Дополнительные главы комбинаторики. Весна 2010.

Лектор: Александр Дайняк

Конспект вели: Стас Смышляев, Полина Гернет, Андрей Скрипников

Этот конспект лекций редактировался мною минимально, поэтому воспринимать его следует «как есть». В частности, я не готов отвечать на вопросы по содержимому данного файла и исправлять в нём ошибки и/или опечатки. *А.Д.*

1 Асимптотические оценки комбинаторных величин

1.1 Некоторые оценки биномиальных коэффициентов

Определение 1.1.

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Утверждение 1.2.

$$\sum_{i=0}^{r} C_n^i \leqslant \frac{n^n}{r^r(n-r)^{n-r}}, 1 \leqslant r \leqslant \frac{n}{2}. \tag{1}$$

Доказательство.

Рассмотрим $t = \frac{r}{n-r} \in (0, 1]$. Нетрудно заметить, что $t^{-r}(t+1)^n = \frac{n^n}{r^r(n-r)^{n-r}}$. С другой стороны, $t^{-r}(t+1)^n = t^{-r}\sum\limits_{i=0}^{r} C_n^i t^i = \sum\limits_{i=0}^{r} C_n^i t^{i-r} \geqslant \sum\limits_{i=0}^{r} C_n^i$, откуда и получим требуемое неравенство (1). □

Замечание 1.3. Положим $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. Тогда неравенство (1) можно переписать в следующем виде:

$$\sum_{i=0}^{r} C_n^i \leqslant 2^{nH(\frac{r}{n})} \tag{2}$$

Тогда, учитывая, что при $0 \leqslant x < \frac{1}{2}$, легко заметить, что при $r \leqslant \epsilon n < \frac{n}{2}$ верно неравенство $\sum\limits_{i=0}^{r} C_n^i \leqslant 2^{\delta n}$ при некотором $\delta = \delta(\epsilon) < 1$.

Утверждение 1.4.

$\sum\limits_{i=0}^{r} C_n^i \leqslant C_n^r \frac{n-r}{n-2r}$, *если* $r < \frac{n}{2}$.

Доказательство.

Легко показать, что $C_n^i = \frac{r(r-1)\ldots(i+1)}{(n-i)(n-i+1)\ldots(n-r+1)} C_n^r$. Числитель в последнем выражении можно оценить сверху величиной r^{r-i}, знаменатель можно оценить снизу величиной $(n-r)^{r-i}$.

$\sum\limits_{i=0}^{r} C_n^i \leqslant \sum\limits_{i=0}^{r} C_n^r (\frac{r}{n-r})^{r-i} \leqslant C_n^r \sum\limits_{i=0}^{r} (\frac{r}{n-r})^i \leqslant C_n^r \sum\limits_{i=0}^{\infty} (\frac{r}{n-r})^i = C_n^r \frac{1}{1-\frac{1}{n-r}} = C_n^r \frac{n-r}{n-2r}$. □

Утверждение 1.5.

$$C_n^k \leqslant \frac{n^k}{k!} e^{\frac{-k(k-1)}{2n}}.$$

Доказательство.

$C_n^k = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!} = \frac{n^k}{k!}(1-\frac{1}{n})(1-\frac{2}{n})\ldots(1-\frac{k-1}{n}) = \frac{n^k}{k!} e^{\ln(1-\frac{1}{n})+\ldots+\ln(1-\frac{k-1}{n})}$. Применяя известное неравенство $\ln(1-x) \leqslant -x, x \in [0, 1)$ к последнему соотношению, получим:

$$\frac{n^k}{k!} e^{\ln(1-\frac{1}{n})+\ldots+\ln(1-\frac{k-1}{n})} \leqslant \frac{n^k}{k!} e^{-\frac{1}{n}-\frac{2}{n}-\ldots-\frac{k-1}{n}} \leqslant \frac{n^k}{k!} e^{-\frac{k(k-1)}{2n}}.$$

□

Замечание 1.6. Если применить неравенство $\ln(1-x) \geqslant -x + O(x^2)$, можно получить следующую оценку:

$$C_n^k \geqslant \frac{n^k}{k!} e^{-\frac{k(k-1)}{2n} + o(\frac{k^3}{n^2})},$$

из которой при $k = o(\sqrt{n})$ следует асимптотическое равенство $C_n^k \sim \frac{n}{k!}$.

1.2 Разбиения чисел

Определение 1.7. *Упорядоченным разбиением* (*неупорядоченным разбиением*) натурального числа N называют любой упорядоченный (неупорядоченный) набор натуральных чисел $(m_1, m_2, \ldots, m_k)$ такой, что $N = m_1 + m_2 + \ldots + m_k$.

Через $p(N)$ ($p(n)$) будем обозначать число всех различных упорядоченных (неупорядоченных) разбиений числа N. Через $p(N; m_1, \ldots, m_s)$ обозначим число всех неупорядоченных разбиений числа n, содержащих только числа из множества $\{m_1, \ldots, m_s\} \subset \mathbb{N}$.

Утверждение 1.8.

$$p(N) = 2^{N-1}.$$

Доказательство.

Каждому упорядоченному разбиению $P = (m_1, m_2, \ldots, m_k)$ числа N можно поставить в соответствие некоторое двоичное слово $(s_1, s_2, \ldots, s_{N-1})$ по следующему правилу:

$$s_i = 1 \Leftrightarrow \exists k' \ (1 \leqslant k' \leqslant k) : i = m_1 + m_2 + \ldots + m_{k'}, i = 1, 2, \ldots, N-1.$$

Легко убедиться, что соответствие, построенное таким образом, является взаимно однозначным соответствием между элементами множества упорядоченных разбиений числа N и двоичными словами длины $N-1$. Оценивая мощность множества двоичных слов длины $N-1$, приходим к требуемому соотношению. □

Утверждение 1.9.

$$p(N; m_1, m_2, \ldots, m_s) = p(N - m_1; m_1, m_2, \ldots, m_s) + p(N, m_2, \ldots, m_s).$$

Доказательство.

Разобьем множество всех разбиений числа N на две части: части, состоящей из разбиений, содержащих m_1, и части, состоящей из разбиений, не содержащих m_1. Тогда мощность первой части равна, очевидно, $p(n - m_1; m_1, \ldots, m_s)$; второй — $p(n; m_2, \ldots, m_s)$. □

Теорема 1.10 (Харди, Рамандужан)**.**

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}.$$

1.3 Обращение Мёбиуса

Определение 1.11. *Функция Мёбиуса* определяется следующим образом:

$$\mu(n) = \begin{cases} 1, \ n = 1 \\ 0, \ n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}, \exists j : \alpha_j > 1 \\ (-1)^s, \ n = p_1, \ldots, p_s \end{cases}$$

, где все p_i — простые числа, все α_i — натуральные числа.

Лемма 1.12.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}.$$

Доказательство.

При $n = 1$ утверждение непосредственно следует из определения функции Мебиуса. Пусть $n \neq 1$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где все p_i — простые. Тогда любое число $d : d|n$ представимо в виде $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, где $\beta_i \leqslant \alpha_i, i = 1, 2, \dots, s$.

Очевидно, при подсчете суммы $\sum\limits_{d|n} \mu(d)$ имеет смысл рассматривать только d вида $d = p_{i_1} p_{i_2} \dots p_{i_r}$ (для некоторого r), для каждого из которых функция Мебиуса принимает значение $\mu(n) = (-1)^r$. Очевидно, для каждого фиксированного r таких d существует ровно C_s^r, откуда $\sum\limits_{d|n} \mu(d) = \sum\limits_{r=0}^{r=s} (-1)^r C_s^r = (1-1)^s = 0$. □

Теорема 1.13 (Об обращении Мебиуса)**.** *Пусть* $f, g : \mathbb{N} \mapsto \mathbb{N}$, $f(n) = \sum\limits_{d|n} g(d)$. *Тогда* $g(n) = \sum\limits_{d|n} f(d)\mu(\frac{n}{d})$.

Доказательство.

$$\sum_{d|n} f(d)\mu(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) \sum_{d'|d} g(d') = \sum_{d'|n} g(d') \sum_{d'|d} \mu(\frac{n}{d}) = \sum_{d|n} g(d) \sum_{d'|\frac{n}{d}} \mu(d').$$

Учитывая предыдущую лемму, получим: $\sum\limits_{d|n} g(d) \sum\limits_{d'|\frac{n}{d}} \mu(d') = g(n)$. □

Определение 1.14. *Периодом* слова a называется минимальное такое $k \in \mathbb{N}$, что a не изменяется при циклическом сдвиге на k букв.

Определение 1.15. *Циклическим словом длины* n называется множество слов длины n, каждые два из которых могут быть получены друг из друга циклическим сдвигом букв.

Пример 1.16. Множество $\{(abca), (bcaa), (caab), (aabc)\}$ является циклическим словом длины 4 в алфавите $\{a, b, c\}$.

Зафиксируем некоторый конечный алфавит A мощности r. Обозначим через $T_r(n)$ число всех циклических слов длины n в произвольном алфавите мощности r.

Утверждение 1.17.

$$T_r(n) = \sum_{d|n} \frac{1}{d} \sum_{d'|d} \mu(d') r^{\frac{d}{d'}}.$$

Доказательство.

Обозначим через V множество всех слов длины n алфавита A ($|V| = r^n$), через V_i для каждого $i : i|n$ обозначим подмножество V, состоящее из всех слов периода i. Нетрудно заметить, что каждое слово периода i порождает циклическим сдвигом ровно i слов длины n и ровно 1 циклическое слово длины n.

Пусть $M(d)$ — количество циклических слов периода d, тогда слов периода d ровно $dM(d)$, то есть, $dM(d) = |V_d|$.

Тогда $|V|$, с одной стороны, равна r^n, а с другой, $|V| = \sum\limits_{d|n} |V_d| = \sum\limits_{d|n} dM(d)$. Пусть $g(d) = dM(d)$, $f(n) = r^n$. Тогда, используя теорему об обращении Мебиуса, получим: $nM(n) = \sum\limits_{d|n} r^d \mu(\frac{n}{d})$. Используя последнее соотношение, окончательно получим: $T_r(n) = \sum\limits_{d|n} M(d) = \sum\limits_{d|n} \frac{1}{d} \sum\limits_{d'|d} r^{d'} \mu(\frac{d}{d'})$. □

В заключение параграфа покажем интересный способ доказательства Малой Теоремы Ферма, предложенный Дейкстрой.

Теорема 1.18.
Если p — простое, $a \in \{1, \ldots, p-1\}$, то $a^{p-1} \equiv 1 (mod\ p)$.

Доказательство.
Перейдем к равносильному соотношению:

$$a^p - a \vdots p. \tag{3}$$

Рассмотрим множество B слов длины p в алфавите из a букв, в которых присутствуют хотя бы две различные буквы. Таких слов ровно $a^p - a$. Разобьем множество B на непересекающиеся классы, такие, что в одном классе лежат слова, получающиеся друг из друга циклическим сдвигом. Учитывая, что p — простое, получим, что в каждый класс состоит ровно из p слов. Окончательно получаем: $a^p - a = |B| = p + p + \ldots + p$, что доказывает (3), а следовательно, и всю Малую Теорему Ферма. □

2 Потоки в сетях

Определение 2.1. *Сеть* — это ориентированный граф с весами на дугах, в котором выделены две вершины — исток (s, source) и сток (t, target).

Определение 2.2. *Поток* — это набор чисел, приписанных дугам, такой что:

1. для любой вершины, за исключением истока и стока, сумма чисел, приписанных входящим дугам, равна сумме чисел, приписанных исходящим дугам;
2. число, приписанное каждой дуге не превышает пропускной способности данной дуги.

Определение 2.3. *Разрезом* называется разбиение множества вершин сети на два множества: S и T, таких, что $s \in S$, $t \in T$

Определение 2.4. *Пропускной способностью разреза* (S, T) называется суммарная пропускная способность дуг из S в T.

Предложение 2.5. Величина потока в сети не превосходит минимальной пропускной способности разрезов.

Оказывается, данная оценка всегда достигается. Для нахождения потока с максимальной величиной можно использовать алгоритм Форда-Фалкерсона.

1. Находим произвольный поток из s в t (например, цепь, с помощью поиска в ширину).
2. Строим остаточную сеть. Остаточная сеть — сеть, содержащуая те же вершины, что и исходная сеть, и строящаяся следующим образом: если по дуге исходной сети с пропускной способностью x проходит поток y, тогда в остаточной сети проводится дуга в том же направлении с пропускной способностью $x - y$ и дуга в противоположном направлении с пропускной способностью y.
3. Ищем поток в остаточной сети.
4. Объединяем потоки: суммируем пропускные способности пар дуг (разнонаправленных — с противоположными знаками) из разных потоков между каждой парой вершин (если получается отрицательное число, проводим дугу в противоположном направлении).
5. Повторяем шаги 2-4, пока у нас в остаточной сети будет хотя бы один ненулевой поток.

Алгоритм остановится, когда на очередном шаге 2 в остаточной сети не будет ненулевого потока из s в t. Поэтому множество вершин, достижимых в остаточной сети по путям из вершины s не содержит t. Тогда пусть S — все вершины, достижимые в остаточной сети из вершины s, оставшиеся вершины — через T. Нетрудно заметить, что (S, T) является разрезом исходной сети, причем таким, что его пропускная способность достигается.

Замечание 2.6. Если в сети все пропускные способности целочисленные, то существует максимальный поток, в котором каждой дуге тоже приписано целое число.

3 Системы различных представителей. Теорема Холла.

Пусть $A_1, A_2, \ldots, A_m \subseteq \{x_1, x_2, \ldots, x_n\}$.

Задача: выбрать $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$, так, чтобы $x_{i_j} \neq x_{i_k}, i \neq k$, $x_{i_1} \in A_1, x_{i_2} \in A_2, \ldots, x_{i_m} \in A_m$. Такой набор $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$ будем называть *системой различных представителей.*

Очевидно, что необходимым условием данной задачи является условие Холла: $|A_{i_1} \cup \ldots \cup A_{i_r}| \geqslant r, \forall i_1, \ldots, i_r, \forall r = 1, \ldots, m$.

Теорема 3.1 (Холла)**.** *Необходимым и достаточным условием существования системы различных представителей является условие Холла.*

Доказательство. Необходимость очевидна. Для доказательства достаточности построим для данных $A_1, \ldots, A_m, x_1, \ldots, x_n$ сеть следующего вида: из истока s идут дуги в каждый x_j, из каждого x_j дуги идут в те A_j, в которые входит x_j. Из каждого A_j в сток t идут дуги. Все дуги в сети имеют вес 1.

Найдем максимальный поток из s в t. Нетрудно заметить, что если его величина равна m, то система различных представителей существует.

Покажем, что пропускная способность любого разреза равна ровно m. Рассмотрим произвольный разрез (S, T) в построенной сети. $S = \{s\} \cup S_x \cup S_A$, где S_x (S_A) — те вершины, входящие в S, которые были сопоставлены x_i (A_i); $T = \{t\} \cup T_x \cup T_A$, где T_x (T_A) — те вершины, входящие в T, которые были сопоставлены x_i (A_i). Пропускная способность любого разреза равна $|T_x| + |S_A|$+число дуг из S_x в T_A. Покажем, что эта величина не меньше m. $|T_x|$+число дуг из S_x в T_A не меньше $m - |S_A| = |T_A|$.

Мы предположили, что условия Холла выполняются. Тогда число дуг из S_x в T_A не меньше числа тех x_i из S_x, которые попали в объединение множеств тех A_j, которым соответствуют вершины из T_A. Тогда $|T_x|$+число дуг S_x в T_A не меньше мощности множества x_i, которым попадают в объединение множеств тех A_i, соответствующих вершинам в T_A. Поэтому, из условия Холла: количество x_i из объединение множеств A_j, соответствующих вершинам из T_A, не меньше мощности T_A.

Любой разрез в сети имеет пропускную способность не меньше m, поэтому существует поток величины m, которому соответствует система различных представителей. □

Определение 3.2. *Совершенное паросочетание* — набор ребер без общих концов, такое, что каждая вершина графа является концом одного из ребер.

Теорема 3.3.
В любом двудольном регулярном (т.е. таком, что степени всех вершин одинаковы) графе существует совершенное паросочетание.

Доказательство.

Пусть вершины в одной доле — элементы (x_i). В качестве множеств A_j возьмем вершины другой доли, очевидным образом определив вложение элементов в множества.

Тогда надо доказать, что выполнены условия Холла (тогда, по теореме Холла, существует система различных представителей, по которой восстанавливаются ребра совершенного паросочетания).

Через $N(A_j)$ обозначим множество вершин, смежных с A_j. Условие Холла можно переформулировать следующим образом: для любых $j_1, \ldots, j_r$ верно $N(A_{j_1}, \ldots, A_{j_r}) \geqslant r$. Осталось показать, что множество соседей любых r вершин из нижней доли графа не меньше r по мощности. Пусть ρ —

число ребер из (некоторых зафиксированных) r вершин нижней доли в верхнюю долю ровно rd, где d — степени вершин в нашем двудольном регулярном графе.

Пусть N — множество соседей этих r вершин, тогда $\rho \leqslant |N|d$, то есть, $|N| \geqslant r$.

□

Следствие 3.4. *Любой регулярный двудольный непустой граф разбивается в объединение совершенных паросочетаний. Отсюда: точное значение хроматического индекса любого регулярного двудольного непустого графа равно d, где d — степень произвольной вершины.*

Пусть есть некоторый полный граф K_n. Разбиваем его на полные двудольные графы $K_{r,s}$.

Задача: минимизировать число графов в разбиении.

Заметим, что такие разбиения всегда существуют: возьмем в качестве первой компоненты произвольную вершину графа и все инцидентные ей $n-1$ ребер. Далее в качестве второй компоненты разбиения возьмем какую-либо из оставшихся вершину графа и все инцидентные ей ребра, не попавшие в первую компоненту. Продолжая действовать таким образом, получим разбиение K_n на $n-1$ «звезд», которые, очевидно, являются полными двудольным графами.

Теорема 3.5 (Грэхэма-Поллака)**.** *В любом разбиении K_n на полные двудольные графы не меньше $n-1$ компоненты.*

Доказательство. Каждой вершине с номером i графа K_n сопоставим некоторую формальную переменную x_i. Каждому ребру графа сопоставим произведение соответствующей пары переменных. Допустим, что граф K_n разбит на m компонент: $(L_1, R_1), (L_2, R_2), \ldots, (L_m, R_m)$. Рассмотрим следующую сумму: $\sum\limits_{i=1}^{m}(\sum\limits_{x_j \in L_i} x_j)(\sum\limits_{x_j \in R_i} x_j)$. По определению множеств L_i, R_i, эта сумма равна $\sum\limits_{i<j} x_i x_j$.

Предположим противное: $m \leqslant n-2$. Рассмотрим следующую систему линейных уравнений:

$$\begin{cases} x_1 + x_2 + \ldots + x_n = 0 \\ \sum\limits_{x_j \in L_1} x_j = 0 \\ \sum\limits_{x_j \in L_2} x_j = 0 \\ \ldots \\ \sum\limits_{x_j \in L_m} x_j = 0 \end{cases} \tag{4}$$

В этой системе $m+1 \leqslant n-1$ линейных уравнений от n переменных. Поэтому существует нетривиальное решение (4) $c_1, c_2, \ldots c_n$, такое, что $c_1^2 + c_2^2 + \ldots + c_n^2 > 0$. Тогда, из (4):

$$0 = (c_1 + c_2 + \ldots + c_n)^2 = c_1^2 + c_2^2 + \ldots + c_n^2 + 2\sum_{i<j} x_i x_j =$$

$$= c_1^2 + c_2^2 + \ldots + c_n^2 + 2\sum_{i=1}^{m}(\sum_{x_j \in L_i} x_j)(\sum_{x_j \in R_i} x_j) = c_1^2 + c_2^2 + \ldots + c_n^2 + 0 > 0.$$

Полученное противоречие завершает доказательство утверждения. □

Теорема 3.6 (Критерий Эйлера)**.** *В графе существует эйлеров цикл тогда и только тогда, когда граф связный и все его вершины четной степени.*

Теорема 3.7. *У любого $2k$-регулярного графа есть 2-фактор (то есть остовный подграф степени 2).*

Доказательство. Очевидно, что достаточно рассмотреть только случай связного графа.

По критерию Эйлера, в графе существует эйлеров цикл. Ориентируем все ребра графа в направлениях, в которых они проходятся в эйлеровом цикле. Расщепим все вершины графа на две. Полученный граф — регулярный степени k, двудольный. Тогда, по утверждению, в полученном графе можно найти совершенное паросочетание.

Склеим вершины. Тогда ребра паросочетания образуют искомую систему циклов. □

Теорема 3.8 (Теорема Рамсея (двуцветная теорема Рамсея для графов)). *Для любых p,q существует $R(p,q)$, такое, что в любом графе на $R(p,q)$ вершинах есть либо полный подграф на p вершинах, либо независимое множество на q вершинах.*

Доказательство. Докажем по индукции.

$R(p,1) = 1 = R(1,q)$; $R(p,2) = p$, $R(2,q) = q$.

Предположим, что существуют $R(p-1,q)$,$R(p,q-1)$. Докажем, что $R(p,q) \leqslant R(p-1,q)+R(p,q-1)$. Рассмотрим произвольную вершину v графа G, такого, что $|V(G)| = R(p-1,q) + R(p,q-1)$. В множестве $V' = V(G) \setminus v$ $R(p-1,q) + R(p,q-1) - 1$ вершина. По принципу Дирихле, либо из v в V' выходит либо не менее, чем $R(p-1,q)$ красных ребер, либо не менее, чем $R(p,q-1)$ синих. Пусть не менее, чем $R(p-1,q)$ красных ребер. Тогда каким бы ни был подграф, в который ведут эти ребра, в любом случае, очевидно, индуктивный переход будет верен. □

Теорема 3.9 (Многоцветная теорема Рамсея). *Для любых $n_1, n_2, \ldots, n_s$ существует $R(n_1, n_2, \ldots, n_s)$ такие, что в $K_{R(n_1,n_2,\ldots,n_s)}$ при любой раскраске в s цветов либо есть K_{n_1} цвета 1, либо есть K_{n_2} цвета 2, либо ... либо есть K_{n_s} цвета s.*

Обоснование (для случая трех цветов). $R(n_1,n_2,n_3) \leqslant R(n_1, R(n_1,n_2))$. «Объединим» два цвета и применим двуцветную теорему Рамсея.

Теорема 3.10 (Теорема Рамсея). *Для любых p,q,r существует $\tilde{R}(p,q,r)$, таких, что для любой раскраски всех r-подмножеств множества мощности $\tilde{R}(p,q,r)$ в красный и синий цвета существует либо подмножество мощности p, все r-подмножества которого красные, либо подмножество мощности q, все r-подмножества синие.*

Доказательство. Докажем по индукции. $\tilde{R}(r,q,r) = q$, $\tilde{R}(p,r,r) = p$ (для $r = 2$ теорема Рамсея уже доказана). Предположение индукции: пусть существуют $\tilde{R}(p,q,r-1)$ для любых $p,q \geqslant r-1$, а также $\tilde{R}(p-1,q,r)$, $\tilde{R}(p,q-1,r)$. Покажем, что существует $\tilde{R}(p,q,r)$.

Покажем, что $\tilde{R}(p,q,r) \leqslant \tilde{R}(p_1,q_1,r-1)+1 = \tilde{R}_0$, где $p_1 = \tilde{R}(p-1,q,r)$, $q_1 = \tilde{R}(p,q-1,r)$. Пусть S — произвольное множество мощности $\tilde{R}_0$, пусть $a \in S$. Раскраска в красный и синий цвета r подмножества множества S порождает раскраски $r-1$ подмножеств множества $S \setminus \{a\}$.

$|S \setminus \{a\}| = \tilde{R}(p_1,q_1,r-1)$, поэтому в $S \setminus \{a\}$ есть либо подмножество S' мощности $\tilde{R}(p-1,q,r)$, все $(r-1)$-ки которого раскрашены в красный цвет, либо мощности $\tilde{R}(p,q-1,r)$, все $(r-1)$-ки которого синие.

По предположению индукции, в S' есть либо подмножество мощности q, все r-ки которого синие (и тогда все хорошо), либо есть подмножество мощности $(p-1)$, у которого все r-ки красные. Добавив к нему a, мы получим множество мощности p, у которого все r-ки красные. □

Теорема 3.11 (Теорема Эрдёша-Секереша). *Для любого m существует $N(m)$ такое, что из любых $N(m)$ плоскостей, лежащих в общем положении (никакие три не коллинеарны) можно выбрать m точек, образующих выпуклый m-угольник.*

Доказательство. Очевидно, что $N(4)$=5. Нетрудно показать также, что верна следующая лемма:

Лемма 3.12. Если m точек в общем положении не образуют выпуклый m-угольник, то среди них можно выбрать 4 точки, не образующие выпуклый 4-угольник.

Рассмотрим на плоскости $\tilde{R}(m,5,4)$ точек в общем положении. Будем считать красными четверки точек, которые образуют выпуклые 4-угольники, а остальные будем считать синими. Тогда, по теореме Рамсея, либо существует m точек (среди данных), таких, что все 4-угольники, на них выпуклые (эти m точек, по лемме, образуют выпуклый m-угольник), либо существует пять точек, среди которых нельзя выбрать выпуклый 4-угольник, чего не может быть по лемме. □

Утверждение 3.13.
$R(p,q) \leqslant C_{p+q-2}^{p-1}$.

Доказательство.

$R(p,q) \leqslant R(p-1,q) + R(p,q-1) \leqslant C_{p+q-3}^{p-2} + C_{p+q-3}^{p-1} = C_{p+q-2}^{p-1}$. □

4 Латинские квадраты

Латинским квадратом порядка n называется матрица, состоящая из элементов множества $\{1, 2, \ldots, n\}$, такая, что в каждой строке и в каждом столбце все элементы различны.

Утверждение 4.1.
Для любого $m < n$ латинский прямоугольник $m \times n$ дополняется до латинского квадрата.

Доказательство.

Докажем, используя Теорему Холла.

Покажем, как можно достроить латинский прямоугольник размера $m \times n$ до латинского прямоугольника размера $m + 1 \times n$. Если $A_1, A_2, \ldots, A_n$ — множество элементов, не встречавшихся в $1, 2, \ldots, n$ столбце прямоугольника.

Осталось найти систему различных представителей для $A_1, A_2, \ldots, A_n$ (чтобы после применить Теорему Холла). Мощность A_i для любого i равна $n - m$. Количество элементов (с повторениями) элементов в множествах $A_{i_1}, A_{i_2}, \ldots, A_{i_r}$ равно $N(i_1, i_2, \ldots, i_r) = r(n - m)$.

Каждое число входит в точности в $n - m$ множеств из набора $A_1, A_2, \ldots, A_n$.

$|A_{i_1} \cup A_{i_2} \cup \ldots \cup A_{i_r}| \geqslant \frac{N(i_1,i_2,\ldots,i_r)}{n-m} = r$. □

4.1 Обобщение задачи построения латинского квадрата

Пусть при тех же условиях на матрицу в каждой позиции (i, j) стоит не произвольный элемент из $\{1, 2, \ldots, n\}$, а некоторый элемент из множества A_{ij}.

Очевидно, если все A_{ij} не пересекаются, такой обобщенный латинский квадрат существует.

Рассмотрим граф G_n, такой, что $V(G) = \{(i, j) | 1 \leqslant i, h \leqslant n\}$, а $E(G) = \{((i, j), (i, j')) | i = 1, 2, \ldots, n, j \neq j'\} \cup \{((i', j), (i, j)) | j = 1, 2, \ldots, n, i \neq i'\}$. Тогда задача построения латинского квадрата порядка n в точности эквивалентна задаче о раскраске графа G_n в n цветов.

Задача о списочной раскраске (прямое обобщение о раскраске): дан граф, и каждой его вершине i сопоставлен список допустимых для этой вершины цветов $L(i)$. Требуется выбрать для каждой вершины цвет из ее списка допустимых цветов, так, чтобы смежные вершины получили разные цвета.

Списочное хроматическое число графа — минимальное число такое, что для любого набора списков, если все списки имеют мощность не меньшую этого числа, то существует списочная раскраска.

Пример 4.2. Чтобы показать, что списочное хроматическое число графа не всегда совпадает (а значит, бывает строго больше) с хроматическим числом графа, достаточно рассмотреть следующий граф: $V = \{1, 2, 3, 4, 5, 6\}$, $E = \{(1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (1, 6), (2, 5)\}$, $L(1) = (2, 3)$, $L(2) = (1, 2)$, $L(3) = (1, 3)$, $L(4) = (2, 3)$, $L(5) = (1, 2)$, $L(6) = (1, 3)$.

Теорема 4.3 (Галвина)**.** *Списочное хроматическое число графа G_n равно n.*

Свойство ориентированного графа, при котором его «удобно» раскрашивать: для любого множества S вершин графа существует подмножество $S' \subseteq S$, где S — независимое множество, для любого $v \in S \setminus S'$ из v идет дуга в S' и $|L(v)| > deg(v)$ для любого $v \in G$.

4.2 Обобщённый латинский квадрат.

$|A_{ij}| = n$

1. $deg^+ v < |L(v)|$
2. $\forall S \subseteq U(G) \quad \exists S' \subseteq S$
   - S' — независимо
   - $\forall u \in S \setminus S' \quad \exists v \in S' : (u, v) \in E(G)$

Выберем цвет, и возьмём все вершины, у которых в $L(v)$ есть данный цвет, обозначим такое множество как S. S'— независимое множество. Окрасим S' в этот цвет (красный) и исключим красный из списков вершин $S \backslash S'$. Осталось показать, что в графе латинского квадрата можно ориентировать ребра так, чтобы он обладал выше указанными свойствами 1) и 2). Это делается следующим образом: ребро ориентируется в соответствии с циклическим латинским квадратом от меньшего k к большему значению в строках циклического квадрата.
Здесь и далее G_n— ориентированный граф.

4.3 Задача об устойчивом паросочетании

(ТУТ ДОЛЖНА БЫТЬ КАРТИНКА) Если (m_i, f_j) не входит в паросочетание, то существует либо (m_i, f_l), либо (m_k, f_j)— лучшее паросочетание для m_i или f_j. ***Предложение 4.4.*** (Алгоритм Гейла-Шейли) "Женим холостяков": по очереди делаем предложения, начиная с более предпочтительных кандидатов. *Обоснование*: очевидно.

Построим по G_n и $S \subseteq V(G_n)$ двудольный граф, где Мужчины— это строки квадрата $1, \ldots, n$, а Женщины— столбцы. m_i предпочитает $f_j > f_k$, если $M(i,j) > M(i,k)$. В этом графе проведём рёбра от m_i к f_j, $(i,j) \in S$. Стабильные паросочетания в полученном графе составляют подмножество вершин $S' \subseteq S$. Оно независимо, т.к. оно - паросочетание. (Вершины лежат в различных строках и столбцах)

Утверждение 4.5.
Для любой вершины $v \in S \backslash S$ существует дуга в S', что соответствует стабильности.

Доказательство.
Рассмотрим вершину v. Она соответствует ребру (m_i, f_j), входящему в двудольный граф, но не входящему в стабильное паросочетание. То есть, должно существовать либо ребро (m_i, f_k), либо ребро (m_l, f_j) □

5 Вероятностные методы

Пусть $R_2(p,q)$— наименьшее число такое, что при любой раскраске рёбер графа $K_{R(p,q)}$ в два цвета, существует либо красный подграф K_p, либо синий подграф K_q.
Нижняя оценка.
Если для некоторого n получится раскрасить получится раскрасить вершины в 2 цвета так, чтобы в них не было K_p или K_q, то $R(p,q) \geqslant n$.
Возьмём случайную раскраску: любое ребро из $\frac{n(n-1)}{2}$ имеющихся красим в красный цвет с вероятность $\frac{1}{2}$.

$$(\text{Число раскрасок}) = 2^{\frac{n(n-1)}{2}}$$

$$P(\text{На конкретном множестве } p \quad K_p \text{— красный}) = \frac{1}{2^{\frac{p(p-1)}{2}}}$$

$$P(K_p \text{ — красный}) \leqslant C_n^p \cdot (\frac{1}{2})^{\frac{p(p-1)}{2}}$$

$$P(\text{Есть красный } K_p \text{ или синий } K_q) \leqslant C_n^q \cdot (\frac{1}{2})^{\frac{q(q-1)}{2}} + C_n^p \cdot (\frac{1}{2})^{\frac{p(p-1)}{2}}$$

Пусть $p = q$. Тогда $P \leqslant C_n^p \cdot 2^{1-\frac{p(p-1)}{2}}$.
Если $p < 1$, то существует следующая раскраска K_n: подберём n так, чтобы $C_n^p \cdot 2^{1-\frac{p(p-1)}{2}} < 1$.

$$C_n^p < 2^{\frac{p(p-1)}{2}} - 1$$

$$\frac{n^p}{p!} < 2^{\frac{p(p-1)}{2}} - 1$$

$$p\log n - p\log p < \frac{p(p-1)}{2}$$

Сокращая обе части на p, получим: $\log n < \frac{p-1}{2}$. Если $n = \lfloor 2^{\frac{p}{3}} \rfloor$, то можно считать, что $R(p,q) < 2^{\frac{p}{3}}$.
Нижняя оценка для чисел Заранкевича.
Пусть $N(m)$— максимальное число единиц в матрице размерности $m \times m$, не содержащей подматрицы из одних единиц размерности $a \times a$.
Построим матрицу размерности $m \times m$, содержащую S единиц, но без $a \times a$ единичных подматриц. Тогда $N_a(m) \geqslant S$.
Пусть в $m \times m$-матрице не более t единичных подматриц $a \times a$. Выкинем по одной единице из каждой такой подматрицы, пока они есть. Получим $T(A)$.

$$\sharp T(A) \geqslant \sharp A - t$$

Выберем случайну матрицу $m \times m$. Получаем 1 — с вероятностью p 0 — $(1-p)$. Полученная матрица - матрица A.

$$\mathbb{E}\sharp A = pm^2$$

$$\mathbb{E}(\text{число единичных } a \times a \text{ подматриц}) = p^{a^2}(C_m^a)^2$$

$$(\sharp(T(A))) \geqslant \mathbb{E}(\sharp(A)) - \mathbb{E}(\text{пара подматриц}) = pm^2 - p^{a^2}(C_m^a)^2$$

Существует конкретная матрица $m \times m$ без $a \times a$ с таким количеством единиц:

$$N_a(m) \geqslant \max_p(m^2p - p^{a^2}(C_m^a)^2)$$

$$f'(p) = m^2 - a^2p^{a^2-1}(C_m^a)^2, \quad p = (\frac{m}{aC_m^a})^{\frac{2}{a^2-1}}$$

$$f(p) = m^2(\frac{m}{aC_m^a})^{\frac{2}{a^2-1}} - (C_m^a)^2(\frac{m}{aC_m^2})\frac{2a^2}{a^2-1} \geqslant$$

$$\{C_m^a < \frac{m^a}{a!}\} \geqslant const(a) \cdot m^{2-\frac{2}{a+1}}$$

$$N_2(n) \leqslant n(\sqrt{n - \frac{3}{4}} + \frac{1}{2})$$

6 Экстремальные задачи на графах

Теорема 6.1 (Турана)**.** *G — граф на n вершинах без полных подграфов на k вершинах и содержит максимально возможное среди всех графов с такими свойствами, то граф представим в виде разбиения на $k-1$ подмножеств вершин, таких, что между двумя вершинами одного подмножества вершин нет, но есть все возможные ребра между различными подмножествами, причем мощности всех этих подмножеств отличаются не более, чем на 1.*

Доказательство. Докажем вначале, что если G — экстремальный граф, то вершина графа G можно разбить на независимые множества, между любыми двумя из которых проведены все возможные ребра.

Рассмотрим отношение «несмежности» вершин в графе. Отношение это, очевидно, рефлексивное и симметричное. Докажем, что оно транзитивное.

Предположим противное: пусть u несмежно с v, v несмежно с w, но u смежно с w. Рассмотрим следующие случаи:

1. степень вершины v строго меньше степени вершины u. Тогда удалим из графа G вершину v и продублируем вершину u. Тогда число ребер в графе увеличится, а новых клик не появится — противоречие с условием экстремальности G;

2. $deg(v) < deg(w)$ — аналогично первому пункту;

3. $deg(v) \geqslant deg(u)$, $deg(v) \geqslant deg(w)$. В таком случае удалим вершины u и v и добавим две копии вершины v. Тогда число ребер E' в получившемся графе: $|E'| = |E| - deg(u) - deg(w) + 2deg(v) + 1$. Снова получили противоречие с экстремальностью.

Отношение несмежности является отношением эквивалентности. Классы эквивалентности по этому отношению — искомые подмножества.

Осталось показать, что эти подмножества N_i ($|N_i| = n_i$) сбалансированы по мощности ($|n_i - n_j| \leqslant 1$, $i, j = 1, 2, \ldots, k-1$). Предположим противное. $|E| = \sum\limits_{1 \leqslant i < j \leqslant k-1} n_i n_j = \frac{1}{2}((n_1 + n_2 + \ldots + n_{k-1})^2 - n_1^2 - n_2^2 - \ldots - n_{k-1}^2)$. Максимизация числа ребер эквивалентна минимизации суммы квадратов $n_1^2 + n_2^2 + \ldots + n_{k-1}^2$. Пусть $n_1 = n_2 + t$, $t \geqslant 2$. Тогда возьмем набор $n_1 - 1, n_2 + 1, n_3, n_4, \ldots, n_{k-1}$. $(n_2 + t - 1)^2 + (n_2 + 1)^2 + n_3 + \ldots + n_{k-1} = (n_1^2 + n_2^2 + \ldots + n_{k-1}^2) + c, c > 0$. □

Проблема Заранкевича: сколько ребер может быть в двудольном графе с долями мощностей m и n без полных двудольных подграфов $K_{a,b}$?

Пусть $N_a(m)$ — число ребер в графе с долями (m, m) без $K_{a,a}$.

$N_a(m)$ — максимальное число единиц в матрице $m \times m$ без $a \times a$ состоящих только из единиц подматриц.

Утверждение 6.2.
$N_2(m) \leqslant m(\sqrt{m - \frac{3}{d}} + \frac{1}{2})$

Доказательство.

Посмотрим на строки матрицы как на вектора и рассмотрим суммы этих векторов. Пусть B_i — i-ая вектор-строка матрицы. Рассмотрим $B = B_1 + B_2 + \ldots + B_m$. Рассмотрим скалярное произведение $(B, B) = (B_1, B_1) + (B_2, B_2) + \ldots + (B_m, B_m) + 2 \sum\limits_{1 \leqslant i \leqslant j \leqslant m} (B_i, B_j) \leqslant N_2(m) + m(m-1)$. Пусть N_j — число единиц в j-м столбце. Тогда $(B, B) = \sum\limits_{j=1}^{m} N_j^2 \geqslant \frac{m(\frac{N_2(m)}{m})^2}{\frac{(N_2(m)^2)}{m}}$. Тогда $m(m-1) + N_2(m) \geqslant \frac{N_2(m)^2}{m}$. □

Определение 6.3. *Числом скрещиваний (crossing number, cr(G))* назовём минимальное число пересечений при изображении графа на плоскости.

$$cr(K_5) = cr(K_{33}) = 1$$

Пусть G — планарный граф, n — число его вершин, m - число ребер, k - число граней. Из курса дискретной математики известно тривиальные неравенства:

$$m \leqslant 3n - 6$$

$$n - m + k = 2$$

Предложение 6.4. Если G не планарный граф, то $cr(G) \geqslant m - 3n$.

Утверждение 6.5.
Если в G $m < 4n$, то $cr(G) \geqslant \frac{m^3}{64n^2}$.

Доказательство.

G - граф, $|E| = m \quad |V| = n < 4n$.

Для доказательства будем выбирать случайно порождённый подграф H в графе G. Любую вершину из G с вероятностью p выберем в этот подграф.

$\mathbb{E}|V_H| = pn$

$\mathbb{E}|E_H| = p^2 m$

$\mathbb{E}cr(H) = p^4 cr(G)$ При данной реализации, используя Утверждение6.4, получим:

$$cr(H) \geqslant cr(G) \geqslant m - 3n \tag{5}$$

$p^4 cr(G) \geqslant p^2 m - 3pn$
Подберем p.
$cr(G) \geqslant \frac{m}{p^2} - \frac{3n}{p^2} \to \max_p$
$(-''-)' = \frac{-m\cdot 2}{p^3} + \frac{3n\cdot 3}{p^2} = \frac{9n}{p^4} - \frac{2m}{p^3} = \frac{9n-2mp}{p^4}$,
откуда $p = \frac{9n}{2m}$. Подставляем.
$\frac{4m^3}{81n^2} - \frac{3n\cdot 8m^3}{729n^3} = \frac{8m^3}{243n^2} \cdot (\frac{3}{2} - 1) = \frac{4m^3}{243n^2}$
Откуда $m > \frac{9}{2}n$

□

Определение 6.6. *Случайный граф*— это вероятностное пространство $(\Omega, \mathcal{F}, P)$, где Ω— это множество всевозможных помеченных n-вершинных графов. $P(G \subseteq \Omega) = P^{|E|} \cdot (1-P)^{\frac{n(n-1)}{2}\cdot|E|}$

Если $P = \frac{1}{2}$, то $P(G) = \frac{1}{2}^{\frac{n(n-1)}{2}}$

Определение 6.7. Почти все графы обладают свойством $\mathcal{P}$, если вероятность того, что граф обладает свойством $\mathcal{P}$ стремится к 1 при $n \to \infty$

Утверждение 6.8.
Почти все графы связны.

Доказательство.
P(случайно порожденный вершинный граф не связен)$\leqslant \sum\limits_{V', V''\neq\varnothing} P(V', V''$ в сл.гр.нет ребер)=
$= \sum\limits_{k=1}^{n-1} C_n^k \frac{1}{2}^{k(n-k)} \leqslant 2 \cdot \sum\limits_{k=1}^{n-2} (\frac{en}{k})^k (\frac{1}{2})^{k(n-k)} = 2 \cdot \sum\limits_{k=1}^{n/2} (\frac{en}{k\cdot 2^{n-k}})^k = \{t = 2^{n/2} \to 0\} \leqslant 3t(1-t^{n/2}) \to 0$ □

Утверждение 6.9.
Диаметр почти всех графов равен двум.

Доказательство.
Очевидно, что диаметр почти всех графов больше единицы.
P(в случайном графе существуют вершины u, v такие, что расстояние между ними больше равно 3)$\leqslant C_n^2 (\frac{3}{4})^{n-2} \to 0 \qquad n \to \infty$
P(любая вершина соединена с u или v при том, что расстоение от u до v больше двух)$\leqslant (\frac{3}{4})^{n-2} \to 0$
□

7 Матроиды

Определение 7.1. *Матроид* — это пара (S, F), где S— конечное множество, а F - семейство подмножеств множества S, обладающая следующими свойствами:

1. Если $A \in F$, то $\forall B \subseteq AB \in F$ (свойство наследственности)
2. $\forall A \subseteq S \quad \Rightarrow \quad \forall B', B'' \in F$
   $B', B'' \subseteq A \quad \Rightarrow \quad |B'| = |B''|$, где B', B'' - максимальные по включению.

Пример 7.2. (S, F), где S — множество строк матрицы, а F — семейство всевозможных линейно независимых множеств строк, - матроид.

Задача. Пусть (S, F) — матроид. Для любого $s \in S$ ставится в соответствие некий параметр $w(s)$. Выбрать независимое подмножество $A \subset F$ такое, что $\sum\limits_{s\in A} \to max$.

Задача. Пусть $w(s)$ — количество нулей. Выбрать линейно независимое множество строк матрицы так, чтобы $\sum\limits_{s\in A} w(s) \to min$, где $\sum\limits_{s\in A} w(s)$ — суммарное количество ненулевых элементов в этих строках.

Оптимальным для решения такого рода задач является жадный алгоритм.
$A = \varnothing$
while $(\exists s \in S : A \cup \{F\})$
{взять максимальный по весу элемент с таким свойством и добавить его к множеству A}

Теорема 7.3.
Пусть (S, F) — наследственная система, тогда следующие свойства эквивалентны:

1. *(S, F) — матроид*
2. *при любом выборе весов жадный алгоритм для выше указанных задач - оптимален*
3. *$\forall I_1, I_2 \in F$ таких, что $|I_1| = |I_2| - 1 \Rightarrow \exists s \in I_2 \backslash I_1 : I_1 \cup \{s\} \in F$*

Доказательство.
$1 \Rightarrow 2$. Для доказательства используем теорему Радо-Эдмондса. Пусть (S, F)— матроид и пусть жадный алгоритм сработал не оптимально. Результат жадного алгоритма — набор $s_1 \dots s_i$, упорядоченный по убыванию весов, и существует $s'_1 \dots s'_j$ — множество из F с большим весом. Заметим также, что $i = j$.
Докажем по индукции, что $w(s_k) > w(s'_k)$ выполняется для любого k, тем самым получив противоречие.
База: $k = 1$ - очевидно, $w(s_1) \geqslant w(s'_1)$.
Шаг: Пусть $w(s_1) \geqslant w(s'_1) \dots w(s_{n-1}) \geqslant w(s'_{n-1})$. Допустим, что $w(s_m) < w(s'_m)$.
Рассмотрим множество $C = \{s \in S | w(s) \geqslant w(s'_m)\}$
$w(s_1) \geqslant \dots \geqslant w(s_{m-1}) \geqslant w(s'_{m-1}) \geqslant w(s'_m)$, где неравенство $w(s_{m-1}) \geqslant w(s'_{m-1})$ достигается по предположению индукции. Следовательно, $\{s_1 \dots s_{m-1}\} \subseteq C$ - максимальное по включению множество. Кроме того, $s'_m \in C$ по построению. Получаем, что $\{s'_1 \dots s'_m\} \subseteq C$ — какое-то независимое множество. Полученное протеворечит свойству 2 из определения матроида.

$2 \Rightarrow 3$. Допустим, пара (S, F) такова, что $\exists I_1, I_2 \in F : \quad |I_1| = |I_2| - 1 = k$ и $\nexists s \in I_1 \backslash I_2 : \quad I_1 \cup \{s\} \notin F$.
Возьмём следующие веса элементов в S:
$$w(s) = \begin{cases} 0, & s \in I_1 \cup I_2 \\ k+1, & s \in I_2 \backslash I_1 \\ k+2, & s \in I_1 \end{cases}$$
Жадный алгоритм при таких весах выберет все элементы из I_1, после чего невозможно будет добавлять элементы с ненулевым весом. Получаем, что вес результата равен $k(k+2)$. При этом $w(I_2) \geqslant (k+1)^2 > k(k+2)$. Следовательно, алгоритм работает неоптимально.
$3 \Rightarrow 1$. Допустим, пара (S, F) не матроид. Следовательно, существуют такие C, I_1, I_2, что I_1, I_2 — максимальные по включению независимые подмножества C, причём $|I_1| = |I_2|$. Не ограничивая общности, будем полагать, что $|I_1| < |I_2|$.
Тогда, в частности, $\nexists s \in I_1 \backslash I_2 : \quad I_1 \cup \{s\} \in F$. Противоречие. □

Пример 7.4. **Алгоритм Краснова** выбора оставного дерева максимального веса. Пусть $A \neq \varnothing$. Пока в G есть ребро минимального веса такое, что в объединении с A оно по прежнему не даст цикл, добавляем это ребро в A.

Предложение 7.5. Пара E, F, где E— множество рёбер исходного графа, а F— множество ребер, не образующих цикл, является матроидом.

8 Локальная лемма Ловаса

$A_1, \dots, A_s$ — события в некотором вероятностном пространстве, причём событие A_i не зависит от группы событий $A_{j_1}, \dots A_{j_r}$, если $P(A_i | A_{j_{l_1}} \cap \dots A_{j_{l_t}}) = P(A_i)$

Определение 8.1. *Орграф зависимости от событий* - это граф, вершинами которого являются события $A_1, \ldots, A_n$, а дуги образуются таким образом, что события A_i не зависят от группы событий, в которой из вершины A_i не идут дуги.

Замечание 8.2. Полный орграф со всеми дугами есть орграф зависимости от любого события.

Лемма 8.3. **(Локальная лемма Ловаса, общий случай)** Пусть события $A_1, \ldots, A_n$ и числа $x_1 \ldots x_n$ таковы что:
$P(A_i) \leqslant x_i \cdot \prod\limits_{x_j}$, причём берутся те номера j в x_j, при которых в орграфе зависимости идёт дуга из A_i в A_j. Тогда вероятность того, что не произойдёт ни одного из событий A_i:

$$P(\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_n) \geqslant \prod_{i=1}^{n}(1 - x_i) > 0$$

Лемма 8.4.
(Локальная лемма Ловаса, симметричный случай) *Пусть события $A_1, \ldots, A_n$ таковы, что вероятность каждого из них не превосходит $p -$ ($P(A_i) \leqslant p$. A_i зависит не более, чем от d других событий (то есть найдётся по крайне мере $n - d$ событий, от которых A_i не зависит). Тогда если $ep(d + 1) \leqslant 1$, то*

$$P(\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_n) > 0$$

Доказательство.

Положим $x_i = \frac{1}{d+1}$
Докажем, что $P(A_i) \leqslant \frac{1}{d+1} \cdot (1 - \frac{1}{d+1})^d$. Если это неравенство выполнено в условиях симметричного случая, то получим сведение к общему случаю.

$$p \leqslant \frac{1}{d+1}(1 - \frac{1}{d+1})^d$$
$$p(d+1)(1 - \frac{1}{d+1})^d \leqslant 1$$

При том, что $1 - \frac{1}{d+1} \to 1$, мы получили неравенство из условий леммы, а следовательно, симметричный случай сводится к общему. □

Докажем общий случай (8.3).

Доказательство. С помощью индукции по s покажем, что

$$P(A_i | \overline{A}_{j_1} \cap \ldots \cap \overline{A}_{j_s}) \leqslant x_i$$

Если $s = 0$, то неравенство очевидно из условия леммы.
Пусть $s > 0$. Воспользуемся равенством

$$P(A|B \cap C) = \frac{P(A \cap B|C)}{P(B|C)}$$

Получаем:

$$P(A_i | \overline{A}_{j_1} \cap \ldots \cap \overline{A}_{j_s}) = \frac{P(A_i \cup \bigcap\limits_{A \in S_1} \overline{A} | \bigcap\limits_{A \in S_2} \overline{A})}{P(\bigcap\limits_{A \in S_1} \overline{A} | \bigcap\limits_{A \in S_2} \overline{A})}$$

Оценим числитель и знаменатель, используя утверждение: $P(A \cap B|C) \leqslant P(A|C)$.

$$(\text{Числитель}) \leqslant P(A_i | \bigcap_{A \in S_1} \overline{A}) = P(A_i) \leqslant x_i \cdot \prod_{A_j \in S_1} (1 - x_j)$$

Докажем, что

$$(\text{Знаменатель}) \geqslant \prod_{A_j \in S_1} (1 - x_j)$$

Не ограничивая общности, будем считать, что $|S_2| > 0$, тогда $|S_1| < s$.
Формула полной вероятности:

$$P(B_1 \cap \ldots \cap B_r) = P(B_1) \cdot P(B_2|B_1) \cdot P(B_3|B_1 \cap B_2) \cdot \ldots \cdot P(B_n|B_1 \cap \ldots \cap B_{n-1})$$

Формула полной условной вероятности:

$$P(B_1 \cap \ldots \cap B_n|C) = P(B_1|C) \cdot \ldots \cdot P(B_n|B_1 \cap \ldots \cap B_{n-1} \cap C)$$

Тогда

$$(\ -\ ) = P(\overline{A}_{j_1}|\bigcap A \in S_2 \cdot P(\overline{A}_{j_2}|\overline{A}_{j_1} \cap \bigcap_{A \in S_2} A) \cdot \ldots \cdot P(\overline{A}_{j_r}|\overline{A}_{j_1} \cap \ldots \cap \overline{A}_{j_{r-1}} \cap \bigcap_{A \in S_2} A)$$

По предположению индукции $P(A_{i-1}|\bigcap\limits_{A \in S_2} A) \leqslant x_i$, поэтому каждый множитель из оценки знаменателя мы можем оценить снизу как $P(\overline{A}_k|\ldots) \geqslant (1 - x_{j_k})$. Отсюда получаем:

$$(\text{Знам-ль}) \geqslant \prod_{A \in S_1} (1 - x_j)$$

Для получения итогового результата, применим формулу полной вероятности:

$$P(A_i|\overline{A}_1 \cap \ldots \cap \overline{A}_n) = P(\overline{A}_1) \cdot P(\overline{A}_2|\overline{A}_1) \cdot \ldots \cdot P(\overline{A}_n|\overline{A}_1 \cap \ldots \cap \overline{A}_{n-1}) \geqslant$$

$$\geqslant \prod_{i=1}^{n} (1 - x_i)$$

□

Определение 8.5. *k-однородный гиперграф* - это гиперграф, в котором любое ребро имеет мощность k.

Определение 8.6. *k-регулярный гиперграф* - это гиперграф, в котором любая вершина содержится ровно в k рёбрах.

Замечание 8.7. Правильная раскраска гиперграфа - это такая раскраска вершин, при которой нет одноцветных рёбер.

Теорема 8.8.
(Эрдёш, Ловас) *Если $k \geqslant 9$, то любой k-однородный и любой k-регулярный гиперграф может быть правильно раскрашен в два цвета.*

Доказательство.

Рассмотрим случай раскраски в два цвета.
Пусть A_i='i-е ребро стало одноцветным'

$$P(A_i) = 2^{1-k}$$

A_i зависит не более, чем от $k(k-1)$ событий. Если $e \cdot 2^{1-k}(k(k-1)+1) \leqslant 1$, то можно применить (8.4) симметричный случай Локальной Леммы Ловаса, откуда следует, что при $k \geqslant 9$ это неравенство выполняется. □

Докажем несколько вспомогательных утверждений, которые понадобятся для дальнейшей работы.

Утверждение 8.9.
(Неравенство Маркова) *Пусть x — неотрицательная случайная величина. Тогда*

$$P(x \geqslant t) \leqslant \frac{\mathbb{E}x}{t}$$

Доказательство.

$$\mathbb{E}x = \sum_x P(X = x) \cdot x = \underbrace{\sum_{x \geqslant t}(X = x)}_{\geqslant \sum\limits_{x \geqslant t} P(X=x)\cdot x} + \underbrace{\sum_{x<1} P(X = x) \cdot x}_{\geqslant 0}$$

При делении обоих слагаемых на t получаем неравенство Маркова.

□

Утверждение 8.10.

$$\frac{e^{\lambda} + e^{-\lambda}}{2} \leqslant e^{\frac{\lambda^2}{2}}$$

Доказательство.

$$\frac{1}{2}(e^{\lambda} + e^{-\lambda}) = \frac{1}{2}(1 + \frac{\lambda}{1!} + \frac{\lambda^2}{2!} + \ldots + 1 - \frac{\lambda}{1!} + \frac{\lambda^2}{2!} - \frac{\lambda^3}{3!} + \ldots) =$$
$$= 1 + \frac{\lambda^2}{2!} + \frac{\lambda^4}{4!} + \frac{\lambda^6}{6!} + \ldots$$

В то же время:

$$e^{\frac{\lambda^2}{2}} = 1 + \frac{\lambda^2}{2!} + \frac{\lambda^4}{2^2 \cdot 2} + \ldots,$$

т.е. утверждение верно. □

Утверждение 8.11.
(Оценка Чернова) *Пусть случайные величины $x_1, \ldots, x^n$ независимы, и $P(x_i = 1) = P(x_i = -1) = \frac{1}{2}$. Тогда для любого числа $a \geqslant 0$ вероятность того, что сумма этих величин сильно отклонится от нуля, не превосходит $e^{-\frac{a^2}{m}}$:*

$$P(\sum_{i=1}^{n} x_i > a) \leqslant e^{-\frac{a^2}{m}}$$

Доказательство.

$$P(\sum X_i > a) = P(e^{\lambda \cdot \sum x_i} > e^{\lambda a})$$

По (8.9) неравенству Маркова получаем:

$$\mathbb{E}e^{\lambda \sum x_i} = \mathbb{E}\prod_{i=1}^{n} e^{\lambda \sum x_i} = \underbrace{\prod_{i=1}^{n} \mathbb{E}e^{\lambda x_i}}_{= \frac{1}{2} \cdot e^{\lambda} + \frac{1}{2} \cdot e^{-\lambda} \leqslant e^{\frac{\lambda^2}{2}}} \leqslant (e^{\frac{\lambda^2}{2}})^n$$

Тогда:

$$P(e^{\lambda \cdot \sum x_i} > e^{\lambda a}) \leqslant \frac{(e^{\frac{\lambda^2}{2}})^n}{e^{\lambda a}} = e^{\frac{n\lambda^2}{2} - a\lambda} \leqslant \{\lambda = \frac{a}{n}\} \leqslant e^{-\frac{a^2}{2n}}$$

□

Теорема 8.12.
Пусть G — k-регулярный граф. Тогда в G существует остовный двудольный подграф, степени вершин в котором находятся в интервале

$$[\frac{k}{2} - 2\sqrt{k \log_2 k}; \quad \frac{k}{2} + 2\sqrt{k \log_2 k}]$$

Доказательство.

Рассмотрим случайную раскраску вершин в два цвета.
A_i =″⩾ $\frac{k}{2} + 2\sqrt{k \log_2 k}$ соседей окрашены в один и тот же цвет". Оценим следующее выражение сверху:

$$P(A_i) \leqslant 2 \cdot P(\sum x_j \geqslant 4\sqrt{k \log_2 k})$$

$$x_j = \begin{cases} 1, & \text{если } j\text{-й сосед } v_i \text{ — красный} \\ -1, & \text{если } j\text{-й сосед } v_i \text{ — синий} \end{cases}$$

Если среди x_j больше чем $\frac{k}{2} + 2\sqrt{k \log_2 k}$ элементов стали равны 1, то

$$\sum x_j \geqslant \frac{k}{2} + 2\sqrt{k \log_2 k} - \frac{k}{2} + 2\sqrt{k \log_2 k} = 4\sqrt{k \log_2 k}$$

Аналогичные рассуждения можно провести и для случая -1. Тогда используя (8.11) оценку Чернова, получим:

$$2 \cdot P(\sum x_j \geqslant 4\sqrt{k \log_2 k}) \leqslant 2 \cdot e^{-\frac{16k \log_2 k}{2k}} = 2e^{-8 \log_2 k}$$

A_i зависит не более, чем от k^2 других событий. Если $(k^2+1)e \cdot e^{-k \ln k} \leqslant 1$, то можно применить Локальную Лемму Ловаса, в результате которой получим:

$$P(\prod \overline{A}_i) > 0$$

Рассмотрим двудольный граф, у которого в одной доле все красные вершины, а в другой — все синие. Все ребра исходного графа соединяют пары вершин разного цвета. □

9 Линейно-алгебраические методы

9.1 Явная оценка чисел Рамсея

$2^{\frac{s}{2}} \leqslant R_2(s,s) \leqslant \frac{4^s}{\sqrt{\pi s}}$ - неявная(вероятностная) оценка числа Рамсея. В свою очередь, из явных оценок чисел Рамсея лучшей на сегодняшний день является следующая:

$$R_2(s,s) \geqslant (e^{\frac{1}{4}} + o(1))^{\frac{ln(s)^2}{ln(ln(s))}} \tag{6}$$

Данная оценка является субэкспоненциальной и сверхполиномиальной, то есть растёт медленнее, чем экспонента, но быстрее любого полинома.

Теорема 9.1 (Франкл-Уилсон)**.** *Рассмотрим граф G, вершины которого - всевозможные векторы длины m, координаты которых принимают значения 0 и 1, и в каждом векторе содержится ровно p^2 единиц, где $m = p^3$, p - простое число.*

$$V = \left\{ (x_1, \ldots, x_m), x_i \in \{0,1\}, \sum_{i=0}^{m} x_i = p^2 \right\}$$

Векторы в графе G соединены ребром, если скалярное произведение векторов равняется нулю по модулю p.

$$E = \{\vec{x} = (x_1, \ldots, x_m), \vec{y} = (y_1, \ldots, y_m) | \, \langle \vec{x}, \vec{y} \rangle = 0 (mod\ p)\}$$

Тогда можно утверждать, что граф G обладает следующими свойствами:

1) $\omega(G) \leqslant \sum\limits_{k=0}^{p-1} C_{p^3}^k$, *где* $\omega(G)$ *- размер максимальной клики в графе G;*

2) $\alpha(G) \leqslant \sum\limits_{k=0}^{p-1} C_{p^3}^k$, *где* $\alpha(G)$ *- максимальный размер независимого множества в графе G.*

Доказательство. Начнём с доказательства утверждения для множества $\alpha(G)$. Пусть векторы $\vec{x}_1, \ldots, \vec{x}_r$ образуют некоторое независимое множество в графе G. Рассмотрим в связи с каждым из этих векторов следующий полином: $F_{\vec{x}}(y_1, \ldots, y_m) = \prod_{i=1}^{p-1}(\langle \vec{x}, \vec{y} \rangle - \ i)$. Степень каждого такого полинома $\leqslant p-1$. Каждому такому полиному поставим в соответствие полином $\overline{F}_{\vec{x}}(\vec{y})$, получающийся из полинома $F_{\vec{x}}(\vec{y})$ путём замены мономов вида $y_{i_1}^{\alpha_1} \ldots y_{i_s}^{\alpha_s}$ на мономы вида $y_{i_1} \ldots y_{i_s}$(по сути дела ничего не меняется, так как $y_{i_1}, \ldots, y_{i_s}$ принимают значения 0 и 1, а, как известно, $0^\alpha = 0$ и $1^\alpha = 1$). Для полиномов $\overline{F}_{\vec{x}}(\vec{y})$ также верно утверждение о том, что их степень не превышает значения p-1. Выясним, когда эти полиномы обращаются в 0 по модулю p. Достаточно очевидно, что для любого вектора $\vec{x} \in V$ выполняется: $\overline{F}_{\vec{x}}(\vec{x}) \neq 0(mod\ p)$(в данном случае $\langle \vec{x}, \vec{x} \rangle = 0(mod\ p)$ и, следовательно, ни один из множителей $(\langle \vec{x}, \vec{x} \rangle - \ i)$ произведения $\prod_{i=1}^{p-1}(\langle \vec{x}, \vec{x} \rangle - \ i)$ не обращается в 0, как и, собственно, всё произведение).

Теперь для каждой пары векторов $\vec{x}_i, \vec{x}_j, i \neq j$, из независимого множества рассмотрим полином $\overline{F}_{\vec{x}_i}(\vec{x}_j)$. Так как векторы $\vec{x}_i$ и $\vec{x}_j$ принадлежат одному независимому множеству($\leftrightarrow$ не соединены ребром в графе G) и не совпадают, то $< \vec{x_i}, \vec{x_j} >\neq 0(mod\ p)$. Следовательно, в произведении $\prod_{i=1}^{p-1}(\langle \vec{x_i}, \vec{x_j} \rangle - \ i)$ один множитель обратится в 0,что повлечёт за собой обращение в 0 всего произведения.

В итоге получаем :

1)$\overline{F}_{\vec{x}}(\vec{x}) \neq 0(mod\ p)$, $\vec{x} \in V$;

2)$\overline{F}_{\vec{x}_i}(\vec{x}_j) = 0(mod\ p)$, $\vec{x}_i, \vec{x}_j, i \neq j$.

Покажем, что полиномы $\overline{F}_{\vec{x}_1}(\vec{y}), \ldots, \overline{F}_{\vec{x}_r}(\vec{y})$ линейно независимы в $\mathbb{F}_p[x_1, \ldots, x_r]$. Допустим, что это не так. Тогда существует нетривиальный набор коэффициентов $c_1, \ldots, c_r$ из множества $\{0, 1, \ldots, p-1\}$ такой, что $c_1\overline{F}_{\vec{x}_1}(\vec{y}) + \ldots + c_r\overline{F}_{\vec{x}_r}(\vec{y}) = 0(mod\ p)$. Будем подставлять в это уравнение поочерёдно вместо $\vec{y}$ векторы $\vec{x_1}, \ldots, \vec{x_r}$. Для каждого вектора $\vec{x_i}$ получим:

$c_1\overline{F}_{\vec{x_1}}(\vec{x_i}) + \ldots + c_i\overline{F}_{\vec{x_i}}(\vec{x_i}) + \ldots + c_r\overline{F}_{\vec{x_r}}(\vec{x_i}) = 0(mod\ p)$.

Как уже было показано выше, в данном уравнении все слагаемые, помимо $c_i\overline{F}_{\vec{x}_i}(\vec{x}_i)$, равны $0(mod\ p)$. В свою очередь, $\overline{F}_{\vec{x_i}}(\vec{x_i}) \neq 0(mod\ p)$, откуда следует, что $c_i = 0(mod\ p)$. В итоге $\forall i \in \{1, \ldots, r\}\ \ c_i = 0(mod\ p)$, что противоречит нетривиальности набора $c_1, \ldots, c_r$.

Доказав утверждение о линейной независимости полиномов $\overline{F}_{\vec{x}_1}(\vec{y}), \ldots, \overline{F}_{\vec{x}_r}(\vec{y})$ в $F_p[x_1, \ldots, x_r]$, убеждаемся в том, что $\overline{F}_{\vec{x}_1}(\vec{y}), \ldots, \overline{F}_{\vec{x}_r}(\vec{y})$ лежат в пространстве полиномов с коэффициентами из $\mathbb{F}_p = \{0, \ldots, p-1\}$ и степенью каждой переменной $\leqslant 1$. У этого пространства есть базис из независимых векторов :

$1, x_1, \ldots, x_m, \ldots, x_ix_j, \ldots$.

В этом базисе $1 + m + C_m^2 + \ldots + C_m^{p-1}$ функций. В итоге получаем верхнюю оценку для r :

$r \leqslant 1 + m + C_m^2 + \ldots + C_m^{p-1}$

Утверждение для множества $\alpha(G)$ доказано.

Для множества $\omega(G)$ утверждение доказывается аналогично, но с некоторыми отличиями:

рассматриваются полиномы вида $F_{\vec{x}}(y_1, \ldots, y_m) = \prod_{i=0}^{p-1}(\langle \vec{x}, \vec{y} \rangle - \ ip)$;

(здесь полином равен нулю в случае $\langle \vec{x}, \vec{y} \rangle = 0(mod\ p)$)

□

Теперь, если положим:

$s = (p+1)C_m^p$,

$n = C_m^{p^2}$,

то получим граф на n вершинах без клик и независимых множеств размера s.

9.2 Теоремы «о нулях»

Теорема 9.2 (Алон)**.** *Пусть $S_1, \ldots, S_n$ - множества элементов из поля $\mathbb{F}$. Определим полиномы g_i следующим образом:*

$g_i(x_i) = \prod_{s \in S_i}(x_i - s)$;

Тогда, если $f(x_1,\dots,x_n)\in F[x_1,\dots,x_m]$ *и обращается в 0 на наборах* $(s_1,\dots,s_n)$, *где* $s_1\in S_1,\dots,s_n\in S_n$, *то существуют полиномы* $h_1,\dots,h_n$ *такие, что:*

1)$deg(h_i)\leqslant deg(f)-deg(g_i)$;

2)$f=\sum\limits_{i=1}^{n}h_ig_i$.

Доказательство. Для доказательства этой теоремы воспользуемся следующим вспомогательным утверждением

Лемма 9.3.
Пусть $f(x_1,\dots,x_n)$ *- полином, имеющий по каждой переменной* x_i *степень* $\leqslant t_i$. *Пусть* $S_1,\dots,S_n$ *- такие множества элементов из поля* $\mathbb{F}$, *что* $|S_i|=t_i+1$. *Тогда, если* $f(s_1,\dots,s_n)=0$, *где* $s_1\in S_1,\dots,s_n\in S_n$, *то* $f\equiv 0$.

Доказательство.

Докажем по индукции. При $n=1$ получаем утверждение, известное из курса математического анализа. Пусть утверждение верно для $k=n-1$. Докажем его справедливость и для $k=n$. Полином из условия леммы допускает следующее представление:

$$f(x_1,\dots,x_n)=P_1(x_1,\dots,x_{n-1})x_n^{t_n}+P_2(x_1,\dots,x_{n-1})x_n^{t_{n-1}}+\dots+P_{n+1}(x_1,\dots,x_{n-1})x_n^0.$$

Если вместо $x_1,\dots,x_{n-1}$ подставить $s_1\in S_1,\dots,s_{n-1}\in S_{n-1}$, то получится полином от x_n.Если, в свою очередь, в него подставить $s_n\in S_n$, то получим 0 и по теореме из курса математического анализа:

$f(s_1,\dots,s_{n-1},x_n)\equiv 0\Rightarrow\forall i\ P_i(s_1,\dots,s_{n-1})=0$.

Следовательно к P_i применимо предположение индукции:

$P_i\equiv 0\Rightarrow f(x_1,\dots,x_n)\equiv 0$.

Утверждение доказано. □

Пусть $f(x_1,\dots,x_n)$ обращается в 0 на $(s_1,\dots,s_n)$, где $s_i\in S_i$.

$$g_i(x_i)=\sum_{s\in S_i}(x_i-s)=x_i^{t_i+1}+\sum_{k=0}^{t_i}x_i^kc_{i,k}\Rightarrow x_i^{t_i+1}=g_i(x_i)-\sum_{k=0}^{t_i}x_i^kc_{i,k}$$

Пользуясь последним равенством, в полиноме $f(x_1,\dots,x_n)$ заменим каждую степень x_i^t, где $t\geqslant t_i+1$. В результате получим :

$f(x_1,\dots,x_n)=\sum\limits_{i=1}^{n}h_ig_i+\{\ \leqslant t_i,\ \ 0\}$.

Теорема доказана.

□

Теорема 9.4 (Алон)**.** *Пусть* $f(x_1,\dots,x_n)$ *- полином степени* $\sum\limits_{i=1}^{n}t_i$, *и коэффициент при мономе* $x_1^{t_1}\dots x_n^{t_n}$ *не равен 0. Тогда, если* $S_1,\dots,S_n$ *- такие множества элементов, что* $|S_i|\geqslant t_i+1$, *то существуют* $s_1\in S_1,\dots,s_n\in S_n$ *такие, что* $f(s_1,\dots,s_n)\neq 0$.

Доказательство. Пусть $\forall s_i\in S_i\quad f(s_1,\dots,s_n)=0$. Тогда существуют полиномы h_i такие, что $f(x_1,\dots,x_n)=\sum\limits_{i=1}^{n}h_ig_i(x_i)$, где $g_i(x_i)=\prod\limits_{s\in S_i}(x_i-s);\quad deg(g_i(x_i))=t_i+1$. В полиноме $f(x_1,\dots,x_n)$ присутствует моном $x_1^{t_1}\dots x_n^{t_n}$, в то время как в $\sum\limits_{i=1}^{n}h_ig_i(x_i)$ этого монома нет, так как $deg(h_i)\leqslant deg(f)-deg(g_i)$ и моном не может быть получен ни из одного слагаемого этой суммы. Пришли к противоречию. Теорема доказана.

□

Теорема 9.5 (Коши-Дэвенпорт)**.** *Пусть* $A,B\subseteq Z_p;A+B=\{a+b|a\in A,b\in B\}$.

$A=\{0,\dots,k\};B=\{0,\dots,m\};A+B=\{0,\dots,k+m\}$.

Тогда $|A+B|\geqslant min\{p,|A|+|B|-1\}$.

Доказательство. а)В случае $|A|+|B|>p$ докажем, что $A+B=Z_p$, откуда будет следовать утверждение теоремы.

$\forall g\in Z_p\ g-B=\{g-b|b\in B\}$;

$|g-B|=|B|$;

$|g-B|+|A|\geqslant p+1\geqslant |Z_p|\Rightarrow$

$A\cap g-B\neq\oslash\Rightarrow g\in A+B\Rightarrow A+B=Z_p$.

б)Пусть $|A+B|\leqslant p$. Предположим, что утверждение теоремы неверно, то есть $|A+B|\leqslant |A|+|B|-2$. Отсюда следует, что существует множество $C\subseteq Z_p$ такое, что $A+B\subseteq C$ и $|C|=|A|+|B|-2<p$. Рассмотрим многочлен $f(x,y)=\prod\limits_{c\in C}(x+y-c)$. По построению:

$1)f(a,b)=0\ \forall a\in A,b\in B$;

$2)deg(f(x,y))=|C|=|A|+|B|-2$;

В $f(x,y)$ есть моном $x^{|A|-1}y^{|B|-1}$ с коэффициентом $c^{|A|-1}_{|A|+|B|-2}\neq 0(mod\ p)$ ($c^{|A|-1}_{|A|+|B|-2}=\frac{(|A|+|B|-2)!}{(|A|-1)!(|B|-1)!}$, в числителе число, не делящееся на p). При заданных условиях можно применить вторую теорему Алона: $\forall$ множеств S_1,S_2 таких, что $|S_1|\geqslant(|A|-1)+1, |S_2|\geqslant(|B|-1)+1$ существуют элементы $s_1\in S_1, s_2\in S_2$ такие, что $f(s_1,s_2)\neq 0$. Но это противоречит свойству 1) построенного многочлена при $S_1=A, S_2=B$. Теорема доказана. □

Теорема 9.6. *Если $H_1,\ldots,H_m$ - гиперплоскости, покрывающие все вершины n-мерного булевого куба, кроме одной(нулевой), то $m\geqslant n$.*

Доказательство. В общем случае гиперплоскость задаётся уравнением

$\langle a_i,\vec{x}\rangle=b_i$,

где a_i,b_i - некоторые коэффициенты и $b_i\neq 0$, если гиперплоскость не проходит через начало координат. Рассмотрим полином

$f(x_1,\ldots,x_m)=\prod\limits_{i=1}^{m}(b_i\ -\langle a_i,\vec{x}\rangle)-(\prod\limits_{i=1}^{m}b_i)\prod\limits_{j=1}^{n}(1-x_j)$.

Рассмотрим поведение этого полинома в точках булевого куба:

$1)f(0,\ldots,0)=0$;

$2)c_1,\ldots,c_n\in\{0,1\}, c_1^2+\ldots+c_n^2>0\ :\ f(c_1,\ldots,c_n)=0$;

$\Rightarrow$ во всех точках куба полином равен 0.

Если утверждение теоремы не выполнятеся и $m<n$, получим:

$deg(\prod\limits_{i=1}^{m}(b_i-\langle a_i,\vec{x}\rangle))\leqslant m$;

$deg((\prod\limits_{i=1}^{m}b_i)\prod\limits_{j=1}^{n}(1-x_j))=n$;

$\Rightarrow degf=n$.

Значит в f будет присутствовать моном $x_1\ldots x_n$(с коэффициентом $(-1)^{n-1}$). При заданных условиях можно применить вторую теорему Алона: $\forall S_1,\ldots,S_n:|S_i|\geqslant 2$ существуют $s_1\in S_1,\ldots,s_n\in S_n$ такие, что $f(s_1,\ldots,s_n)\neq 0$. Но это противоречит утверждению о том, что полином равен 0 во всех точках куба. Теорема доказана. □

Следующая теорема была предложена Артином в 1934 г., доказана Чивалли и дополнена Варнингом в 1935 г.

Теорема 9.7. *Пусть p - простое число. Рассмотрим m полиномов из кольца $Z_p[x_1,\ldots,x_n]$:*

$$P_1=P_1(x_1,\ldots,x_n),P_2=P_2(x_1,\ldots,x_n),\ldots,P_n=P_n(x_1,\ldots,x_n).$$

Тогда, если $n>\sum\limits_{i=1}^{m}deg(P_i)$ и существует набор $(c_1,\ldots,c_n)$, на котором все вышеперечисленные полиномы обращаются в 0, то имеется ещё один такой набор.

Доказательство. Пусть это неверно. Положим

$$f=f(x_1,\ldots,x_n)=\prod_{i=1}^{m}(1-P_i(x_1,\ldots,x_n)^{p-1})-\delta\prod_{j=1}^{n}\prod_{c\in Z_p,c\neq c_j}(x_j-c),$$

где δ подобрано так, что

$$f(c_1, \ldots, c_n) = 0.$$

Заметим, что это условие однозначно определяет значение δ, и это значение является ненулевым. Также заметим, что

$$f(s_1, \ldots, s_1) = 0 \ \forall s_i \in Z_p$$

Действительно, это выполняется при $(s_1, \ldots, s_n) = (c_1, \ldots, c_n)$. Для остальных значений $(s_1, \ldots, s_n)$ по предположению существует такой полином P_j, что $P_j(s_1, \ldots, s_n) \neq 0$, откуда следует $1 - P_j(s_1, \ldots, s_n)^{p-1} = 0$(малая теорема Ферма). К тому же с того момента, как $s_i \neq c_i$ для некоторого i, произведение $\prod\limits_{c \in Z_p, c \neq c_j} (x_j - c)$ обращается в 0, как и значение функции f на данном наборе $(s_1, \ldots, s_n)$.

Пусть $t_i = p - 1$ для каждого i.Заметим, что коэффициент при $\prod\limits_{i=1}^{n} x_i^{t_i}$ в функции f равен $-\delta \neq 0$, в то время как степень выражения

$$\prod_{i=1}^{m} (1 - P_i(x_i, \ldots, x_n)^{p-1})$$

есть $(p-1)\sum\limits_{i=1}^{m} deg(P_i) < (p-1)n$. И как следствие, положив $\forall i \ S_i = Z_p$ и используя 2ую теорему Алона, заключаем, что существуют $s_1, \ldots, s_n \in Z_p$, для которых $f(s_1, \ldots, s_n) \neq 0$, что противоречит утверждению о том, что $f(s_1, \ldots, s_1) = 0 \ \forall s_i \in Z_p$. Теорема доказана. □

Хорошо известная гипотеза Берга и Сойера, доказанная Таскиновым, говорит о том, что любой простой 4-связный граф содержит 3-связный подграф. Легко видеть, что это утверждение не выполняется для графов с кратными рёбрами, но также можно показать, что достаточно одного дополнительного ребра для существования 3-связного подграфа и в этом более общем случае.

Теорема 9.8. *Для любого простого числа p и ациклического графа $G = (V, E)$, средняя степень которого $> 2p - 2$, а максимальное значение степени, в свою очередь, равно $2p - 1$, содержит p-связный подграф.*

Доказательство. Обозначим через $(a_{v,e})_{v \in V, e \in E}$ матрицу инцидентности графа G, где $a_{v,e} = 1$ при $v \in e$ и $a_{v,e} = 0$ иначе. Сопоставим каждому ребру графа G переменную x_e и рассмотрим полином

$$F = \prod_{v \in V} [1 - (\sum_{e \in E} a_{v,e} x_e)^{p-1}] - \prod_{e \in E} (1 - x_e),$$

над $\mathbb{F}(p)$.Заметим, что $deg(F) = |E|$, в то время как максимальное значение, которое может принять степень первого слагаемого, равно $(p-1)|V| < |E|$ по предположению о средней степени G. Более того, коэффициент при $\prod\limits_{e \in E} x_e$ в F равен $(-1)^{|E|+1} \neq 0$. Как следствие, с учётом 2ой теоремы Алона, существуют такие значения $x_e \in \{0, 1\}$, что $F(x_e : e \in E) \neq 0$. По определению F вектор $(x_e : e \in E)$ не является нулевым, потому что в этом случае $F \equiv 0$. К тому же для этого вектора $\sum\limits_{e \in E} a_{v,e} x_e = 0 (mod\ p) \ \ \forall v$, потому что в другом случае F опять же обнулится. По этой причине в подграфе, состоящем из всех рёбер $e \in E$ таких, что $x_e = 1$, все степени кратны p, и, так как максимальная степень $< 2p$, то все положительные степени равны p - получаем p-связный подграф, что и требовалось доказать. □