Листок 4*

Кое-что об экстремальной комбинаторике

Дополнительная часть

1. Поле $\mathbb{F}_2$. Линейная алгебра имеет широчайшее применение в дискретной математике, комбинаторике и теории кодирования. При этом часто удобно использовать векторные пространства над самым маленьким полем – полем $\mathbb{F}_2$, состоящим из двух элементов 0 и 1. Операции сложения и умножения в этом поле устроены следующим образом:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

Другими словами, операции выполняются «по модулю 2» (например, $1+1 \equiv 0 \mod 2$). Убедитесь, что эти операции ассоциативны, коммутативны и дистрибутивны, и что для любого $a \in \mathbb{F}_2$ существует элемент $-a$ (такой что $a+(-a)=0$) и a^{-1} (такой что $a \times a^{-1} = 1$).

Так же, как в случае поля $\mathbb{R}$ и пространства $\mathbb{R}^n$, можно рассмотреть арифметическое векторное пространство строк $\mathbb{F}_2^n$. Его элементы — строки длины n, каждый элемент строки равен 0 или 1. Сложение векторов и умножение их на элементы поля происходит по описанным выше правилам.

2. Странный город. Рассмотрим забавный пример[1] применения линейной алгебры над $\mathbb{F}_2$.

В Странном городе живут n человек. Они постоянно образовывают клубы по интересам. Однажды клубов стало так много, что правительство решило установить следующие правила:

- В каждом клубе должно быть *нечетное* количество членов.
- Каждые два клуба должны иметь *четное* число общих членов.

Теорема 1 (Oddtown Theorem)**.** *Следуя этим правилам, невозможно организовать клубов больше, чем число жителей n.*

Доказательство теоремы. Для простоты будем называть жителей $1, 2, \ldots, n$, а клубы — $K_1, K_2, \ldots, K_m$. Определим $m \times n$ матрицу $A = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{F}_2)$ правилом

$$a_{ij} = \begin{cases} 1, & \text{если } j \in K_i, \\ 0, & \text{иначе.} \end{cases}$$

[1] В англоязычном оригинале эта миниатюра называется Oddtown (это игра слов: odd в английском имеет значения «странный» и «нечетный».)

Ясно, что $\operatorname{rk} A \leqslant n$. Рассмотрим теперь матрицу $B = AA^T$, где A^T обозначает транспонированную матрицу A. Матрица $B = (b_{ij})$ имеет размер $m \times m$, причем

$$b_{ij} = \sum_{s=1}^{n} a_{is}a_{js}.$$

Но это значит, что b_{ij} равно числу жителей в $K_i \cap K_j$. Более того, поскольку мы работаем над $\mathbb{F}_2$, это число равно 1, если $|K_i \cap K_j|$ нечетно, и 0, если $|K_i \cap K_j|$ четно (здесь через $|M|$ обозначено число элементов множества M).

Следовательно, правила правительства означают, что $B = E$ — единичная матрица размера $m \times m$, а потому $\operatorname{rk} B = \operatorname{rk} AA^T = m$. Поскольку ранг произведения матриц не превосходит минимума рангов сомножителей, получаем $\operatorname{rk} A \geqslant m$. Значит, $m \leqslant n$.

□

Задача 1. Обозначим через $J_m \in \mathrm{Mat}_{m,m}(\mathbb{F}_2)$ матрицу, все элементы которой равны 1, а через $I_m \in \mathrm{Mat}_{m,m}(\mathbb{F}_2)$ — единичную матрицу. Рассмотрим матрицу $J_m - I_m$ (у которой 0 на диагонали и 1 в остальных местах).

(1) Покажите, что $\operatorname{rk}(J_m - I_m) = m$, если m четно.
(2) Покажите, что $\operatorname{rk}(J_m - I_m) = m - 1$, если m нечетно.

Задача 2. Поменяем в правилах правительства слова «четный» и «нечетный» местами. Другими словами, обяжем клубы иметь четное число членов, причем в любых попарных пересечениях должно быть нечетное число членов. Докажите, что число таких клубов все равно не может превосходить числа жителей города.

Задача 3. В условиях предыдущей задачи, найдите максимальное число клубов, которое *действительно* могут образовать жители города (в предыдущей задаче мы оценили это число, но не показали, что оно достигается).

3. Экстремальная комбинаторика. Приведенный пример принадлежит области математики под названием *экстремальная комбинаторика* или, более точно, *экстремальная теория множеств* (extremal set theory). В очень общих чертах, эта область занимается следующими вопросами. Пусть $\mathcal{A}$ — некоторый набор подмножеств в конечном множестве из n элементов, причем множества из $\mathcal{A}$ удовлетворяют некоторому условию (ограничению). Спрашивается, каково максимальное число множеств в $\mathcal{A}$?

Вот несколько известных примеров такого рода вопросов:

- **Oddtown Theorem** Если каждое $A \in \mathcal{A}$ содержит нечетное число элементов, а $|A \cap B|$ четно для любых различных $A, B \in \mathcal{A}$, то $|\mathcal{A}| \leqslant n$.
- **Лемма Шпернера**. Если не существует различных множеств $A, B \in \mathcal{A}$ с $A \subset B$, то

$$|\mathcal{A}| \leqslant \binom{n}{\lfloor n/2 \rfloor}.$$

- **Теорема Эрдёша-Ко-Радо** Если $k \leqslant n/2$, каждое $A \in \mathcal{A}$ содержит ровно k элементов, и $A \cap B = \varnothing$ для любых двух $A, B \in \mathcal{A}$, то

$$|\mathcal{A}| \leqslant \binom{n-1}{k-1}.$$

Многие подобные результаты, хоть и выглядят слегка неестественно, с успехом применяются в решении классических проблем. Вот один из самых знаменитых примеров такой проблемы из области *комбинаторной геометрии*.

Гипотеза Бóрсука (Borsuk's conjecture). *Верно ли, что любое тело диаметра d в $\mathbb{R}^n$ можно разбить на $n+1$ часть так, что диаметр каждой части будет меньше d?*

Здесь под *диаметром* тела понимается наибольшее из расстояний между двумя его точками. Этот вопрос был поставлен польским математиком Каролем Бóрсуком в 1933 г. и долгое время оставался открытым (хотя и был положительно решен во многих частных случаях). И только в 1993 г. Калай и Кан построили контрпример в размерности $n = 1325$. В 1997 г. А. М. Райгородский (работает на мехмате) получил контрпример в размерности $n = 561$, а в 2013 г. было доказано, что гипотеза Борсука неверна для всех $n \geqslant 64$.

Что про это читать? Есть много отличных брошюр А. М. Райгородского для начинающих, например

А. М. Райгородский, *Линейно-алгебраический метод в комбинаторике*, МЦНМО, 2007.

А. М. Райгородский, *Вероятность и алгебра в комбинаторике*, МЦНМО, 2008.

А. М. Райгородский, *Проблема Борсука*, МЦНМО, 2006.