

Министерство образования и науки Российской Федерации

Государственное образовательное учреждение
высшего профессионального образования
«Московский физико-технический институт (государственный
университет)»
Факультет инноваций и высоких технологий
Кафедра анализа данных

Магистерская диссертация

Тема: **Название моей работы (TODO)**

Направление: 010400
Прикладные математика и информатика

Выполнил:
студент 093 группы _____ Попов М.В.

Научный руководитель:
д.физ.-мат.н., проф.(todo) _____ Ромашенко А.Е.

г. Москва 2016

Содержание

Введение	3
Коммуникационная сложность	3
1.1 Постановка задачи	3
1.2 Одноцветные комбинаторные прямоугольники	4
1.3 Графовая интерпретация	5
Оценивание $bcc(G)$	7
2.1 Метод трудного множества	8
2.2 Метод Куликова-Юкны	9
2.3 Метод энтропийных неравенств	10
Геометрические конфигурации	12
3.1 Описание двудольного графа	12
3.2 Оценки для (p_γ, l_π)	12
3.3 Сравнение методов оценивания	15
Теорема Турана и граф четырехсторонников	17
4.1 Теорема Турана и ее следствие	17
4.2 Граф четырехсторонников	19
Случайные графы	21
5.1 Случайные двудольные графы Эрдеша-Реньи	21
5.2 Неравенство Хефдинга	22
5.3 Размер максимального паросочетания	24
5.4 Трудное множество и оценка Куликова-Юкны на случай- ных графах	26
5.5 Количество трудных множеств размера k	29
Обобщение методов оценивания	33
6.1 t -Мерная коммуникационная сложность	33
6.2 Одноцветные комбинаторные параллелепипеды	34
6.3 Метод трудного множества	35
6.4 Метод энтропийных неравенств	36

Список литературы	39
-----------------------------	----

Введение

(ToDo) Актуальность, новизна, краткая выжимка.

Коммуникационная сложность

1.1 Постановка задачи

Мы будем рассматривать задачи следующего вида: пусть имеются два человека, которые хотят совместно вычислить значение некоторой функции от двух переменных $f(x, y)$. По традиции мы будем называть первого участника игры Алисой, а второго – Бобом. Сложность у этой задачи в том, что Алиса знает только значение аргумента x , а Боб значение аргумента y . Алиса и Боб могут обмениваться сообщениями по каналу связи. Требуется вычислить значение $f(x, y)$, переслав по каналу связи минимальное количество информации.

Мы предполагаем, что Алиса и Боб заранее (до того, как им станут известны значения x и y) договариваются о коммуникационном протоколе — о наборе соглашений, какие именно данные и в каком порядке они будут пересылать друг другу при тех или иных значениях x и y .

Опишем теперь всю задачу более формально. Пусть имеются конечные множества X, Y, Z и задана некоторая функция $f : X \times Y \rightarrow Z$.

Определение. *Коммуникационным протоколом для вычисления некоторой функции $f : X \times Y \rightarrow Z$ называется ориентированное двоичное дерево со следующей разметкой на вершинах и ребрах:*

- каждая нелистовая вершина помечена буквой A или B ;
 - у вершин с пометкой A определена функция $g_i : X \rightarrow \{0, 1\}$;
 - у вершин с пометкой B определена функция $f_j : Y \rightarrow \{0, 1\}$;
- каждой листовой вершине сопоставлен элемент множества Z ;
- каждое ребро помечено 0 или 1.

Пусть Алиса и Боб договорились, что будут действовать по некоторому протоколу \mathcal{P} . Затем Алиса получила $x \in X$, а Боб получил $y \in Y$.

Поместим фишку в корневую вершину нашего протокола \mathcal{P} и будем перемещать ее вниз по дереву, последовательно удаляясь от корня, пока она не попадет в один из листьев. Перемещение фишки выполняется следующим образом. Если текущая вершина помечена буквой A , то это означает, что сейчас очередь Алисы. Она применяет функцию g_i текущей вершины к своему значению x . Алиса отправляет по каналу связи бит равный $g_i(x)$ и перемещает фишку по ребру, помеченному как $g_i(x)$. Боб получает отправленный бит и понимает куда была сдвинута фишка. Для вершин помеченных буквой B эту же процедуру выполняет Боб. Когда фишка попадает в лист дерева, записанное там значение $z \in Z$, объявляется результатом выполнения протокола.

Мы говорим, что протокол \mathcal{P} вычисляет функцию $f : X \times Y \rightarrow Z$, если для любого $x \in X$ и любого $y \in Y$ при движении из корня по пути, соответствующему заданным x и y , мы попадаем в лист, помеченный $z = f(x, y)$.

Определение. *Сложностью коммуникационного протокола называется его глубина. Коммуникационной сложностью функции f называется минимальная сложность протокола, вычисляющего f . Мы будем обозначать её $CC(f)$.*

1.2 Одноцветные комбинаторные прямоугольники

Определение. *Множество $S \subseteq X \times Y$ называется комбинаторным прямоугольником (или просто прямоугольным множеством), если существуют такие $A \subseteq X$ и $B \subseteq Y$, что $S = A \times B$.*

Пусть \mathcal{P} – некоторый коммуникационный протокол для вычисления функции $f : X \times Y \rightarrow Z$ и l – один из листьев протокола. Определим S_l как множество пар $(x, y) \in X \times Y$ таких, что на входе (x, y) Алиса и Боб, следуя протоколу \mathcal{P} , приходят в лист l .

Утверждение 1.1. *Для всякого коммуникационного протокола \mathcal{P} и для всякого листа l множество S_l является комбинаторным прямоугольником.*

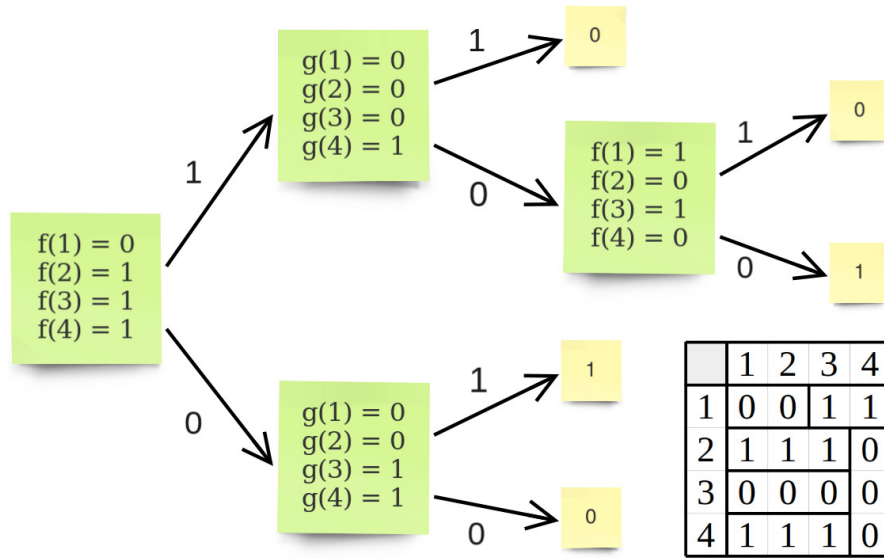


Рис. 1: Пример протокола и разбиения таблицы значений.

Доказательство этого утверждения можно прочитать, например, в [1]. В итоге мы получаем, что коммуникационный протокол для вычисления функции f задаёт разбиение $X \times Y$ - таблицы значений f на прямоугольные множества, соответствующие листьям. Поскольку каждому листу протокола приписано одно значение функции f , эти прямоугольные множества являются одноцветными, то есть во всех точках такого прямоугольного множества функция f принимает одно и то же значение. Например, для $X = Y = \{1, 2, 3, 4\}$, $Z = \{0, 1\}$ и протокола \mathcal{P} (рис. 1) получаем разбиение на 5 одноцветных прямоугольных множеств.

Подведем промежуточные итоги: всякий протокол с l листьями (вычисляющий функцию f) задаёт разбиение таблицы значений f на l одноцветных прямоугольных множеств. Значит, чтобы доказать, что коммуникационная сложность $CC(f)$ не меньше n , достаточно показать, что таблицу значений невозможно разбить на менее, чем 2^n одноцветных прямоугольных множеств.

1.3 Графовая интерпретация

Давайте теперь посмотрим на другое представление множества значений функции f . Рассмотрим полный двудольный граф $G = (X, Y, E)$, ребра которого раскрашены в $|Z|$ цветов. Вершины левой доли соот-

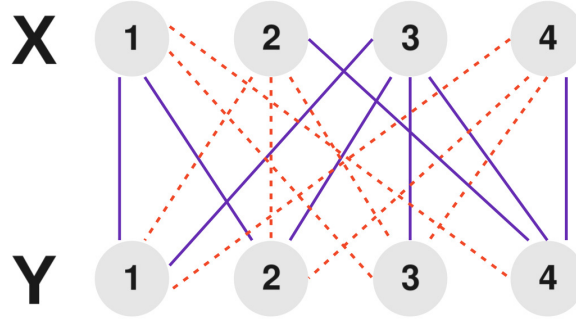


Рис. 2: Графовая интерпретация: синие – 0, красные – 1.

ветствуют элементам множества X , вершины правой доли – элементам множества Y . Ребро $(x, y) \in X \times Y$ имеет цвет $z \in Z$, если $f(x, y) = z$.

Из определения комбинаторного прямоугольника видно, что в графовой интерпретации он является ничем иным, как полным двудольным подграфом. А разбиение таблицы значений f на одноцветные прямоугольные множества – это разбиение нашего полного двудольного графа G на одноцветные непересекающиеся биклики (полные двудольные подграфы). Для нашего примера графовую интерпретацию можно посмотреть на рис. 2.

Определение. Бикликовым разбиением $bcp(G)$ двудольного графа G будем называть наименьшее число непересекающихся биклик, которыми можно покрыть все ребра графа G .

Определение. Бикликовым покрытием $bcc(G)$ двудольного графа G будем называть наименьшее число, возможно, пересекающихся биклик, которыми можно покрыть все ребра графа G .

Утверждение 1.2. Для произвольного двудольного графа G верно

$$bcp(G) \geq bcc(G)$$

Для каждого $z \in Z$ определим двудольный граф $G_z = (X, Y, E_z)$, как граф, получающийся из G выкидыванием всех ребер цвета, отличного от z . Иначе говоря $E_z = \{(x, y) \in X \times Y \mid f(x, y) = z\}$.

Величины $bcp(G_z)$ и $bcc(G_z)$ дают некоторую нижнюю оценку на коммуникационную сложность функции f , с которой намного удобнее рабо-

тать:

$$2^{CC(f)} \geq \sum_{z \in Z} bcp(G_z) \geq \sum_{z \in Z} bcc(G_z)$$

Замечание. На самом деле величины $bcc(G_z)$ тесно связаны с неопределенной коммуникационной сложностью $NCC(f)$. Для произвольного множества Z верно:

- $2^{NCC(f)} \geq \sum_{z \in Z} bcc(G_z)$,
- $NCC(f) \leq \lceil \log_2(\sum_{z \in Z} bcc(G_z)) \rceil + 1$

Иначе говоря, величины $bcc(G_z)$ и $NCC(f)$ по существу задают одну и ту же меру "сложности" функции f . Подробнее про это можно прочитать, например, в [2].

В итоге мы получили мощный инструмент для доказательства нижних оценок коммуникационной сложности. К сожалению, задача нахождения величины $bcc(G)$ является PSPACE-полной [3], а точное значение известно только для очень скудного класса графов (например, для "crown graphs" [4]), поэтому напрямую мы не можем использовать эту оценку. В следующей главе я рассмотрю несколько методов, позволяющих для произвольного двудольного графа оценивать снизу величину $bcc(G)$.

Оценивание $bcc(G)$

В этом разделе я опишу три различных метода оценивания бикликового покрытия:

- метод трудного множества ("fooling set");
- метод Куликова-Юкны;
- метод энтропийных неравенств.

Первые два метода работают для произвольных графов (необязательно двудольных), а третий применим к большому классу двудольных графов.

2.1 Метод трудного множества

Данный метод тесно связан с одноцветными прямоугольными множествами. Классическое определение трудного множества выглядит следующим образом:

Определение. Для функции $f : X \times Y \rightarrow Z$ и элемента $z \in Z$ будем называть множество $S_z \subset X \times Y$ трудным (в англоязычной литературе *fooling set*), если верно:

- для всякой пары $(x, y) \in S_z$ имеем $f(x, y) = z$;
- для любых двух несовпадающих пар $(x, y) \in S_z$ и $(x', y') \in S_z$ имеем $f(x, y') \neq z$ или $f(x', y) \neq z$.

Нас будет интересовать немного более общее определение трудного множества (графовая интерпретация):

Определение. Пусть $G = (V, E)$ произвольный неориентированный граф. Будем называть подмножество ребер $S \subseteq E$ трудным, если для любых двух различных ребер $(x, y) \in S$ и $(x', y') \in S$ имеем $(x, y') \notin E$ или $(x', y) \notin E$. Обозначение $\text{fool}(G)$ - размер максимального по мощности трудного множества.

Замечание. Классическое определение получается из графового, применением к двудольному графу $G_z = (X, Y, E_z)$, который строится по функции $f : X \times Y \rightarrow Z$.

Теорема 2.1. Для произвольного неориентированного графа $G = (V, E)$, если подмножество ребер $S \subseteq E$ является трудным, то $\text{bcs}(G) \geq |S|$.

Доказательство. Достаточно доказать, что два ребра, лежащие одновременно в одном трудном множестве, не могут попасть в одну биклику. Пусть не так, значит существуют два ребра $(x, y) \in B \cap S$ и $(x', y') \in B \cap S$, где B - биклика, а S - трудное подмножество ребер. Но тогда ребра (x, y') и (x', y) также принадлежат биклике B , а значит лежат и в нашем множестве ребер E . Противоречие. ■

2.2 Метод Куликова-Юкны

Следующий метод был впервые описан в статье [5], и работает он для произвольного неориентированного графа.

Теорема 2.2. *Для произвольного неориентированного графа $G = (V, E)$ верно:*

$$bcc(G) \geq \left\lceil \frac{v(G)^2}{|E|} \right\rceil$$

где $v(G)$ – размер максимального паросочетания графа G .

Доказательство. Пусть $M \subseteq E$ – это максимальное паросочетание, тогда рассмотрим бикликовое покрытие, на котором достигается минимум $E = B_1 \cup B_2 \cup \dots \cup B_{bcc(G)}$. Определим отображение $g : M \rightarrow \{1, \dots, bcc(G)\}$, как $g(e) = \min\{i \mid e \in B_i\}$ и пусть $M_i = \{e \in M \mid g(e) = i\}$. Иначе говоря M_i содержит только те ребра максимального паросочетания M , которые покрываются бикликой B_i в первый раз.

Пусть $F_i \subseteq B_i$ биклика, индуцированная вершинами ребер из M_i . Пусть $F = F_1 \sqcup F_2 \sqcup \dots \sqcup F_{bcc(G)}$ (биклики F_i не пересекаются по построению).

Очевидно, что F_i – биклика размера $r_i \times r_i$, где $r_i = |M_i|$. Получаем следующие соотношения:

$$r_1 + r_2 + \dots + r_{bcc(G)} = |M| = v(G)$$

и

$$r_1^2 + r_2^2 + \dots + r_{bcc(G)}^2 = |F|$$

Из неравенства Коши-Буняковского получаем

$$v(G)^2 = (r_1 + r_2 + \dots + r_{bcc(G)})^2 \leq bcc(G) \cdot (r_1^2 + r_2^2 + \dots + r_{bcc(G)}^2) = bcc(G) \cdot |F|$$

А так как $F \subseteq E$, то

$$v(G)^2 \leq bcc(G) \cdot |F| \leq bcc(G) \cdot |E| \blacksquare$$

В этой же статье [5] этот метод сравнивался с другой оценкой: пусть

$bcl(G) = \max_{K_{r,r} \subseteq G} \{r\}$, тогда

$$bcc(G) \geq \left\lceil \frac{v(G)}{bcl(G)} \right\rceil \quad (*)$$

Данная оценка очевидным образом следует из того, что любая биклика $K_{r,s}$ содержит как максимум $\min\{r, s\}$ ребер максимального паросочетания.

Приведем примеры графов, на которых метод Куликова-Юкны работает намного лучше, чем оценка (*), и наоборот:

- пусть двудольный граф $G = (L, R, E)$ состоит из совершенного паросочетания размера $n = |L| = |R|$ и еще некоторого константного числа непересекающихся биклик $K_{r,r}$. К тому же, пусть $r = \Theta(\sqrt{n})$, тогда

$$\left\lceil \frac{v(G)^2}{|E|} \right\rceil = \left\lceil \frac{n^2}{cr^2 + n} \right\rceil = \Theta(n) \gg \Theta(\sqrt{n}) = \left\lceil \frac{n}{r} \right\rceil = \left\lceil \frac{v(G)}{bcl(G)} \right\rceil$$

- рассмотрим двудольный граф Леви, построенный при помощи конечной проективной плоскости порядка $p \in \mathbb{P}$. В каждой доле этого графа содержится $n = p^2 + p + 1$ вершин, причем степень каждой $p + 1$. Этот граф не содержит $K_{2,2}$ (любые две прямые пересекаются максимум в одной точке). А так как в регулярных двудольных графах обязательно найдется совершенное паросочетание, то

$$\begin{aligned} \left\lceil \frac{v(G)^2}{|E|} \right\rceil &= \left\lceil \frac{(p^2 + p + 1)^2}{(p^2 + p + 1)(p + 1)} \right\rceil = \Theta(\sqrt{n}) \ll \\ &\ll \Theta(n) = \left\lceil \frac{p^2 + p + 1}{1} \right\rceil = \left\lceil \frac{v(G)}{bcl(G)} \right\rceil \end{aligned}$$

2.3 Метод энтропийных неравенств

Следующий метод оценивания бикликового покрытия был описан в статье [6], как результат применения энтропийного неравенства:

$$H(A|B, X) + H(A|B, Y) \leq H(A|B)$$

К сожалению, это неравенство выполняется не для произвольного совместного распределения случайных величин A, B, X, Y , и соответственно на двудольный граф будет накладываться дополнительное условие (**).

Теорема 2.3. Пусть ребра двудольного графа $G = (L, R, E)$ раскрашены следующим образом:

(**) для произвольной биклики $C \subseteq E$ и для произвольной пары ребер (x, y') и (x', y) из C , покрашенных в цвет a , цвет ребер (x, y) и (x', y') тоже a .

Пусть также на ребрах этого графа задано произвольное вероятностное распределение. Определим случайные величины (X, Y, A) следующим образом:

- $X = [\text{левый конец ребра}]$,
- $Y = [\text{правый конец ребра}]$,
- $A = [\text{цвет ребра}]$.

Тогда выполняется неравенство:

$$b_{cc}(G) \geq 2^{\frac{1}{2}(H(A|X)+H(A|Y)-H(A))}$$

Пример. Определим двудольный граф $G_{n,k} = (L, R, E)$ следующим образом:

- L и R всевозможные k -элементные подмножества $\{1, 2, \dots, n\}$,
- $E \subseteq L \times R$ состоит из пар непересекающихся множеств.

Определим цвет ребра $(x, y) \in E$, как $x \sqcup y$, и пусть на ребрах задано равномерное распределение. Условие (**) выполнено, потому что любые два одноцветных ребра не могут лежать в одной биклике. А так как $H(A|X) = H(A|Y) = \log_2 \binom{n-k}{k}$ и $H(A) = \log_2 \binom{n}{2k}$, то

$$b_{cc}(G_{n,k}) \geq \sqrt{\binom{n-k}{k}^2 / \binom{n}{2k}}$$

Если $n \gg k$, то $\binom{n-k}{k}^2 / \binom{n}{2k}$ близко к $\binom{2k}{k} \approx 2^{2k}$ и мы получаем нижнюю оценку $b_{cc}(G_{n,k}) \geq 2^k$.

Геометрические конфигурации

В этом разделе мы приведем класс двудольных графов, построенных при помощи некоторой геометрической конфигурации Γ . Мы увидим, что к этим двудольным графам применимы все наши оценки, и поэтому, изменяя Γ , мы можем сравнить какие методы работают лучше, а какие хуже.

3.1 Описание двудольного графа

Определение. Геометрической конфигурацией Γ (*Partial Linear Space*) будем называть конечное множество прямых A и конечное множество точек V на них, что выполняются следующие две аксиомы:

- Любые две точки лежат как максимум на одной прямой.
- На каждой прямой лежит хотя бы две точки.

Определение. Геометрической конфигурацией с параметрами (p_γ, l_π) будем называть такую конфигурацию, которая состоит из p точек и l прямых, причем через каждую точку проходит ровно γ прямых и на каждой прямой лежит ровно π точек.

Пусть у нас имеется некоторая геометрическая конфигурация $\Gamma = (V, A)$, тогда определим двудольный граф $G_{n,\Gamma} = (L, R, E)$ следующим образом:

- $L = R = V^n$
- $E = \{(x, y) \in L \times R \mid \forall i : x_i \neq y_i \text{ и лежат на одной прямой из } A\}$

3.2 Оценки для (p_γ, l_π)

Для геометрической конфигурации Γ с параметрами (p_γ, l_π) (предполагаем, что $l \geq 3$) найдем какие оценки на $bcc(G_{n,\Gamma})$ дают наши методы:

– Метод трудного множества:

Лемма 3.1. Если в Γ имеется цикл нечетной длины, то в $G_{1,\Gamma}$ можно найти трудное множество размера 3.

Доказательство. Рассмотрим нечетный цикл минимальной длины $\{v_1, v_2, \dots, v_{2k+1}\}$, где $k \geq 1$. Заметим, что прямые могут проходить только через соседние точки этого цикла, иначе бы мы нашли нечетный цикл меньшей длины. Тогда, если $k > 1$, то множество ребер $\{(v_1, v_2), (v_2, v_3), (v_3, v_4)\}$ образует трудное множество, а если $k = 1$, то $\{(v_1, v_2), (v_2, v_3), (v_3, v_1)\}$ образует трудное множество. \square

Замечание. Если на какой-нибудь прямой лежит по крайней мере три точки v_1, v_2, v_3 , то мы можем найти трудное множество $\{(v_1, v_2), (v_2, v_3), (v_3, v_1)\}$ размера 3.

Если в Γ нет нечетных циклов и на каждой прямой лежит ровно 2 точки, то мы получаем геометрическую конфигурацию, аналогичную двудольному графу. Если этот двудольный граф полный, то наибольшее трудное множество имеет размер 2, а если неполный, то рассмотрим два случая:

- 1) Если $\gamma = 1$, то Γ является паросочетанием, а значит все ребра графа $G_{1,\Gamma}$ образуют трудное множество (ребер ровно $l \geq 3$).
- 2) Если $\gamma \geq 2$ и нет прямой проходящей через точки v_1 и v_2 из разных долей, то существуют точки v_3, v_4, v_5, v_6 такие, что прямые проходят через пары точек $(v_1, v_4), (v_2, v_3)$ и (v_2, v_5) . Но тогда множество ребер $\{(v_1, v_4), (v_3, v_2), (v_2, v_5)\}$ образуют трудное множество размера 3.

Иначе говоря, мы показали, что если Γ аналог не полного двудольного графа, то мы можем найти трудное множество размера 3.

Лемма 3.2. Если в $G_{1,\Gamma}$ существует трудное множество размера k , то в $G_{n,\Gamma}$ существует трудное множество размера k^n

Доказательство. Докажем вначале, что если в графе G_1 имеется трудное множество размера n_1 , а в графе G_2 – трудное множество размера n_2 , тогда в $G_1 \otimes G_2$ можно найти трудное множество размера $n_1 \cdot n_2$ (где \otimes – произведение Кронекера). Пусть $\{v_{i,j}\}$ трудное множество в графе G_1 , тогда в каждой подматрице $v_{i,j} \cdot G_2$ матрицы графа $G_1 \otimes G_2$ рассмотрим клетки, соответствующие

трудному множеству графа G_2 . Всего мы получили $n_1 \cdot n_2$ клеток, образующих трудное множество графа $G_1 \otimes G_2$ по построению. Вернемся к доказательству леммы. Так как матрица графа $G_{n,\Gamma}$ есть не что иное, как Кронекерово произведение n матриц графа $G_{1,\Gamma}$, то мы можем найти трудное множество размера k^n . \square

В итоге мы получили, что если Γ является аналогом полного двудольного графа, то

$$bcc(G_{n,\Gamma}) \geq 2^n$$

иначе

$$bcc(G_{n,\Gamma}) \geq 3^n$$

– Метод Куликова-Юкны:

Так как Γ имеет параметры (p_γ, l_π) , то каждая вершина графа $G_{1,\Gamma}$ соединена с $\gamma \cdot (\pi - 1)$ другими, а значит всего ребер $\gamma \cdot (\pi - 1) \cdot p$. Тогда в графе $G_{n,\Gamma}$ всего ребер $\gamma^n \cdot (\pi - 1)^n \cdot p^n$. Так как у нас однородный двудольный граф, то имеется совершенное паросочетание, а значит $v(G_{n,\Gamma}) = p^n$. В итоге получаем оценку:

$$bcc(G_{n,\Gamma}) \geq \frac{p^{2n}}{\gamma^n \cdot (\pi - 1)^n \cdot p^n} = \left(\frac{p}{\gamma \cdot (\pi - 1)} \right)^n$$

– Метод энтропийных неравенств:

Определим раскраску ребер нашего графа $G_{n,\Gamma} = (L, R, E)$: сопоставим каждой прямой из конфигурации Γ свой цвет, тогда цвет ребра $(x, y) \in E$ равен n -мерному вектору цветов прямых, проходящих через x_i и y_i .

Проверим свойство (**): пусть (x, y') и (x', y) одного цвета и лежат в одной биклике C , значит для любого i точки x_i, y'_i, x'_i, y_i лежат на одной прямой (некоторые точки могут совпадать), но тогда очевидно, что ребро (x, y) такого же цвета.

Пусть на ребрах графа задано равномерное распределение, тогда $H(A) = \log_2 l^n = n \cdot \log_2 l$ и $H(A|X) = H(A|Y) = \log_2 \gamma^n = n \cdot \log_2 \gamma$.

В итоге получаем оценку:

$$bcc(G_{n,\Gamma}) \geq 2^{n \cdot \log_2 \gamma - \frac{n}{2} \cdot \log_2 l} = \left(\frac{\gamma}{\sqrt{l}} \right)^n$$

3.3 Сравнение методов оценивания

Рассмотрим какие оценки получаются на известных геометрических конфигурациях. Симметричные конфигурации ($p = l$ и $\gamma = \pi$) будем обозначать сокращенно (p_γ) .

Название	FS	KJ	EI	Результат
Треугольник (3 ₂)	$\geq 3^n$	$\left(\frac{3}{2}\right)^n$	$\left(\frac{2}{\sqrt{3}}\right)^n$	$FS > KJ > EI$
Полный четырех- сторонник (4 ₃ , 6 ₂)	$\geq 3^n$	$\left(\frac{4}{3}\right)^n$	$\left(\frac{3}{\sqrt{6}}\right)^n$	$FS > KJ > EI$
K_m при $m > 4$ $(m_{m-1}, \binom{m}{2}_2)$	$\geq 3^n$	$\left(\frac{m}{m-1}\right)^n$	$\left(\sqrt{\frac{2(m-1)}{m}}\right)^n$	$FS > EI > KJ$
$K_{m,m}$ при $m > 0$ $(2m_m, m_2^2)$	$\geq 2^n$	2^n	1^n	$FS = KJ > EI$
Плоскость Фано (7 ₃)	$\geq 3^n$	$\left(\frac{7}{6}\right)^n$	$\left(\frac{3}{\sqrt{7}}\right)^n$	$FS > KJ > EI$
Конфигурация Мёбиуса-Кантора (8 ₃)	$\geq 3^n$	$\left(\frac{4}{3}\right)^n$	$\left(\frac{3}{\sqrt{8}}\right)^n$	$FS > KJ > EI$
Конфигурация Дезарга (10 ₃)	$\geq 3^n$	$\left(\frac{5}{3}\right)^n$	$\left(\frac{3}{\sqrt{10}}\right)^n$	$FS > KJ > EI$
Конфигурация Гессе (9 ₄ , 12 ₃)	$\geq 3^n$	$\left(\frac{9}{8}\right)^n$	$\left(\frac{2}{\sqrt{3}}\right)^n$	$FS > EI > KJ$
Конфигурация Шлефли (12 ₅ , 30 ₂)	$\geq 3^n$	$\left(\frac{12}{5}\right)^n$	$\left(\frac{5}{\sqrt{30}}\right)^n$	$FS > KJ > EI$
Проективная плоскость $((m^2 + m + 1)_{m+1})$	$\geq 3^n$	$\left(\frac{m^2+m+1}{m(m+1)}\right)^n$	$\left(\frac{m+1}{\sqrt{m^2+m+1}}\right)^n$	$FS > EI > KJ$
Конфигурация Кокса $((2^{m-1})_m)$	$\geq 3^n$	$\left(\frac{2^{m-1}}{m(m-1)}\right)^n$	$\left(\frac{m}{\sqrt{2^{m-1}}}\right)^n$	$FS > KJ > EI$

Из таблицы видно, что метод трудного множества всегда работает лучше, чем остальные. Почти во всех примерах мы нашли трудное множество размера 3^n , но максимальное трудное множество может иметь очень большой размер. Оценки 3^n не достаточно, чтобы доказать, что на геометрических конфигурациях метод трудного множества всегда работает лучше, чем оценка Куликова-Юкны, но зато достаточно для метода

энтропийных неравенств:

Утверждение 3.1. Для произвольной геометрической конфигурации (p_γ, l_π) оценка, получаемая по методу трудного множества, превосходит оценку метода энтропийных неравенств. Иначе говоря

$$2 \geq \frac{\gamma}{\sqrt{l}}$$

Доказательство. Условия

$$\begin{cases} p \cdot \gamma = l \cdot \pi, \\ p \geq \gamma \cdot (\pi - 1) + 1. \end{cases}$$

должны обязательно выполняться для того, чтобы геометрическая конфигурация была корректно определена.

Используя эти ограничения, получаем

$$\frac{\gamma^2}{l} = \frac{\pi \cdot \gamma}{p} \leq \frac{p + \gamma - 1}{p} = 1 + \frac{\gamma - 1}{p} < 4$$

Что и требовалось доказать. \square

Теперь давайте сравним метод Куликова-Юкны и метод энтропийных неравенств. Рассмотрим два случая:

- Пусть выполняется условие $l \geq \gamma^2$, тогда

$$\gamma^2 \cdot (\pi - 1) \leq l \cdot (\pi - 1) < p \cdot \gamma \leq p \cdot \sqrt{l}$$

То есть получаем, что $KJ > EI$.

- Пусть теперь верно $l \leq \gamma^2$, тогда

$$\gamma^2 \cdot (\pi - 1) \geq l \cdot (\pi - 1) = p \cdot \gamma - l \geq p \cdot \sqrt{l} - l$$

Поделив обе части на $\sqrt{l} \cdot \gamma \cdot (\pi - 1)$, получаем

$$\frac{\gamma}{\sqrt{l}} \geq \frac{p}{\gamma \cdot (\pi - 1)} - \frac{\sqrt{l}}{\gamma \cdot (\pi - 1)}$$

В итоге получаем, что с небольшой погрешностью $EI \gtrsim KJ$

Теорема Турана и граф четырехсторонников

В этом разделе мы докажем, что метод трудного множества всегда дает оценку лучше, чем метод Куликова-Юкны. Также мы сведем задачу нахождения $bcc(G)$ к задаче поиска хроматического числа графа, что позволит нам получить переформулированный метод трудного множества и обобщение оценки (*).

4.1 Теорема Турана и ее следствие

Как уже видно из названия, для дальнейших изысканий нам потребуется классическая теорема Турана:

Теорема 4.1. (Туран) Пусть дан неориентированный граф $G = (V, E)$, где $|V| = n$ и число независимости равно α . Тогда в графе выполняется следующая оценка

$$|E| \geq n \cdot \left\lfloor \frac{n}{\alpha} \right\rfloor - \alpha \cdot \frac{\left\lfloor \frac{n}{\alpha} \right\rfloor \cdot \left(\left\lfloor \frac{n}{\alpha} \right\rfloor + 1 \right)}{2}$$

Доказательство этой теоремы можно найти в книге [7]. Используя эту теорему, мы можем доказать следующее:

Теорема 4.2. Пусть имеется неориентированный граф $G = (V, E)$, тогда среди ребер максимального паросочетания можно найти трудное множество размера

$$\left\lceil \frac{v(G)^2}{|E|} \right\rceil$$

Доказательство. Давайте вместо графа $G = (V, E)$ рассмотрим граф $\hat{G} = (\hat{V}, \hat{E})$, в котором останутся только вершины из максимального паросочетания. Так как $|E| \geq |\hat{E}|$, то достаточно найти трудное множество размера

$$\left\lceil \frac{v(G)^2}{|\hat{E}|} \right\rceil$$

Пусть $(v_1, v'_1), (v_2, v'_2), \dots, (v_m, v'_m)$ – ребра максимального паросочетания. Построим граф $\tilde{G} = (\tilde{V}, \tilde{E})$ такой, что вершин в нем ровно m .

Обозначим вершины $\{\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_m\}$, причем $\tilde{v}_i \leftrightarrow (v_i, v'_i)$. Определим множество ребер \tilde{E} следующим образом

$$(\tilde{v}_i, \tilde{v}_j) \in \tilde{E} \text{ если } (v_i, v'_i) \notin \hat{E} \text{ или } (v_j, v'_j) \notin \hat{E}$$

Очевидно, что трудное множество на ребрах максимального паросочетания соответствует клике в \tilde{G} такого же размера. Пусть число независимости дополнения графа \tilde{G} равно α , тогда мы можем предъявить трудное множество размера α . Используя теорему Турана для дополнения графа \tilde{G} , получаем

$$|\tilde{E}| \geq m \cdot \left\lfloor \frac{m}{\alpha} \right\rfloor - \alpha \cdot \frac{\left\lfloor \frac{m}{\alpha} \right\rfloor \cdot \left(\left\lfloor \frac{m}{\alpha} \right\rfloor + 1\right)}{2} =$$

Пусть $m = k \cdot \alpha + r$, где $r < \alpha$

$$= (k \cdot \alpha + r) \cdot k - \alpha \cdot \frac{k \cdot (k + 1)}{2} = \frac{\alpha \cdot k^2}{2} + r \cdot k - \frac{\alpha \cdot k}{2}$$

Так как каждое ребро из дополнения графа \tilde{G} порождает два ребра в \hat{G} , а также еще имеется m ребер самого паросочетания, то получаем

$$\begin{aligned} |\hat{E}| &\geq m + 2 \cdot \left(\frac{\alpha \cdot k^2}{2} + r \cdot k - \frac{\alpha \cdot k}{2} \right) = \\ &= \alpha \cdot k^2 + 2r \cdot k + r \geq \alpha \cdot k^2 + 2r \cdot k + \left\lfloor \frac{r^2}{\alpha} \right\rfloor = \left\lfloor \frac{m^2}{\alpha} \right\rfloor \end{aligned}$$

В итоге получили, что

$$|\hat{E}| \geq \left\lfloor \frac{m^2}{\alpha} \right\rfloor \iff \alpha \geq \left\lfloor \frac{m^2}{|\hat{E}|} \right\rfloor = \left\lfloor \frac{v(G)^2}{|\hat{E}|} \right\rfloor \blacksquare$$

Эта теорема говорит нам о том, что на любом неориентированном графе точная оценка по методу трудного множества лучше, чем оценка Куликова-Юкны.

4.2 Граф четырехсторонников

При доказательстве предыдущей теоремы мы использовали некоторый модифицированный граф $\tilde{G} = (\tilde{V}, \tilde{E})$. По аналогии можно рассмотреть более общую конструкцию, которую мы будем называть графом четырехсторонников.

Определение. Пусть имеется двудольный неориентированный граф $G = (L, R, E)$. Определим граф четырехсторонников $\tilde{G} = (\tilde{V}, \tilde{E})$ следующим образом:

- $e_{i,j} \in E \leftrightarrow v_{i,j} \in \tilde{V}$, значит $|E| = |\tilde{V}|$.
- $(v_{i,j}, v_{k,l}) \in \tilde{E}$ тогда и только тогда, когда $v_{i,l} \notin \tilde{E}$ или $v_{k,j} \notin \tilde{E}$

Введем также понятия хроматического, кликового и антикликового чисел:

Определение. Хроматическое число графа G – минимальное число k такое, что множество вершин графа можно покрасить в k цветов, причем любое ребро графа соединяет разноцветные вершины. Обозначение $\chi(G)$.

Определение. Кликовое число графа G – максимальное число k такое, что в нашем графе содержится полный граф на k вершинах (k -клика). Обозначение $w(G)$.

Определение. Антикликовое число графа G – максимальное число k такое, что в графе дополнения содержится полный граф на k вершинах (k -антиклика). Обозначение $\alpha(G)$.

Используя конструкцию графа четырехсторонников, мы можем сформулировать следующую теорему:

Теорема 4.3. Для любого двудольного графа $G = (L, R, E)$ верно:

- 1) $fool(G) = w(\tilde{G})$
- 2) $\max_{K_{r,s} \subseteq G} \{r \cdot s\} = \alpha(\tilde{G})$
- 3) $bcc(G) = \chi(\tilde{G})$

Доказательство. Так как каждому трудному множеству размера k в G соответствует k -клика в \tilde{G} и наоборот, то $\text{fool}(G) = w(\tilde{G})$.

Очевидно, что биклике $K_{r,s}$ в G , соответствует антиклике размера $r \cdot s$ в \tilde{G} . Обратно, если $(v_{i,j}, v_{k,l}) \notin \tilde{E}$, то вершины $v_{i,l}$ и $v_{k,j}$ определены, и между ними нет ребра. И следовательно, если рассмотреть какую-нибудь антиклику в \tilde{G} , то ее можно расширить до "прямоугольной" антиклики, которой будет соответствовать биклика в G .

Последняя часть теоремы сразу следует из того, что все вершины антиклики мы можем красить в один цвет. Имея произвольное покрытие $\text{bcc}(G)$, мы получаем покрытие вершин графа \tilde{G} антикליками. Пусть каждой биклике из $\text{bcc}(G)$ сопоставлен свой цвет. Красим вершину в тот цвет, который соответствует покрывающей ее биклике (если таких биклик несколько, то в любой из них). В итоге получаем правильную раскраску графа в $\text{bcc}(G)$ цветов. Обратно, правильная покраска графа \tilde{G} порождает покрытие антикליками, которые мы расширяем до "прямоугольных". А так как эти антиклики соответствуют бикликам в G , то мы получили покрытие бикликами (возможно пересекающимися) размера $\chi(\tilde{G})$. ■

Эта теорема позволяет нам переформулировать известные оценки для хроматического числа нового графа \tilde{G} в виде оценок для величины трудного множества исходного графа G

$$\chi(\tilde{G}) \geq w(\tilde{G}) \iff \text{bcc}(G) \geq \text{fool}(G)$$

и

$$\chi(\tilde{G}) \geq \left\lceil \max_{U \subseteq \tilde{V}} \frac{|U|}{\alpha(\tilde{G}(U))} \right\rceil \iff \text{bcc}(G) \geq \left\lceil \max_{\mathcal{E} \subseteq E} \frac{|\mathcal{E}|}{\max_{K_{r,s} \subseteq G(\mathcal{E})} |K_{r,s} \cap \mathcal{E}|} \right\rceil$$

где $G(\mathcal{E})$ наименьший подграф G , содержащий все ребра \mathcal{E} .

Если в качестве \mathcal{E} рассмотреть максимальное паросочетание, тогда

$$\max_{K_{r,s} \subseteq G(\mathcal{E})} |K_{r,s} \cap \mathcal{E}| = \max_{K_{r,r} \subseteq G(\mathcal{E})} |K_{r,r} \cap \mathcal{E}| = \max_{K_{r,r} \subseteq G(\mathcal{E})} \{r\} \leq \max_{K_{r,r} \subseteq G} \{r\} = \text{bcl}(G).$$

В итоге получаем оценку, которую мы уже раньше встречали:

$$bcc(G) \geq \left\lceil \max_{\mathcal{E} \subseteq E} \frac{|\mathcal{E}|}{\max_{K_{r,s} \subseteq G(\mathcal{E})} |K_{r,s} \cap \mathcal{E}|} \right\rceil \geq \left\lceil \frac{v(G)}{bcl(G)} \right\rceil$$

Если же в качестве \mathcal{E} взять вообще все ребра, то

$$bcc(G) \geq \left\lceil \max_{\mathcal{E} \subseteq E} \frac{|\mathcal{E}|}{\max_{K_{r,s} \subseteq G(\mathcal{E})} |K_{r,s} \cap \mathcal{E}|} \right\rceil \geq \left\lceil \frac{|E|}{\max_{K_{r,s} \subseteq G} \{r \cdot s\}} \right\rceil$$

Случайные графы

В этом разделе мы докажем существование двудольных графов, у которых оценки по методу трудного множества и по методу Куликова-Юкны очень сильно отличаются. Доказывать этот факт мы будем вероятностным методом, причем будем использовать модель Эрдеша-Реньи.

5.1 Случайные двудольные графы Эрдеша-Реньи

Пусть у нас имеются два n -элементных множества L и R , элементы которого будем называть вершинами левой и правой долей графа. Понятно, что случайным будет множество ребер графа. Мы рассматриваем неориентированные графы без петель и кратных рёбер, поэтому потенциальных ребер не больше, чем n^2 штук. Будем соединять любые две вершины $i \in L$ и $j \in R$ ребром с некоторой вероятностью $p \in [0, 1]$ независимо от всех остальных $n^2 - 1$ пар вершин. Иными словами, ребра появляются в соответствии со стандартной схемой Бернулли, в которой n^2 испытаний и "вероятность успеха" p . Обозначим через E случайное множество ребер, которое возникает в результате реализации такой схемы. Положим $G = (L, R, E)$. Это и есть случайный двудольный граф в модели Эрдеша – Реньи.

Если записывать приведенное только что определение в формате аксиоматики Колмогорова, то мы имеем вероятностное пространство

$$G(n, p) = (\Omega_n, \mathcal{F}_n, P_{n,p})$$

в котором

$$\Omega_n = \{G = (L, R, E)\}, \mathcal{F}_n = 2^{\Omega_n}, P_{n,p}(G) = p^{|E|} \cdot (1-p)^{n^2-|E|}$$

Если нам хочется найти вероятность, с которой двудольный граф на $2n$ вершинах обладает данным свойством A , то мы просто берем множество $\mathcal{A} \in \mathcal{F}_n$, состоящее из всех графов, для которых выполнено свойство A , и вычисляем

$$P_{n,p}(\mathcal{A}) = \sum_{G \in \mathcal{A}} P_{n,p}(G)$$

Далее будем рассматривать не фиксированное p , а некоторую функцию $p(n)$, заключенную между нулем и единицей. Скажем, наконец, что свойство выполнено почти всегда, если его вероятность стремится к единице при $n \rightarrow \infty$.

5.2 Неравенство Хефдинга

Пусть $\xi_1, \xi_2, \dots, \xi_n$ — последовательность независимых случайных величин таких, что для любого $i = 1, 2, \dots, n$ верно $\xi_i \in [a_i, b_i]$ с вероятностью 1 для некоторых $a_i, b_i \in \mathbb{R}$. Введем обозначение $S_n = \sum_{i=1}^n \xi_i$. Мы хотим изучать отклонение случайной величины S_n от ее среднего значения $\mathbb{E}[S_n]$. Иначе говоря, получить неравенство концентрации для $\xi = S_n - \mathbb{E}[S_n]$. Воспользовавшись для этого неравенством Чернова получим, что для любого $\lambda > 0$ верно

$$\begin{aligned} P\{S_n - \mathbb{E}[S_n] \geq \varepsilon\} &= P\{e^{\lambda(S_n - \mathbb{E}[S_n])} \geq e^{\lambda\varepsilon}\} \leq \frac{\mathbb{E}[e^{\lambda(S_n - \mathbb{E}[S_n])}]}{e^{\lambda\varepsilon}} = \\ &= \frac{\mathbb{E}[e^{\lambda \sum_{i=1}^n (\xi_i - \mathbb{E}[\xi_i])}]}{e^{\lambda\varepsilon}} = \frac{\mathbb{E}[\prod_{i=1}^n e^{\lambda(\xi_i - \mathbb{E}[\xi_i])}]}{e^{\lambda\varepsilon}} = \frac{\prod_{i=1}^n \mathbb{E}[e^{\lambda(\xi_i - \mathbb{E}[\xi_i])}]}{e^{\lambda\varepsilon}} \end{aligned}$$

Нам остается построить верхние оценки для производящих функций $\varphi_{\xi_i}(\lambda)$. Следующий результат дает нам такие оценки в тех случаях, когда случайные величины ξ_i принимают значения из ограниченных интервалов.

Лемма 5.1. (Хефдинг) *Для произвольной случайной величины ξ та-*

кой, что $\mathbb{E}[\xi] = 0$ и $\xi \in [a, b]$ с вероятностью 1 для любого $\lambda > 0$ справедливо

$$\mathbb{E}[e^{\lambda \xi}] \leq e^{\frac{\lambda^2(b-a)^2}{8}}$$

Доказательство основано на выпуклости экспоненты.

Применив эту лемму к нашей цепочке неравенств для случайных величин $\xi_i - \mathbb{E}[\xi_i]$, которые почти наверное лежат в интервалах $[a_i - \mathbb{E}[\xi_i], b_i - \mathbb{E}[\xi_i]]$, мы получаем

$$P\{S_n - \mathbb{E}[S_n] \geq \varepsilon\} \leq \frac{\prod_{i=1}^n \mathbb{E}[e^{\lambda(\xi_i - \mathbb{E}[\xi_i])}]}{e^{\lambda \varepsilon}} \leq \frac{\prod_{i=1}^n e^{\lambda^2(b_i - a_i)^2/8}}{e^{\lambda \varepsilon}} = \frac{e^{\lambda^2 \sum_{i=1}^n (b_i - a_i)^2/8}}{e^{\lambda \varepsilon}}$$

Остается минимизировать правую часть по $\lambda \geq 0$. Выбирая

$$\lambda = \frac{4\varepsilon}{\sum_{i=1}^n (b_i - a_i)^2}$$

мы получаем следующий результат

Теорема 5.1. (Неравенство Хефдинга) Пусть $\xi_1, \xi_2, \dots, \xi_n$ — последовательность независимых случайных величин, таких что для любого $i = 1, 2, \dots, n$ верно $\xi_i \in [a_i, b_i]$ с вероятностью 1 для некоторых $a_i, b_i \in \mathbb{R}$. Тогда для любого $\varepsilon > 0$ верно

$$P\{S_n - \mathbb{E}[S_n] \geq \varepsilon\} \leq \exp\left(\frac{-2\varepsilon^2}{\sum_{i=1}^n (b_i - a_i)^2}\right)$$

Аналогичное неравенство верно для $P\{\mathbb{E}[S_n] - S_n \geq \varepsilon\}$, поскольку условия теоремы инвариантны относительно замены знака слагаемых. Применив дважды неравенство Хефдинга, мы получаем

$$\begin{aligned} P\{|S_n - \mathbb{E}[S_n]| \geq \varepsilon\} &\leq P\{S_n - \mathbb{E}[S_n] \geq \varepsilon\} + P\{\mathbb{E}[S_n] - S_n \geq \varepsilon\} \leq \\ &\leq 2 \cdot \exp\left(\frac{-2\varepsilon^2}{\sum_{i=1}^n (b_i - a_i)^2}\right) \end{aligned}$$

Воспользуемся этим неравенством для того, чтобы изучить отклонение числа ребер в случайном двудольном графе Эрдеша-Реньи. Определим индикаторные случайные величины $X_{i,j} = I\{e_{i,j} \in E\}$. Так как случайная величина $|E| = \sum_{i,j} X_{i,j}$, то получаем

$$\mathbb{E}[|E|] = \sum_{i,j} \mathbb{E}[X_{i,j}] = \sum_{i,j} P\{e_{i,j} \in E\} = n^2 \cdot p$$

Наконец, воспользуемся неравенством Хефдинга для $\varepsilon = n^{1+\delta}$

$$P\{||E| - \mathbb{E}[|E|]| \geq n^{1+\delta}\} \leq 2 \cdot e^{-\frac{2n^{2+2\delta}}{n^2}} = 2 \cdot e^{-2n^{2\delta}} \xrightarrow{n \rightarrow \infty} 0$$

В итоге мы получили, что почти наверное число ребер в графе не сильно отличается от его матожидания:

$$n^2 \cdot p - n^{1+\delta} \leq |E| \leq n^2 \cdot p + n^{1+\delta}$$

.

5.3 Размер максимального паросочетания

Для изучения отклонения величины максимального паросочетания нам потребуется теорема Холла.

Теорема 5.2. (Холл) Пусть имеется неориентированный двудольный граф $G = (L, R, E)$. Для произвольного $A \subseteq L$ определим множество соседей

$$N(A) = \{y \in R \mid (x, y) \in E, x \in A\}$$

В двудольном графе существует совершенное паросочетание тогда и только тогда, когда для любого $A \subseteq L$ выполнено $|A| \leq |N(A)|$.

Пусть имеется двудольный граф Эрдеша-Реньи $G = (L, R, E)$, где $|L| = |R| = n$. Множество $S \subseteq L$ не удовлетворяет условию теоремы Холла, если существует множество $T \subseteq R$ такое, что $|S| + |T| = n + 1$ и $N(S) \cap T = \emptyset$ (нет ребер между множествами S и T).

Очевидно, что

$$P\{N(S) \cap T = \emptyset\} = (1 - p)^{|S| \cdot |T|}$$

тогда

$$\begin{aligned} P\{\text{нет совершенного паросочетания}\} &\leq \sum_S \sum_T (1 - p)^{|S| \cdot |T|} = \\ &= \sum_{k=1}^n \binom{n}{k} \binom{n}{n-k+1} (1 - p)^{k(n-k+1)} \leq \sum_{k=1}^{(n+1)/2} \binom{n}{k} \binom{n}{k-1} (1 - p)^{kn/2} \leq \\ &\leq \sum_{k=1}^{(n+1)/2} n^{2k} (1 - p)^{kn/2} \end{aligned}$$

Если предположить, что $p = p(n) = n^{-\alpha}$ при $\alpha < 1$, то получаем

$$\begin{aligned} P\{\text{нет совершенного паросочетания}\} &\leq \sum_{k=1}^{(n+1)/2} n^{2k} (1 - p)^{kn/2} = \\ &= \sum_{k=1}^{(n+1)/2} n^{2k} e^{-\frac{kn}{2} \cdot n^{-\alpha} + O(n^{1-2\alpha}) \cdot k} = \sum_{k=1}^{(n+1)/2} \left(n^2 e^{-\frac{1}{2} n^{1-\alpha} + O(n^{1-2\alpha})} \right)^k \xrightarrow{n \rightarrow \infty} 0 \end{aligned}$$

Последнее утверждение верно потому, что с некоторого момента величина стоящая под степенью будет меньше 1, а значит первое слагаемое будет больше всех остальных

$$\sum_{k=1}^{(n+1)/2} \left(n^2 e^{-\frac{1}{2} n^{1-\alpha} + O(n^{1-2\alpha})} \right)^k \leq \frac{n+1}{2} \left(n^2 e^{-\frac{1}{2} n^{1-\alpha} + O(n^{1-2\alpha})} \right) \xrightarrow{n \rightarrow \infty} 0$$

В итоге мы получили, что почти наверное (при $n \rightarrow \infty$) в нашем графе будет совершенное паросочетание.

5.4 Трудное множество и оценка Куликова-Юкны на случайных графах

Если предположить, что $p = p(n) = n^{-\alpha}$ ($0 < \alpha < 1$), то можно доказать следующее утверждение:

Утверждение 5.1. *Для произвольного δ такого, что $0 < \delta < 1 - \alpha$ верно:*

$$n^\alpha - O(n^{2\alpha+\delta-1}) \leq \frac{v(G)^2}{|E|} \leq n^\alpha + O(n^{2\alpha+\delta-1})$$

Доказательство. Рассмотрим вероятность

$$\begin{aligned} P \left\{ \frac{n^2}{n^{2-\alpha} + n^{1+\delta}} \leq \frac{v(G)^2}{|E|} \leq \frac{n^2}{n^{2-\alpha} - n^{1+\delta}} \right\} &\geq \\ &\geq 1 - P \{v(G) \neq n\} - P \{|E| - n^{2-\alpha}| \geq n^{1+\delta}\} \xrightarrow{n \rightarrow \infty} 1 \end{aligned}$$

В параграфах 4.4 и 4.5 мы доказали, что соответствующие вероятности стремятся к 0 при $n \rightarrow \infty$, поэтому итоговая вероятность стремится к 1. Поделив числители и знаменатели на $n^{2-\alpha}$, получаем

$$\frac{n^\alpha}{1 + n^{\alpha+\delta-1}} \leq \frac{v(G)^2}{|E|} \leq \frac{n^\alpha}{1 - n^{\alpha+\delta-1}}$$

а так как $\alpha + \delta < 1$, то можно применить разложение в ряд Тейлора

$$n^\alpha (1 - O(n^{\alpha+\delta-1})) \leq \frac{v(G)^2}{|E|} \leq n^\alpha (1 + O(n^{\alpha+\delta-1})) \quad \square$$

Теперь посчитаем вероятность того, что в случайном графе найдется трудное множество размера k . Обозначим $f_k(G)$ - число различных трудных множеств размера k в графе G . Нас интересует вероятность $P\{f_k(G) > 0\}$, которая превосходит вероятность того, что фиксированные k пар вершин образуют трудное множество. Иначе говоря

$$P\{f_k(G) > 0\} \geq p^k (1 - p^2)^{\binom{k}{2}}$$

Предположим теперь, что $p = p(n) = n^{-\alpha}$ ($0 < \alpha < 1$) и величина

$k = k(n) = n^\beta$ ($0 < \beta < 2$), тогда

$$P\{f_k(G) > 0\} \geq n^{-\alpha k} e^{\binom{k}{2} \cdot (-n^{-2\alpha} + O(n^{-4\alpha}))} = n^{-\alpha n^\beta} e^{-\frac{1}{2}n^{2\beta-2\alpha} + \frac{1}{2}n^{\beta-2\alpha} + O(n^{2\beta-4\alpha})}$$

К тому же, если $0 < \delta < 1 - \alpha$ и мы докажем, что при $n \rightarrow \infty$

$$P\{f_k(G) > 0\} > P\{v(G) \neq n\} + P\{|E| - n^{2-\alpha} \geq n^{1+\delta}\}$$

то получим, что существует граф, у которого имеется трудное множество размера n^β и оценка Куликова-Юкны не превосходит $n^\alpha + O(n^{2\alpha+\delta-1})$. Чтобы это было верно, достаточно показать, что

$$n^{-\alpha n^\beta} e^{-\frac{1}{2}n^{2\beta-2\alpha} + \frac{1}{2}n^{\beta-2\alpha} + O(n^{2\beta-4\alpha})} > 2 \cdot e^{-2n^{2\delta}} + \sum_{i=1}^{(n+1)/2} \left(n^2 e^{-\frac{1}{2}n^{1-\alpha} + O(n^{1-2\alpha})} \right)^i$$

Сравним левую часть с каждым слагаемым из правой части по отдельности:

1) Если $2\delta > \beta > \alpha$ и $2\delta > 2\beta - 2\alpha$, то

$$-\alpha \cdot \ln n \cdot n^\beta - \frac{1}{2} \cdot n^{2\beta-2\alpha} \gg -2 \ln 2 \cdot n^{2\delta}$$

2) Поделим левую часть на n и сравним с первым членом суммы, заранее прологарифмировав. При $1 - \alpha > \beta > \alpha$ и $1 + \alpha > 2\beta$ верно

$$-\alpha \cdot \ln n \cdot n^\beta - 1 - \frac{1}{2} \cdot n^{2\beta-2\alpha} \gg 2 \ln n - \frac{1}{2} n^{1-\alpha}$$

что верно, так как

$$n^{1-\alpha} \gg \ln n, \quad n^{1-\alpha} \gg \ln n \cdot n^\beta, \quad n^{1-\alpha} \gg n^{2\beta-2\alpha}$$

Пример. Если взять $\alpha = 0.05$, $\beta = 0.5$ и $\delta = 0.5$, тогда все требуемые неравенства выполняются. А значит существует двудольный граф, на котором метод трудного множества дает оценку хотя бы $n^{0.5}$, а оценка Куликова-Юкны не превосходит $n^{0.05} + O(n^{-0.4})$.

Ограничение, которое накладываются только на α и β имеет вид

$\min \left\{ \frac{1+\alpha}{2}, 1-\alpha \right\} > \beta > \alpha$, а значит $\alpha \in [0, \frac{1}{2})$. Далее рассмотрим два случая:

1) Пусть $0 \leq \alpha < \frac{1}{3}$, тогда $\frac{1+\alpha}{2} < 1-\alpha$. А значит можно доказать следующую теорему:

Теорема 5.3. Для произвольных $\alpha \in [0, \frac{1}{3})$ и $\beta \in (\alpha, \frac{1+\alpha}{2})$ существует двудольный граф $G = (L, R, E)$ ($|L| = |R| = n$), на котором метод трудного множества дает оценку хотя бы n^β , а оценка Куликова-Юкны не превосходит $n^\alpha + o(1)$.

Доказательство. Пусть $\delta = \frac{1-\alpha}{2}$, тогда все неравенства, в которых участвует δ , выполняются:

- $\delta + \alpha = \frac{1-\alpha}{2} + \alpha = \frac{1+\alpha}{2} < 1$
- $2\delta = 1-\alpha > \frac{1+\alpha}{2} > \beta > \alpha$
- $\delta = \frac{1-\alpha}{2} = \frac{1+\alpha}{2} - \alpha > \beta - \alpha$

а значит существует граф, у которого метод трудного множества дает оценку n^β , а оценка по методу Куликова-Юкны не превосходит $n^\alpha + O(n^{2\alpha+\delta-1}) = n^\alpha + O(n^{2\alpha+\frac{1-\alpha}{2}-1}) = n^\alpha + O(n^{\frac{3\alpha-1}{2}}) = n^\alpha + o(1)$. ■

2) Пусть $\frac{1}{3} \leq \alpha < \frac{1}{2}$, тогда $\frac{1+\alpha}{2} \geq 1-\alpha$. А значит можно доказать следующую теорему:

Теорема 5.4. Для произвольных $\alpha \in [\frac{1}{3}, \frac{1}{2})$ и $\beta \in (\alpha, 1-\alpha)$ существует двудольный граф $G = (L, R, E)$ ($|L| = |R| = n$), на котором метод трудного множества дает оценку хотя бы n^β , а оценка Куликова-Юкны не превосходит $n^\alpha + o(n^{\frac{\alpha}{2}})$.

Доказательство. Пусть $\delta = \frac{1-\alpha}{2}$, тогда все неравенства, в которых участвует δ , выполняются:

- $\delta + \alpha = \frac{1-\alpha}{2} + \alpha = \frac{1+\alpha}{2} < 1$
- $2\delta = 1-\alpha > \beta > \alpha$
- $\delta = \frac{1-\alpha}{2} = \frac{1+\alpha}{2} - \alpha > (1-\alpha) - \alpha > \beta - \alpha$

а значит существует граф, у которого метод трудного множества дает оценку n^β , а оценка по методу Куликова-Юкны не превосходит $n^\alpha + O(n^{2\alpha+\delta-1}) = n^\alpha + O(n^{2\alpha+\frac{1-\alpha}{2}-1}) = n^\alpha + o(n^{\frac{\alpha}{2}})$. ■

К сожалению, мы смогли показать лишь существование такого графа, но не смогли доказать, что это верно для почти всех графов. Чтобы преодолеть эту трудность, нужно исследовать отклонение числа трудных множеств размера k .

5.5 Количество трудных множеств размера k

Вспомним, что $f_k(G)$ – число трудных множеств размера k в графе G . Давайте оценим матожидание этой случайной величины

$$\mathbb{E}[f_k(G)] = \binom{n}{k}^2 \cdot k! \cdot \mathbb{E}[I_k(G)] = \binom{n}{k}^2 \cdot k! \cdot p^k (1 - p^2)^{\binom{k}{2}}$$

Лемма 5.2. Если $k = o(\sqrt{n})$, то $\binom{n}{k} \sim \frac{n^k}{k!}$, к тому же, если $k \rightarrow \infty$ при $n \rightarrow \infty$, то $\binom{n}{k} \sim n^k k^{-k-\frac{1}{2}} e^k$.

Доказательство. Применим неравенство $\ln(1 - x) < -x$

$$\begin{aligned} \binom{n}{k} &= \frac{n^k}{k!} \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{k-1}{n}\right) = \\ &= \frac{n^k}{k!} e^{\ln(1-\frac{1}{n}) + \ln(1-\frac{2}{n}) + \cdots + \ln(1-\frac{k-1}{n})} < \frac{n^k}{k!} e^{-\frac{1}{n} - \frac{2}{n} - \cdots - \frac{k-1}{n}} = \\ &= \frac{n^k}{k!} e^{-\frac{k(k-1)}{2n}} = \frac{n^k}{k!} e^{-O(\frac{k^2}{n})} \end{aligned}$$

Если использовать неравенство $\ln(1 - x) > -x - \frac{1}{2}x^2$, то получаем

$$\begin{aligned} \binom{n}{k} &> \frac{n^k}{k!} e^{-\frac{1}{n} - \frac{1}{2} \cdot \frac{1^2}{n^2} - \frac{2}{n} - \frac{1}{2} \cdot \frac{2^2}{n^2} - \cdots - \frac{1}{n} - \frac{k-1}{2} \cdot \frac{(k-1)^2}{n^2}} = \\ &= \frac{n^k}{k!} e^{-\frac{k(k-1)}{2n} - \frac{1}{2n} \sum_{i < k} i^2} > \frac{n^k}{k!} e^{-\frac{k^2}{2n} - O(\frac{k^3}{n^2})} \end{aligned}$$

В итоге мы получили, что

$$\frac{n^k}{k!} e^{-\frac{k^2}{2n} - O(\frac{k^3}{n^2})} < \binom{n}{k} < \frac{n^k}{k!} e^{-O(\frac{k^2}{n})}$$

При $k = o(\sqrt{n})$ мы получаем $\binom{n}{k} \sim \frac{n^k}{k!}$. Применяя формулу Стирлинга к $k!$, получаем второе утверждение леммы. \square

Эта лемма позволяет найти точный порядок величины $\mathbb{E}[f_k(G)]$ в предположении, что $p = n^\alpha$.

$$\begin{aligned}\mathbb{E}[I_k(G)] &= p^k(1-p^2)^{\binom{k}{2}} = n^{-\alpha k} e^{\binom{k}{2} \cdot \ln(1-\frac{1}{n^{2\alpha}})} = \\ &= n^{-\alpha k} e^{-\binom{k}{2} \cdot \frac{1}{n^{2\alpha}} + \binom{k}{2} \cdot \frac{1}{2n^{4\alpha}} + O\left(\frac{k^2}{n^{6\alpha}}\right)} = n^{-\alpha k} e^{-\frac{k^2}{2n^{2\alpha}} + \frac{k^2}{4n^{4\alpha}} + O\left(\frac{k^2}{n^{6\alpha}}\right)}\end{aligned}$$

Если предположить, что $k = n^{2\alpha+\varepsilon}$, то

$$\begin{aligned}\mathbb{E}[f_k(G)] &\sim n^{2n^{2\alpha+\varepsilon} - (2\alpha+\varepsilon)(n^{2\alpha+\varepsilon} + \frac{1}{2})} \cdot e^{n^{2\alpha+\varepsilon}} \cdot n^{-\alpha n^{2\alpha+\varepsilon}} \cdot e^{-\frac{1}{2}n^{2\alpha+2\varepsilon} + O(n^{2\varepsilon})} = \\ &= n^{n^{2\alpha+\varepsilon}(2-3\alpha-\varepsilon) - \alpha - \frac{\varepsilon}{2}} \cdot e^{-\frac{1}{2}n^{2\alpha+2\varepsilon} + O(n^{2\alpha+\varepsilon})} \xrightarrow{n \rightarrow +\infty} 0\end{aligned}$$

А если $k = n^{2\alpha-\varepsilon}$, то

$$\begin{aligned}\mathbb{E}[f_k(G)] &\sim n^{2n^{2\alpha-\varepsilon} - (2\alpha-\varepsilon)(n^{2\alpha-\varepsilon} + \frac{1}{2})} \cdot e^{n^{2\alpha-\varepsilon}} \cdot n^{-\alpha n^{2\alpha-\varepsilon}} \cdot e^{-\frac{1}{2}n^{2\alpha-2\varepsilon} + O(n^{-\varepsilon})} = \\ &= n^{n^{2\alpha-\varepsilon}(2-3\alpha+\varepsilon) - \alpha + \frac{\varepsilon}{2}} \cdot e^{n^{2\alpha-\varepsilon} + O(n^{2\alpha-2\varepsilon})} \xrightarrow{n \rightarrow +\infty} +\infty\end{aligned}$$

В итоге мы доказали следующую теорему:

Теорема 5.5. Пусть $p = n^{-\alpha}$, тогда

- $k = n^{2\alpha-\varepsilon}$ и $2\alpha - \varepsilon < \frac{1}{2} \implies \mathbb{E}[f_k(G)] \xrightarrow{n \rightarrow +\infty} +\infty$
- $k = n^{2\alpha+\varepsilon}$ и $2\alpha + \varepsilon < \frac{1}{2} \implies \mathbb{E}[f_k(G)] \xrightarrow{n \rightarrow +\infty} 0$

Используя теорему при $k = n^{2\alpha+\varepsilon}$ и неравенство Маркова мы получаем

$$P\{f_k(G) > 0\} = P\{f_k(G) \geq 1\} \leq \mathbb{E}[f_k(G)] \xrightarrow{n \rightarrow +\infty} 0$$

Иначе говоря, размер максимального трудного множества почти наверное меньше $k = n^{2\alpha+\varepsilon}$. Обратно, для того чтобы доказать, что мы почти наверное найдем трудное множество размера $k = n^{2\alpha-\varepsilon}$ рассматривают неравенство Чебышева:

$$P\{f_k(G) = 0\} \leq P\{|f_k(G) - \mathbb{E}[f_k(G)]| \geq \mathbb{E}[f_k(G)]\} \leq \frac{\mathbb{D}[f_k(G)]}{\mathbb{E}[f_k(G)]^2} \xrightarrow{n \rightarrow +\infty} 0$$

Для того, чтобы доказать сходимость к 0 обычно рассматривают ин-

дикаторные случайные величины:

$$I_k(S) = \begin{cases} 1, & \text{если } S \text{ - образует трудное множество;} \\ 0, & \text{если } S \text{ - не образует трудное множество.} \end{cases}$$

где S – фиксированные k -пар вершин. Далее используя $f_k(G) = \sum_S I_k(S)$, получают

$$\mathbb{D}[f_k(G)] = \mathbb{D}\left[\sum_S I_k(S)\right] = \sum_S \mathbb{D}[I_k(S)] + \sum_{S \neq T} \text{cov}(I_k(S), I_k(T))$$

Далее мы будем писать $S \sim T$, если $I_k(S)$ и $I_k(T)$ зависимы, то есть $S \neq T$ и эти два множества имеют хотя бы одной совпадающей вершине из каждой доли.

$$\begin{aligned} \mathbb{D}[f_k(G)] &= \sum_S \mathbb{D}[I_k(S)] + \sum_{S \sim T} \text{cov}(I_k(S), I_k(T)) \leq \\ &\leq \sum_S \mathbb{E}[I_k(S)^2] + \sum_{S \sim T} \mathbb{E}[I_k(S) \cdot I_k(T)] = \\ &= \sum_S \mathbb{E}[I_k(S)] + \sum_{S \sim T} \mathbb{E}[I_k(S) \cdot I_k(T)] = \\ &= \mathbb{E}[f_k(G)] + \sum_{S \sim T} \mathbb{E}[I_k(S) \cdot I_k(T)] \end{aligned}$$

В цепочке равенств мы использовали $I_k(S) = I_k(S)^2$ и в итоге получили

$$\frac{\mathbb{D}[f_k(G)]}{\mathbb{E}[f_k(G)]^2} \leq \frac{1}{\mathbb{E}[f_k(G)]} + \frac{1}{\mathbb{E}[f_k(G)]^2} \cdot \sum_{S \sim T} \mathbb{E}[I_k(S) \cdot I_k(T)]$$

а так как $\mathbb{E}[f_k(G)] \xrightarrow{n \rightarrow +\infty} +\infty$, то достаточно показать

$$\sum_{S \sim T} \mathbb{E}[I_k(S) \cdot I_k(T)] = o(\mathbb{E}[f_k(G)]^2)$$

На самом деле используя тот факт, что все множества S симметричны

друг относительно друга, можно показать

$$\begin{aligned}
\sum_{S \sim T} \mathbb{E}[I_k(S) \cdot I_k(T)] &= \sum_{S \sim T} P\{I_k(S) = 1 \wedge I_k(T) = 1\} = \\
&= \sum_{S \sim T} P\{I_k(S) = 1\} \cdot P\{I_k(T) = 1 \mid I_k(S) = 1\} = \\
&= \sum_S \left(P\{I_k(S) = 1\} \sum_{T: T \sim S} P\{I_k(T) = 1 \mid I_k(S) = 1\} \right) = \\
&= \sum_{T: T \sim S_0} P\{I_k(T) = 1 \mid I_k(S_0) = 1\} \sum_S P\{I_k(S) = 1\} = \\
&= \mathbb{E}[f_k(G)] \sum_{T: T \sim S_0} P\{I_k(T) = 1 \mid I_k(S_0) = 1\}
\end{aligned}$$

А значит мы получили

$$\frac{\mathbb{D}[f_k(G)]}{\mathbb{E}[f_k(G)]^2} \leq \frac{1}{\mathbb{E}[f_k(G)]} + \frac{1}{\mathbb{E}[f_k(G)]} \cdot \sum_{T: T \sim S_0} P\{I_k(T) = 1 \mid I_k(S_0) = 1\}$$

а так как $\mathbb{E}[f_k(G)] \xrightarrow{n \rightarrow +\infty} +\infty$, то достаточно показать

$$\sum_{T: T \sim S_0} P\{I_k(T) = 1 \mid I_k(S_0) = 1\} = o(\mathbb{E}[f_k(G)]) \quad (***)$$

К сожалению, для $f_{ool}(G)$ данное утверждение не столь тривиально, как, например, для кликового числа $w(G)$. И если бы мы смогли показать это, то было бы верно

Утверждение 5.2. Пусть $\alpha \leq \frac{1}{4}$ и $\varepsilon > 0$, тогда почти на верное метод трудного множества дает оценку хотя бы $n^{2\alpha-\varepsilon}$, а оценка Куликова-Юкны в точности равна n^α .

Доказательство. Так как $\alpha \leq \frac{1}{4}$, то $k = n^{2\alpha-\varepsilon} = o(\sqrt{n})$. Следовательно из теоремы 5.5 и выполнимости условия $(***)$ мы получаем

$$P\{f_k(G) > 0\} = 1 - P\{f_k(G) = 0\} \xrightarrow{n \rightarrow +\infty} 1$$

Оценка Куликова-Южны следует из утверждения 5.1 при $\delta = \frac{1}{2}$:

$$n^\alpha - o(1) \leq \frac{v(G)^2}{|E|} \leq n^\alpha + o(1) \quad \square$$

Обобщение методов оценивания

Существует несколько классических обобщений коммуникационной задачи с двумя игроками. Одним из самых популярных обобщений является модель "number-in-hand": имеется m игроков, которые хотят вычислить некоторую функцию $f(x_1, x_2, \dots, x_m)$, причем i -ый игрок знает только аргумент x_i . В данной модели общение будет происходить по принципу широковещания: каждое пересылаемое сообщение видно всем игрокам.

В этом разделе мы формализуем модель "number-in-hand", определим коммуникационную сложность, а также обобщим метод трудного множества и метод энтропийных неравенств.

6.1 m -Мерная коммуникационная сложность

Опишем модель более формально. Пусть имеются конечные множества X_1, X_2, \dots, X_m, Z и задана некоторая функция от m переменных $f : X_1 \times X_2 \times \dots \times X_m \rightarrow Z$.

Определение. m -Мерным коммуникационным протоколом для вычисления некоторой функции $f : X_1 \times X_2 \times \dots \times X_m \rightarrow Z$ называется ориентированное двоичное дерево со следующей разметкой на вершинах и ребрах:

- каждая нелистовая вершина помечена индексом игрока i ;
- в j -ой вершине (в произвольной нумерации) с меткой i записана функция $g_{i,j} : X_i \rightarrow \{0, 1\}$
- каждой листовой вершине сопоставлен элемент множества Z ;
- каждое ребро помечено 0 или 1.

Все игроки договариваются, что будут действовать по некоторому протоколу \mathcal{P} , после чего они получают по аргументу $x_i \in X_i$. Поместим

фишку в корневую вершину нашего протокола \mathcal{P} и будем перемещать ее вниз по дереву, последовательно удаляясь от корня, пока она не попадет в один из листьев. Перемещение фишки выполняется следующим образом. Если текущая вершина помечена индексом i , то это означает, что сейчас очередь i -ого игрока. Он применяет функцию $g_{i,j}$ текущей вершины к своему значению x_i , отправляет по каналу связи бит равный $g_{i,j}(x_i)$ и перемещает фишку по ребру, помеченному как $g_{i,j}(x_i)$. Все остальные игроки видят отправленный бит и понимают куда была сдвинута фишка по дереву протокола. Данная процедура заканчивается в тот момент, когда фишка попадает в лист дерева, а записанное там значение $z \in Z$, объявляется результатом выполнения протокола.

Мы говорим, что протокол \mathcal{P} вычисляет $f : X_1 \times X_2 \times \dots \times X_m \rightarrow Z$, если для любого набора $(x_1, x_2, \dots, x_m) \in X_1 \times X_2 \times \dots \times X_m$ при движении из корня по пути, соответствующему заданным x_1, x_2, \dots, x_m , мы попадаем в лист, помеченный $z = f(x_1, x_2, \dots, x_m)$.

Определение. Сложностью t -мерного коммуникационного протокола называется его глубина. Коммуникационной сложностью функции f называется минимальная сложность протокола, вычисляющего f . Как и для случая с двумя игроками мы будем обозначать её $CC(f)$.

6.2 Одноцветные комбинаторные параллелепипеды

Определение. Множество $S \subseteq X_1 \times X_2 \times \dots \times X_m$ называется комбинаторным параллелепипедом (или просто параллелепипедальным множеством), если существуют такие $Y_1 \subseteq X_1, Y_2 \subseteq X_2, \dots, Y_m \subseteq X_m$, что $S = Y_1 \times Y_2 \times \dots \times Y_m$.

Пусть \mathcal{P} – некоторый коммуникационный протокол для вычисления функции $f : X_1 \times X_2 \times \dots \times X_m \rightarrow Z$ и l – один из листьев протокола. Определим S_l как множество $(x_1, x_2, \dots, x_m) \in X_1 \times X_2 \times \dots \times X_m$ таких, что на входе (x_1, x_2, \dots, x_m) игроки, следуя протоколу \mathcal{P} , приходят в l .

Утверждение 6.1. Для всякого t -мерного коммуникационного протокола \mathcal{P} и для всякого листа l множество S_l является комбинаторным параллелепипедом.

Доказательство. Докажем, что это верно не только для листьев, но и для произвольной вершины протокола. Будем доказывать при помощи математической индукции по глубине вершины v . Для корня это очевидно $S_{root} = X_1 \times X_2 \times \dots \times X_m$. Пусть у нас в дереве протокола имеется переход $w \rightarrow v$ по биту b и вершина w помечена индексом i . Тогда верно

$$S_v = S_w \cap \{(x_1, \dots, x_i, \dots, x_m) \mid f_{i,w}(x_i) = b\}$$

По предположению индукции $S_w = Y_{1,w} \times Y_{2,w} \times \dots \times Y_{m,w}$, а значит верно

$$S_v = Y_{1,w} \times \dots \times (Y_{i,w} \cap \{x_i \mid f_{i,w}(x_i) = b\}) \times \dots \times Y_{m,w}$$

Переход доказан. \square

6.3 Метод трудного множества

Данный метод тесно связан с одноцветными параллелепипедальными множествами.

Определение. Для функции $f : X_1 \times X_2 \times \dots \times X_m \rightarrow Z$ и элемента $z \in Z$ будем называть множество $S_z \subset X_1 \times X_2 \times \dots \times X_m$ трудным (в англоязычной литературе *fooling set*), если верно:

- для всякого $(x_1, x_2, \dots, x_m) \in S_z$ имеем $f(x_1, x_2, \dots, x_m) = z$;
- для любых двух несовпадающих векторов $(x_1, x_2, \dots, x_m) \in S_z$ и $(x'_1, x'_2, \dots, x'_m) \in S_z$ существует вектор (y_1, y_2, \dots, y_m) такой, что $f(y_1, y_2, \dots, y_m) \neq z$ и для любого i верно $y_i \in \{x_i, x'_i\}$.

По аналогии с коммуникационным протоколом для двух игроков можно определить гиперграф $G_z = (X_1 \sqcup \dots \sqcup X_m, E_z)$, ребрами которого являются вектора $(x_1, x_2, \dots, x_m) \in X_1 \times X_2 \times \dots \times X_m$ такие, что $f(x_1, x_2, \dots, x_m) = z$. Из определения комбинаторного параллелепипеда видно, что в гиперграфовой интерпретации он является полным m -дольным гиперграфом. Понятия $bcr(G)$ и $bcc(G)$ определяются естественным образом, а трудное множество есть не что иное, как множество ребер

гиперграфа такое, что любые два ребра не могут лежать в одном полном m -дольном гиперграфе.

Теорема 6.1. *Для произвольного неориентированного m -дольного гиперграфа $G = (X_1 \sqcup X_2 \sqcup \dots \sqcup X_m, E)$, если подмножество ребер $S \subseteq E$ является трудным, то $bcc(G) \geq |S|$.*

6.4 Метод энтропийных неравенств

Далее везде мы будем случайные величины обозначать заглавными буквами, а их значение строчными. Для упрощения формул мы будем использовать следующие обозначения маргинальных распределений (как обычных, так и условных):

$$p(a, b) = P\{A = a, B = b\}, \quad p(a|b) = P\{A = a|B = b\}$$

Для начала докажем следующую лемму:

Лемма 6.1. *Для произвольных случайных величин X_1, X_2, \dots, X_m и F, G выполняется неравенство:*

$$H(F|X_1, G) + H(F|X_2, G) + \dots + H(F|X_m, G) \leq (m-1)H(F|G) + \Delta$$

где

$$\Delta = \log_2 \left(\sum_{\substack{(f, x_1, \dots, x_m, g) \\ \forall i: p(f, x_i, g) > 0}} \frac{p(x_1, g) \cdot \dots \cdot p(x_m, g)}{p(g)^{m-1}} \right)$$

Доказательство. Рассмотрим распределение

$$p'(f, x_1, \dots, x_m, g) = \begin{cases} \frac{p(f, x_1, g) \cdot \dots \cdot p(f, x_m, g)}{p(f, g)^{m-1}} & \text{если } p(f, g) > 0, \\ 0 & \text{иначе.} \end{cases}$$

Если $p(f, g) = 0$, то $p(f, x_i, g) = p'(f, x_i, g) = 0$. А если $p(f, g) \neq 0$, то

$$p'(f, x_i, g) = \sum_{(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m)} \frac{p(f, x_1, g) \cdot \dots \cdot p(f, x_m, g)}{p(f, g)^{m-1}} =$$

$$\begin{aligned}
&= \left(\sum_{x_1} \frac{p(f, x_1, g)}{p(f, g)} \right) \cdot \dots \cdot \left(\sum_{x_{i-1}} \frac{p(f, x_{i-1}, g)}{p(f, g)} \right) \cdot p(f, x_i, g) \cdot \\
&\cdot \left(\sum_{x_{i+1}} \frac{p(f, x_{i+1}, g)}{p(f, g)} \right) \cdot \dots \cdot \left(\sum_{x_m} \frac{p(f, x_m, g)}{p(f, g)} \right) = p(f, x_i, g)
\end{aligned}$$

В итоге мы получили, что для любого натурального $i \in \{1, \dots, m\}$ выполняется $p'(f, x_i, g) = p(f, x_i, g)$, а значит и $p'(f, g) = p(f, g)$. Но тогда сумма

$$\begin{aligned}
&H(F|X_1, G) + H(F|X_1, G) + \dots + H(F|X_m, G) - (m-1)H(F|G) = \\
&= \sum_{(f, x_1, \dots, x_m, g)} p(f, x_1, \dots, x_m, g) \cdot \log_2 \left(\frac{p(f|g)^{m-1}}{p(f|x_1, g) \cdot \dots \cdot p(f|x_m, g)} \right) = \\
&= (m-1) \cdot \sum_{(f, g)} p(f, g) \log_2 \frac{p(f, g)}{p(g)} + \sum_{i=1}^m \sum_{(f, x_i, g)} p(f, x_i, g) \log_2 \frac{p(f, x_i, g)}{p(f, g)} = \\
&= (m-1) \cdot \sum_{(f, g)} p'(f, g) \log_2 \frac{p(f, g)}{p(g)} + \sum_{i=1}^m \sum_{(f, x_i, g)} p'(f, x_i, g) \log_2 \frac{p(f, x_i, g)}{p(f, g)} = \\
&= \sum_{(f, x_1, \dots, x_m, g)} p'(f, x_1, \dots, x_m, g) \cdot \log_2 \left(\frac{p(f|g)^{m-1}}{p(f|x_1, g) \cdot \dots \cdot p(f|x_m, g)} \right) \leq
\end{aligned}$$

Далее мы применяем неравенство Йенсена:

$$\alpha_1 \log_2 \beta_1 + \dots + \alpha_k \log_2 \beta_k \leq \log_2(\alpha_1 \beta_1 + \dots + \alpha_k \beta_k)$$

и получаем

$$\begin{aligned}
&\leq \log_2 \left(\sum_{\substack{(f, x_1, \dots, x_m, g) \\ p'(f, x_1, \dots, x_m, g) > 0}} \frac{p(x_1, g) \cdot \dots \cdot p(x_m, g)}{p(g)^{m-1}} \right) = \\
&= \log_2 \left(\sum_{\substack{(f, x_1, \dots, x_m, g) \\ \forall i: p(f, x_i, g) > 0}} \frac{p(x_1, g) \cdot \dots \cdot p(x_m, g)}{p(g)^{m-1}} \right)
\end{aligned}$$

Лемма доказана. \square

Определение. Будем говорить, что случайные величины X_1, \dots, X_m и F удовлетворяют условию регулярности (R) , если для любого набора (f, f', x_1, \dots, x_m) верно:

$$\begin{cases} p(f, x_1) > 0, \dots, p(f, x_m) > 0 \\ p(f', x_1) > 0, \dots, p(f', x_m) > 0 \end{cases} \implies f = f'$$

Утверждение 6.2. Если F – детерминированная функция от X_1, \dots, X_m (н.н.) и X_1, X_2, \dots, X_m независимы в совокупности относительно F , тогда выполняется условию регулярности (R) .

Доказательство. Пусть условие регулярности (R) не выполняется, значит существуют f, f', x_1, \dots, x_m такие, что

$$\begin{cases} p(f, x_1) > 0, \dots, p(f, x_m) > 0 \\ p(f', x_1) > 0, \dots, p(f', x_m) > 0 \end{cases} \text{ и } f \neq f'$$

Так как $p(f, x_1) > 0$ и $p(f', x_1) > 0$, то $p(f) > 0$ и $p(f') > 0$. Но тогда используя независимость случайных величин, мы получаем

$$\begin{aligned} p(x_1, \dots, x_m | f) &= p(x_1 | f) \cdot \dots \cdot p(x_m | f) \implies \\ \implies p(f)^{m-1} \cdot p(f, x_1, \dots, x_m) &= p(f, x_1) \cdot \dots \cdot p(f, x_m) > 0 \end{aligned}$$

То есть получаем, что $p(f, x_1, \dots, x_m) > 0$. Аналогично доказываем, что $p(f', x_1, \dots, x_m) > 0$. В итоге приходим к противоречию с тем, что F – детерминированная функция от X_1, \dots, X_m (н.н.). \square

Посмотрим какие значения может принимать Δ , если выполняется условие регулярности (R) . В Δ суммирование ведется по таким наборам (f, x_1, \dots, x_m, g) , что $\forall i : p(f, x_i, g) > 0$, а значит и $\forall i : p(f, x_i) > 0$. В данном случае условие регулярности говорит нам о том, что не существует двух различных наборов (f, x_1, \dots, x_m, g) и (f', x_1, \dots, x_m, g) ,

дающих ненулевой вклад в суммирование, а значит

$$\begin{aligned}
\Delta &= \log_2 \left(\sum_{\substack{(f, x_1, \dots, x_m, g) \\ \forall i: p(f, x_i, g) > 0}} \frac{p(x_1, g) \cdot \dots \cdot p(x_m, g)}{p(g)^{m-1}} \right) = \\
&= \log_2 \left(\sum_{\substack{(x_1, \dots, x_m, g) \\ \forall i: p(x_i, g) > 0}} \frac{p(x_1, g) \cdot \dots \cdot p(x_m, g)}{p(g)^{m-1}} \right) = \\
&= \log_2 \left(\sum_{g: p(g) > 0} p(g) \cdot \left(\sum_{x_1: p(x_1, g) > 0} \frac{p(x_1, g)}{p(g)} \right) \cdot \dots \cdot \left(\sum_{x_m: p(x_m, g) > 0} \frac{p(x_m, g)}{p(g)} \right) \right) = \\
&= \log_2 \left(\sum_{g: p(g) > 0} p(g) \right) = \log_2 1 = 0
\end{aligned}$$

А значит мы доказали следующую теорему:

Теорема 6.2. *Если случайные величины X_1, X_2, \dots, X_m и F удовлетворяют условию регулярности (R) , тогда*

$$H(F|X_1, G) + H(F|X_2, G) + \dots + H(F|X_m, G) \leq (m - 1) \cdot H(F|G)$$

Список литературы

- [1] Kushilevitz Eyal, Nisan Noam. Communication Complexity. Cambridge University press, 2006.
- [2] Razborov Alexander. Communication Complexity. In: An Invitation to Mathematics: from Competitions to Research. Springer, 2011.
- [3] Gruber H., Holzer M. Finding lower bounds for nondeterministic state complexity is hard. Springer, 2006.
- [4] D. Caen D. A. Gregory, Pullman N. J. The Boolean rank of zero-one matrices. Department of Mathematics, University of the West Indies, 1981.

- [5] Jukna S., Kulikov A. S. On covering graphs by complete bipartite subgraphs. Discrete Math, 2009.
- [6] Kaced Tarik, Romashchenko A. E., Vereshchagin N. K. Conditional Information Inequalities and Combinatorial Applications. CoRR, 2015.
- [7] Оре Ойстин. Теория графов. Наука, 1968.