^n.$$

Поскольку $g_* < g_{\max}$, существует такая константа c_7, что для любого n выполняется $c_1n^4g_*^n \le c_7g_{\max}^n/n$. Следовательно,

$$M(X^2) \le c_4c_5\frac{2A}{n}g_{\max}^n + \frac{c_4c_6}{n}g_{\max}^n + \frac{c_7}{n}g_{\max}^n = \frac{B}{n}g_{\max}^n, \qquad (46)$$

где $B = 2Ac_4c_5 + c_4c_6 + c_7$ – константа, не зависящая от n. Остается сравнить $Bg_{\max}^n/n$ и $M(X)^2$. Как было показано выше,

$$M(X) = 2^{(1-s)n}C_n^{ns}f_w\left(\frac{(1-s)^2}{2}\right)^{\frac{rn}{2}}. \qquad (47)$$

Известно, что

$$C_n^{ns} > \frac{36}{49}\frac{1}{\sqrt{2\pi n}}\frac{1}{\sqrt{s(1-s)}}2^{nH(s)}.$$

А значит, существует такая константа $c_8 > 0$, что

$$C_n^{ns} > \frac{c_8}{\sqrt{n}}2^{nH(s)}.$$

Тогда из (47) следует, что

$$M(X)^2 > 2^{2(1-s)n}\frac{c_8^2}{n}2^{2nH(s)}f_w\left(\frac{(1-s)^2}{2}\right)^{rn}. \qquad (48)$$

Но $g_{\max} = g\left(\frac{(1-s)^2}{2}, s(1-s)\right) =$

$$= 2^{1-s}2^{H(s)}2^{s(1-s)}2^{(1-s)H\left(\frac{s(1-s)}{1-s}\right)}2^{sH\left(\frac{s(1-s)}{s}\right)}2^{(1-s-s(1-s))H\left(\frac{(1-s)^2}{2(1-s-s(1-s))}\right)}\times$$

$$\times f_w\left(\frac{(1-s)^2}{2}\right)^r =$$

$$= 2^{1-s}2^{H(s)}2^{s(1-s)}2^{(1-s)H(s)}2^{sH(s)}2^{(1-s)^2H(1/2)}f_w\left(\frac{(1-s)^2}{2}\right)^r =$$

$$= 2^{2(1-s)}2^{2H(s)}f_w\left(\frac{(1-s)^2}{2}\right)^r,$$

и из (48) следует, что

$$M(X)^2 > \frac{c_8^2}{n}g_{\max}^n. \qquad (49)$$

Сравнивая (46) и (49), получим, что при $C = c_8^2/B$

$$M(X)^2/M(X^2) \geq C,$$

и из леммы 1 следует, что вероятность присутствия в $N_{F_k(n,rn)}$ грани размерности ns ограничена снизу положительной константой. Но тогда по следствию 2 эта вероятность стремится к единице, что и требовалось доказать. ■

Литература

1. D. Achlioptas and C. Moore, The asymptotic order of the random k-SAT threshold. *In Proc. 43th Annual Symposium on Foundations of Computer Science* (2002) 126 - 127.

2. D. Achlioptas and Y. Peres, The threshold for random k-SAT is $2^k \ln 2 - O(k)$. *J. Amer. Math. Soc.* (2004), 17: 947 - 973.

3. Ф. Ю. Воробьев, О нижней оценке порога 4-выполнимости. *Дискретная математика.* (2007), 19(2): 101 - 108.

4. E. Friedgut, Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-SAT problem. *J. Amer. Math. Soc.* (1999), 12: 1017 - 1054.

5. N. G. de Bruijn, *Asymptotic methods in analysis.* Dover Publications Inc., New York, 3rd edition (1981).

6. V. Chvatal and B. Reed, Mick gets some (the odds are on his side). *In Proc. 33th Annual Symposium on Foundations of Computer Science* (1992) 620 - 627.

7. M. Mezard, T. Mora, and R. Zecchina, Pairs of SAT Assignments and Clustering in Random Boolean Formulae. `arxiv:cond-mat/0506053`, 2005.