Алгебраические структуры и их приложения к задачам дискретной математики

Александр Дайняк

Актуальная версия файла доступна на www.dainiak.com

Оглавление

Введение

В этом пособии мы вводим понятия частично-упорядоченных множеств, конечных групп и полей и показываем, какую службу они могут сослужить в решении комбинаторных задач. Эти важнейшие понятия алгебры излагаются предельно сжато, поскольку цель настоящего пособия — дать основные определения и как можно скорее перейти к приложениям в комбинаторике. Читателю, не привыкшему «скакать по верхам» рекомендуется более плотно ознакомиться с алгеброй по одной из следующих книг.

1. Г. Биркгоф, Т. Барти. Современная прикладная алгебра. М., Мир, 1976.
2. Э.Б. Винберг. Курс алгебры. М.: Факториал, 2001.
3. Ю.И. Журавлев, Ю.А. Флеров, М.Н. Вялый. Дискретный анализ. Основы высшей алгебры. М.: МЗ Пресс, 2007.
4. А.Г. Курош. Курс высшей алгебры. М.: Наука, 1965.

Книги [1] и [4], хотя и давно изданы, хорошо себя зарекомендовали. Книга [4] предназначена, в первую очередь, для студентов-теоретиков, в то время, как в [1] обсуждаются приложения алгебры в теории проектирования вычислительных устройств и теории кодирования. Самой доступной из перечисленных книг является, на наш взгляд, учебник [3], хотя охват его не так широк, как у остальных книг. Книга [2] является хорошим примером современного вводного учебника высшей алгебры.

Также нужно отметить две книги по комбинаторике (которые нельзя назвать вводными), поскольку в них на более высоком уровне излагаются данные в пособии теория обращения Мёбиуса и теория Редфилда—Пойи соответственно.

- М. Айгнер. Комбинаторная теория. М.: Мир, 1982.
- Комбинаторная прикладная математика / Под ред. Э.Беккенбаха. М.: Мир, 1968.

Пререквизиты

Предполагается, что читателю известны базовые обозначения теории множеств и понятия отображения и отношения. В отдельных разделах также предполагается знакомство с начальными понятиями линейной алгебры, асимптотикой, элементарными понятиями комбинаторики (факториал, биномиальные коэффициенты, графы).

Мы принимаем следующие обозначения и сокращения.

- «Т. и т.т.» — тогда и только тогда.
- «Б.о.о.» — без ограничения общности.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ — множества натуральных (без нуля), целых, рациональных и действительных чисел соответственно.
- $\mathbb{N}_0$ — множество целых неотрицательных чисел.
- $\mathbb{1}_{\text{условие}}$ — индикатор (величина, равная единице/нулю соответственно при выполнении/невыполнении условия)
- $x|y$ — число x является делителем числа y.
- $\{x \in S \mid \text{свойство}\}$ — множество всех объектов, принадлежащих множеству S и обладающих заданным свойством.
- # — сокращение для слова «количество». Например, запись $\#\{x \in \mathbb{N} \mid 1 \le x^2 \le 10\}$ означает «количество натуральных чисел, квадраты которых лежат в отрезке от 1 до 10».
- $A \subseteq B$ — множество A вложено в B и, возможно, совпадает с B.
- $A \subset B$ — множество A вложено в B и не совпадает с B.

1. Частично упорядоченные множества

1.1. Определения

Частично упорядоченное множество (ч. у. м.) — это пара $(S, \preccurlyeq)$, где S — произвольное множество (*носитель*), а $\preccurlyeq$ — отношение частичного порядка. Отношение $\preccurlyeq$ должно обладать следующими свойствами:

- антисимметричность: $\forall a, b \in S \quad (a \preccurlyeq b \wedge b \preccurlyeq a \quad \Rightarrow \quad a = b)$,
- рефлексивность: $\forall a \in S \quad a \preccurlyeq a$,
- транзитивность: $\forall a, b, c \in S \quad (a \preccurlyeq b \wedge b \preccurlyeq c \quad \Rightarrow \quad a \preccurlyeq c)$.

Стандартными примерами ч. у. м. являются множества $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ относительно обычного сравнения чисел. На первый взгляд необычным, но очень полезным ч. у. м., является множество $\mathbb{N}$ относительно делимости: в этом ч. у. м. каждое натуральное число предшествует всем, делителями которых оно является. Частично упорядоченными является множество слов в конечном алфавите относительно лексикографического сравнения. Ниже мы рассмотрим ещё одно очень важное ч. у. м., *булеан*.

Цепь в ч. у. м. — это последовательность элементов $a_1, \ldots$, где $a_i \preccurlyeq a_{i+1}$ для каждого i. *Антицепь* в ч. у. м. — это подмножество попарно несравнимых элементов.

Иными словами, цепь — это последовательность попарно сравнимых элементов, а антицепь — множество попарно несравнимых элементов. Каждая цепь и антицепь имеют не больше одного общего элемента.

Элемент a *непосредственно предшествует* элементу b, если $a \preccurlyeq b$ и не существует c, такого, что $a \prec c \prec b$.

Элемент *максимальный*, если в ч. у. м. нет элементов, больших него. Элемент *наибольший*, если он максимальный и сравнимый с любым элементом ч. у. м.

Булеан конечного множества X — это семейство всех подмножеств X, упорядоченных по вложенности.

Булев куб — множество двоичных наборов фиксированной длины, упорядоченных по покоординатному сравнению: $(\alpha_1, \ldots, \alpha_n) \preccurlyeq (\beta_1, \ldots, \beta_n) \quad \Leftrightarrow \quad \forall i \quad \alpha_i \leq \beta_i$.

Булеан и булев куб *изоморфны*, как частично упорядоченные множества. Изоморфными называют ч. у. м., между элементами которых можно установить взаимно-однозначное соответствие, сохраняющее порядок (т.е. если взять пару сравнимых элементов в одном ч. у. м., то их образы будут сравнимы и в другом ч. у. м.).

1.2. Теоремы о разложении ч. у. м. на цепи и антицепи

Разложить ч. у. м. на цепи — это значит представить носитель ч. у. м. объединением попарно непересекающихся цепей. Аналогично определяется разложение на антицепи.

Очевидно, если в некотором ч. у. м. есть антицепь порядка l, то меньше чем на l цепей ч. у. м. разложить нельзя, поскольку каждая из этих цепей будет пересекаться с антицепью не более чем по одной вершине. Аналогично, если в ч. у. м. есть цепь размера l, то его не получится разложить менее чем на l цепей. Следующие две теоремы показывают, что, на самом деле, указанные нижние оценки на число цепей и антицепей в разложении всегда являются точными. Отметим, что, хотя утверждения теорем выглядят очень похоже, доказательство второй из теорем ощутимо труднее.

Теорема. Минимальное число антицепей, на которое можно разложить ч. у. м., равно максимальному размеру цепи в этом ч. у. м..

Доказательство. Пусть l — максимальный размер цепи в ч. у. м.. Назовём высотой элемента a максимальный размер цепей вида $x_1 \prec x_2 \prec \cdots \prec a$. Для каждого $i \in \{1, \dots, l\}$ обозначим через S_i множество всех элементов высоты i. Очевидно, $S_i \cap S_j = \emptyset$ для каждого i. Осталось заметить, что S_i — антицепь для каждого i, а значит, $S_1 \sqcup \dots \sqcup S_l$ — искомое разложение ч. у. м. на антицепи.

Теорема Дилуорта. Минимальное число цепей, на которое можно разложить ч. у. м., равно максимальному размеру антицепи в этом ч. у. м..

Доказательство. Докажем эту часть теоремы индукцией по мощности частично упорядоченного множества S. Утверждение легко проверяется перебором при $|S| \leq 2$. Пусть $|S| > 2$, и для меньших ч. у. м. теорема верна; докажем её для S. Пусть a — произвольный максимальный элемент в S, и пусть l — максимальный размер антицепи в $S \setminus \{a\}$. По предположению, $S \setminus \{a\}$ можно разбить на l цепей:

$$S \setminus \{a\} = C_1 \sqcup \dots \sqcup C_l.$$

Назовём элемент *хорошим*, если существует l-элементная антицепь в $S \setminus \{a\}$, в которую он входит. Для каждого i обозначим через a_i максимальный из хороших элементов цепи C_i. Заметим, что для каждого i на C_i есть хотя бы один хороший элемент, поскольку любая l-элементная антицепь в $S \setminus \{a\}$ содержит ровно по одному элементу из каждой цепи C_i.

Покажем, что $\{a_1, \dots, a_l\}$ — антицепь в $S \setminus \{a\}$. Предположим противное: пусть $a_i \prec a_j$ для некоторых i, j. Пусть A — произвольная антицепь в $S \setminus \{a\}$, содержащая a_j. Тогда A не содержит ни a_i, ни любой другой элемент на C_i, предшествующий a_i. Но поскольку a_i — максимальный из хороших элементов цепи C_i, мы получаем, что $|A| < l$. Это противоречит тому, что должны существовать l-элементные антицепи, содержащие a_j. Значит, $\{a_1, \dots, a_l\}$ — антицепь.

Если $\{a\} \cup \{a_1, \dots, a_l\}$ — антицепь, то мы легко можем предъявить разложение S на минимально возможное число цепей: $\{a\} \sqcup C_1 \sqcup \dots \sqcup C_l$.

Остаётся рассмотреть случай, когда $\{a\} \cup \{a_1, \dots, a_l\}$ не является антицепью, то есть $a_k \prec a$ для некоторого k. В этом случае рассмотрим множество $K \coloneqq \{x \in C_k \mid x \preccurlyeq a_k\} \cup \{a\}$. Из определения K вытекает, что в $S \setminus K$ нет l-элементных антицепей (так как в K были все хорошие элементы цепи C_k). Тогда, по предположению, $S \setminus K$ разложимо на $(l-1)$ цепей. Добавив к этим цепям K, получим разложение S на l цепей.

1.2.1. Вывод теоремы Холла из теоремы Дилуорта

Труды, потраченные на доказательство теорем о разложении, окупаются, в частности, почти «бесплатным» выводом известной теоремы Холла.

Системой различных представителей (с. р. п.) для набора множеств $X_1, \dots, X_m \subseteq \{1, \dots, n\}$, где $m \leq n$, называется набор элементов $\{y_1, \dots, y_m\} \subseteq \{1, \dots, n\}$, такой, что $y_i \in X_i$ для каждого i, и $y_i \neq y_j$ при $i \neq j$.

Теорема Холла. Для существования с. р. п. для набора множеств $X_1, \dots, X_m$ необходимо и достаточно выполнение условий

$$\forall k \forall i_1 \dots \forall i_k \quad \left|X_{i_1} \cup \dots \cup X_{i_k}\right| \geq k.$$

Доказательство. Необходимость условий очевидна. Докажем достаточность. Построим ч. у. м. на множестве $S \coloneqq \{X_1, \dots, X_m\} \cup \{1, \dots, n\}$, определив порядок так:

$$a \succ b \quad \Leftrightarrow \quad (a \in \{X_1, \dots, X_m\}) \wedge (b \in \{1, \dots, n\}) \wedge (b \in a).$$

Покажем, что в этом ч. у. м. нет антицепей мощности больше m. Пусть антицепь имеет вид $T = T' \cup T''$, где $T' \subseteq \{X_1, \dots, X_m\}$ и $T'' \subseteq \{1, \dots, n\}$. Тогда $(\bigcup_{X \in T'} X) \cap T'' = \emptyset$, и поэтому $|\bigcup_{X \in T'} X| + |T''| \leq n$.

Непосредственно из условий теоремы следует, что $|\bigcup_{X \in T'} X| \geq |T'|$, отсюда

$$|T| = |T'| + |T''| \leq \left|\bigcup_{X \in T'} X\right| + |T''| \leq n.$$

Мы показали, что при выполнении условий теоремы мощность любой антицепи не больше n. По теореме Дилуорта, S можно разложить на n непересекающихся цепей. В каждой из этих цепей либо один, либо два элемента. Те из цепей, в которых по два элемента, имеют вид $\{y_i, X_i\}$, где $y_1, \dots, y_m$ — искомая с. р. п..

1.3. Обращение Мёбиуса на ч. у. м.

1.3.1. Определение функции Мёбиуса

В этом разделе мы будем рассматривать потенциально бесконечные ч. у. м., но будем всегда предполагать, что для любого элемента ч. у. м. есть лишь конечное число элементов, предшествующих ему.

Функция Мёбиуса на ч. у. м. определяется на парах сравнимых элементов:

$$\mu(a,b) = \begin{cases} 1, & \text{если } a = b \\ -\sum\limits_{c:\, a \leqslant c < b} \mu(a,c), & \text{если } a \prec b \end{cases}$$

Лемма. При любых z, x, таких, что $z \leqslant x$, выполнено

$$\sum_{y:\, z \leqslant y \leqslant x} \mu(y,x) = \mathbb{1}_{z=x}$$

Доказательство. Если $z = x$, то $\sum_{y:\, z \leqslant y \leqslant x} \mu(y,x) = \mu(x,x) = \mathbb{1}_{z=x}$. Пусть теперь $z \prec x$. Поведём индукцию по максимальному количеству элементов в цепях вида $z \leqslant \dots \leqslant x$. Обозначим это количество через $\tau(z,x)$. Если $\tau(z,x) = 2$, т. е. z непосредственно предшествует x, то

$$\sum_{y:\, z \leqslant y \leqslant x} \mu(y,x) = \mu(z,x) + \mu(x,x) = \big(-\mu(z,z)\big) + \mu(x,x) = 0 = \mathbb{1}_{z=x}.$$

Далее будем считать, что $\tau(z,x) \geq 3$. Тогда

$$\sum_{y:\, z \leqslant y \leqslant x} \mu(y,x) = \mu(x,x) + \sum_{y:\, z \leqslant y < x} \left(-\sum_{u:\, y \leqslant u < x} \mu(y,u) \right) = 1 - \sum_{y,u:\, z \leqslant y \leqslant u < x} \mu(y,u)$$

$$= 1 - \sum_{u:\, z \leqslant u < x} \sum_{y:\, z \leqslant y \leqslant u} \mu(y,u) = 1 - \mu(z,z) - \sum_{u:\, z < u < x} \underbrace{\sum_{y:\, z \leqslant y \leqslant u} \mu(y,u)}_{= \mathbb{1}_{z=x} = 0 \text{ по предп.инд.}} = 0.$$

Лемма доказана.

Важность функции Мёбиуса определяется следующей теоремой, позволяющей обращать операцию суммирования.

Теорема (формула обращения Мёбиуса). Пусть для каждого x функция f выражается через g по формуле $f(x) = \sum_{y \leqslant x} g(y)$. Тогда справедлива формула

$$g(x) = \sum_{y \leqslant x} f(y) \cdot \mu(y, x).$$

Доказательство. Пользуясь леммой, выводим

$$\sum_{y:\, y \leqslant x} f(y) \cdot \mu(y, x) = \sum_{y:\, y \leqslant x} \left(\sum_{z:\, z \leqslant y} g(z) \right) \mu(y, x) = \sum_{y:\, y \leqslant x} \left(\sum_{z:\, z \leqslant y} g(z) \mu(y, x) \right) = \sum_{y, z:\, z \leqslant y \leqslant x} g(z) \mu(y, x)$$
$$= \sum_{z:\, z \leqslant x} \sum_{y:\, z \leqslant y \leqslant x} g(z) \mu(y, x) = \sum_{z:\, z \leqslant x} g(z) \sum_{y:\, z \leqslant y \leqslant x} \mu(y, x) = \sum_{z:\, z \leqslant x} g(z) \cdot \mathbb{1}_{z=x} = g(x).$$

Теорема доказана.

В следующих двух разделах мы применим теорему об обращении в двух частных случаях: когда в качестве ч. у. м. рассматриваются соответственно булеан и множество натуральных чисел с делимостью в качестве отношения сравнения.

1.3.2. Обращение Мёбиуса на булеане и формула включения-исключения

Вычислим функцию Мёбиуса для булеана множества $\{1, \dots, n\}$ с отношением включения множеств в качестве отношения порядка: $\left(2^{\{1, \dots, n\}}, \subseteq\right)$.

Докажем индукцией по $|Y|$, что для любой пары X, Y, такой, что $X \subseteq Y$, выполнено

$$\mu(X, Y) = (-1)^{|Y| - |X|} = (-1)^{|Y \setminus X|}.$$

База очевидна. Индуктивный переход:

$$\mu(X, Y) = -\sum_{Z:\, X \subseteq Z \subset Y} \mu(X, Z) = -\sum_{Z:\, X \subseteq Z \subset Y} (-1)^{|Z| - |X|} = -\sum_{k=0}^{|Y| - |X| - 1} \binom{|Y| - |X|}{k} (-1)^k = (-1)^{|Y| - |X|}.$$

Покажем, что из теоремы обращения Мёбиуса на булеане можно вывести формулу включения-исключения

$$|A_1 \cup A_2 \cup \dots \cup A_n|$$
$$= |A_1| + \dots + |A_n| - |A_1 \cap A_2| - |A_1 \cap A_3| - \dots - |A_{n-1} \cap A_n| + |A_1 \cap A_2 \cap A_3| + \dots$$
$$+ (-1)^k \cdot \left|A_{i_1} \cap \dots \cap A_{i_k}\right| + \dots + (-1)^{n+1} \cdot |A_1 \cap \dots \cap A_n|.$$

Пусть $A \coloneqq \bigcup_{i=1}^{n} A_i$. Пусть $f(\{i_1, \dots, i_s\})$ обозначает количество объектов из A, которые могут не принадлежать каким-либо из множеств $A_{i_1}, \dots, A_{i_s}$, но должны принадлежать каждому из остальных множеств. По определению, $f(\{1, \dots, n\}) = |A|$ и $f(I) \coloneqq \left|\bigcap_{i \notin I} A_i\right|$ при $I \neq \{1, \dots, n\}$.

Аналогично, пусть $g(\{i_1, \dots, i_s\})$ обозначает количество объектов из A, которые не принадлежат ни одному из множеств $A_{i_1}, \dots, A_{i_s}$ и принадлежат каждому из остальных множеств. Заметим, что $g(\{1, \dots, n\}) = 0$.

Функция f считает количество объектов с заданным набором *возможных* непринадлежностей, а g считает количество объектов, у которых набор непринадлежностей *в точности равен* заданному. Из определений f и g следует, что для каждого множества индексов I выполнено

$$f(I) = \sum_{I' \subseteq I} g(I').$$

Применив обращение Мёбиуса, и учитывая соотношение для f, мы получаем

$$0 = g(\{1,\dots,n\}) = \sum_{I\subseteq\{1,\dots,n\}} f(I)\cdot(-1)^{n-|I|} = \sum_{I\subseteq\{1,\dots,n\}} f(I)\cdot(-1)^{n-|I|}$$
$$= |A| + \sum_{I\subset\{1,\dots,n\}} \left|\bigcap_{i\notin I} A_i\right|\cdot(-1)^{n-|I|}.$$

Отсюда

$$|A| = \sum_{I\subset\{1,\dots,n\}} \left|\bigcap_{i\notin I} A_i\right|\cdot(-1)^{n-|I|+1} = \sum_{\emptyset\neq I\subseteq\{1,\dots,n\}} \left|\bigcap_{i\in I} A_i\right|\cdot(-1)^{|I|+1},$$

что и требовалось.

1.3.3. Арифметическая теорема об обращении и количество циклических слов

«Теоретико-числовая» функция Мёбиуса определяется следующим образом:

$$\hat{\mu}(n) = \begin{cases} 1, & \text{если } n = 1 \\ 0, & \text{если } \exists p \text{ т. что } p^2|n \\ (-1)^s, & \text{если } n = p_1\cdot\ldots\cdot p_s \end{cases}$$

«Теоретико-числовая» теорема об обращении. Если для каждого $n \in \mathbb{N}$ выполнено равенство

$$f(n) = \sum_{k|n} g(k),$$

то для каждого $m \in \mathbb{N}$ имеем

$$g(m) = \sum_{l|m} f(l)\cdot\hat{\mu}(m/l).$$

Доказательство. Рассмотрим ч. у. м. натуральных чисел, с отношением делимости в качестве частичного порядка. Докажем индукцией по x/y соотношение $\mu(y,x) = \hat{\mu}(x/y)$, отсюда, в силу справедливости «общей» теоремы об обращении, будет следовать и «теоретико-числовая» теорема.

База $x/y = 1$ очевидна: $\mu(x,x) = 1 = \hat{\mu}(x/x)$. Пусть далее $y|x$ и $y < x$. Тогда $x = y\cdot p_1^{\alpha_1}\dots p_k^{\alpha_k}$ для некоторых простых p_i и положительных α_i. Выполним индуктивный переход. Имеем

$$\mu(y,x) = -\sum_{z:\ y|z \text{ и } z|x \text{ и } z<x} \mu(y,z) = -\sum_{z:\ y|z \text{ и } z|x \text{ и } z<x} \hat{\mu}(z/y) = -\sum_{\substack{\beta_1\le\alpha_1,\dots,\beta_k\le\alpha_k \\ (\beta_1,\dots,\beta_k)\neq(\alpha_1,\dots,\alpha_k)}} \hat{\mu}\left(p_1^{\beta_1}\dots p_k^{\beta_k}\right)$$
$$= -\sum_{\substack{\beta_1,\dots,\beta_k\in\{0,1\} \\ (\beta_1,\dots,\beta_k)\neq(\alpha_1,\dots,\alpha_k)}} \hat{\mu}\left(p_1^{\beta_1}\dots p_k^{\beta_k}\right).$$

Если $\alpha_1 = \dots = \alpha_k = 1$, то

$$\mu(y,x) = -\sum_{i=0}^{k-1}\binom{k}{i}\cdot(-1)^i = (-1)^k = \hat{\mu}(x/y).$$

Если же $\alpha_j > 1$ для некоторого j, то

$$\mu(y,x) = -\sum_{i=0}^{k}\binom{k}{i}\cdot(-1)^i = 0 = \hat{\mu}(x/y).$$

В обоих случаях индуктивный переход выполнен и теорема доказана.

Применим доказанную теорему для решения задачи о количестве циклических слов. Циклическое слово — это класс эквивалентности «обычных» слов относительно циклического сдвига. Неформально говоря, циклическое слово — это обычное слово, «замкнутое в круг». Разные обычные слова

могут порождать одно и то же циклическое: например, слова «абракадабра» и «акадабраабр». Или, если представить это наоборот, одно циклическое слово порождает несколько обычных.

Наша задача: найти $T_r(n)$ — количество циклических слов длины n в r-буквенном алфавите. Назовём *периодом* циклического слова w такое минимальное число k, что w может быть получено многократным повторением слова k. Очевидно, число k должно делить длину w. Каждое циклическое слово периода k порождает ровно k обычных слов, и каждое обычное слово может быть получено из некоторого циклического «разрывом» в нужной позиции. Отсюда, учитывая, что всего обычных слов ровно r^n, и обозначив через $s(k)$ число циклических слов периода k, получаем

$$r^n = \sum_{k|n} k \cdot s(k).$$

Применив теоретико-числовое обращение Мёбиуса, взяв $f(n) \coloneqq r^n$ и $g(k) \coloneqq k \cdot s(k)$, получим

$$m \cdot s(m) = \sum_{l|m} r^l \cdot \hat{\mu}(m/l).$$

Окончательно находим

$$T_r(n) = \sum_{m|n} s(m) = \sum_{m|n} \frac{1}{m} \sum_{l|m} r^l \cdot \hat{\mu}(m/l).$$

Утверждение. При любом фиксированном r при $n \to \infty$ выполнено

$$T_r(n) \sim \frac{r^n}{n}.$$

Доказательство. Одно и то же циклическое слово длины n порождает не более n обычных слов, поэтому

$$r^n \le n \cdot T_r(n) \quad \Rightarrow \quad T_r(n) \ge \frac{r^n}{n}.$$

Осталось оценить $T_r(n)$ сверху. Имеем

$$T_r(n) = \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \cdot \mu(k/l) \le \sum_{k|n} \frac{1}{k} \sum_{l|k} r^l \le \sum_{k|n} \frac{1}{k} \left(r^k + \sum_{l \le k/2} r^l \right) \le \sum_{k|n} \frac{1}{k} \left(r^k + \frac{k}{2} \cdot r^{k/2} \right)$$
$$\le \frac{1}{n} \left(r^n + \frac{n}{2} \cdot r^{n/2} \right) + n \cdot \left(r^{n/2} + \frac{n}{4} \cdot r^{n/4} \right) \lesssim r^n/n.$$

2. Группы

2.1. Определения

Группа — это множество $\mathbb{G}$ с заданной на нём бинарной операцией $\circ$, которая удовлетворяет следующим свойствам (*аксиомам группы*).

- Ассоциативность. $\forall a, b, c \in \mathbb{G} \quad (a \circ b) \circ c = a \circ (b \circ c)$.
- Существование нейтрального элемента. $\exists e \in \mathbb{G}: \quad \forall a \in \mathbb{G} \quad a \circ e = e \circ a = a$.
- Существование обратных элементов. $\forall a \in \mathbb{G} \quad \exists b \in \mathbb{G}: \quad a \circ b = b \circ a = e$.

Группы, в которых операция $\circ$ коммутативна (то есть $a \circ b = b \circ a$ для любых a, b), называют *абелевыми* или *коммутативными* группами.

Количество элементов в группе называется её *порядком*.

Операция $\circ$ часто обозначается также знаком «$+$» (и тогда говорят об аддитивных обозначениях) или «$\cdot$» (тогда обозначения называют мультипликативными).

Общая запись	В обозначении «+»	В обозначении «·»
$a \circ b$	$a + b$	$a \cdot b$ или просто ab
Нейтральный элемент e	0	1
Обратный элемент к элементу a	$-a$	a^{-1}
$\underbrace{a \circ a \circ \ldots \circ a}_{n \text{ раз}}$	na	a^n

Вместо $a + (-b)$ сокращённо пишут: $a - b$. Вместо $a \cdot b^{-1}$ сокращённо пишут: a/b.

Примеры групп.

- $\mathbb{Z}$ относительно операции $+$,
- множество чётных чисел относительно $+$,
- $\mathbb{Q}$ относительно операции $+$
- $\mathbb{Q} \setminus \{0\}$ относительно операции $\times$,
- $\mathbb{R}^n$ относительно операции покоординатного сложения векторов.
- множество невырожденных матриц из $\mathbb{R}^{n \times n}$ относительно операции умножения матриц.

Примеры множеств, не являющихся группами.

- $\mathbb{Z}$ относительно операции $\times$,
- множество нечётных чисел относительно $+$,
- $\mathbb{R}^{n \times n}$ относительно операции умножения матриц.

Группой является множество всевозможных поворотов плоскости относительно начала координат. В ней операция $a \circ b$ означает, что сначала выполняется поворот a, а затем b (*композиция поворотов*). Нейтральный элемент в этой группе — поворот на 0°. Обратным элементом к повороту на угол α является поворот на угол $(-\alpha)$.

Утверждение. В любой группе нейтральный элемент единственный.

Доказательство. Пусть e' и e'' — нейтральные элементы. Т.к. e'' нейтральный, то $e' \circ e'' = e'$, т.к. e' нейтральный, то $e' \circ e'' = e''$. Отсюда $e' = e''$.

Утверждение. В любой группе для любого элемента a обратный к a элемент единственный.

Доказательство. Пусть b' и b'' — обратные к a элементы. Тогда

$$b' = b' \circ e = b' \circ (a \circ b'') = (b' \circ a) \circ b'' = e \circ b'' = b''.$$

Группы $(\mathbb{G}', \circ)$ и $(\mathbb{G}'', \blacksquare)$ называются *изоморфными*, если существует биекция $\phi: \mathbb{G}' \leftrightarrow \mathbb{G}''$, такая, что

$$\forall a, b \in \mathbb{G}' \quad \phi(a) \blacksquare \phi(b) = \phi(a \circ b).$$

Нетрудно показать, что изоморфизм ϕ всегда отображает нейтральный элемент в нейтральный. Кроме того, если a и b — взаимно обратные элементы в $\mathbb{G}'$, то $\phi(a)$ и $\phi(b)$ будут взаимно обратными в $\mathbb{G}''$. Читателю предлагается доказать это самостоятельно.

Примеры изоморфных групп.

- Группа $(\mathbb{Z}, +)$ изоморфна группе чётных чисел с операцией сложения. Изоморфизм: $x \to 2x$.

- Группа поворотов плоскости на угол, кратный $\frac{\pi}{2}$, с операцией композиции изоморфна группе чисел $\{0,1,2,3\}$ с операцией сложения по модулю 4.

2.2. Эквивалентные определения групп

2.2.1. Определение через существование решений уравнений

Утверждение. Группу можно определить как множество $\mathbb{G}$ с ассоциативной операцией $\circ$, такой, что для любых $a, b \in \mathbb{G}$ существуют решения уравнений $a \circ x = b$ и $x \circ a = b$ относительно x.

Доказательство. Будем работать в мультипликативных обозначениях. Пусть $\mathbb{G}$ — группа, согласно основному определению. Тогда любое уравнение вида $ax = b$ имеет решение:

$$x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b,$$

то есть x существует и определён однозначно. Аналогично рассматривается уравнение $xa = b$.

Обратно, пусть уравнения вида $ax = b$ и $xa = b$ разрешимы во множестве $\mathbb{G}$. Докажем существование нейтрального элемента. Зафиксируем $a \in \mathbb{G}$. Пусть e_{left} — решение уравнения $xa = a$. Пусть $b \in \mathbb{G}$ — произвольный элемент $\mathbb{G}$. Пусть c — решение уравнения $ax = b$. Имеем

$$e_{\text{left}}b = e_{\text{left}}(ac) = (e_{\text{left}}a)c = ac = b.$$

Итак, $e_{\text{left}}b = b$ для любого $b \in \mathbb{G}$. Пусть e_{right} — решение уравнения $ax = a$. Совершенно аналогично доказывается, что $be_{\text{right}} = b$ для любого b. Кроме того, $e_{\text{left}} = e_{\text{left}}e_{\text{right}} = e_{\text{right}}$, то есть $e \coloneqq e_{\text{left}} = e_{\text{right}}$ — «полноценный» нейтральный элемент в $\mathbb{G}$. Существование нейтрального элемента $e \in \mathbb{G}$ доказано.

Осталось доказать существование обратных элементов. Для любого a пусть a_{left}^{-1} и a_{right}^{-1} — решения уравнений $xa = e$ и $ax = e$ соответственно. Достаточно показать, что $a_{\text{left}}^{-1} = a_{\text{right}}^{-1}$. Имеем

$$a_{\text{left}}^{-1} = a_{\text{left}}^{-1}\, e = a_{\text{left}}^{-1}\, a\, a_{\text{right}}^{-1} = e a_{\text{right}}^{-1} = a_{\text{right}}^{-1},$$

что и требовалось.

Утверждение доказано.

2.2.2. Альтернативное определение для конечных групп

Читателю в качестве простого упражнения на применение принципа Дирихле предлагается доказать, что следующее определение эквивалентно второму определению групп в случае конечном случае.

Конечная группа — это множество $\mathbb{G} = \{g_1, \dots, g_n\}$ с бинарной ассоциативной операцией $\circ$, такой, что для каждого $a \in \mathbb{G}$ все элементы

$$a \circ g_1 \quad a \circ g_2 \quad \dots \quad a \circ g_n$$

различны и все элементы

$$g_1 \circ a \quad g_2 \circ a \quad \dots \quad g_n \circ a$$

различны.

2.3. Группы перестановок и теорема Кэли

Подстановка (*перестановка*) — это биекция множества на себя. *Композиция* перестановок — это их последовательное применение. Например, композиция перестановок $(1 \to 3,2 \to 2,3 \to 1,4 \to 4)$ и $(1 \to 4,2 \to 3,3 \to 1,4 \to 2)$ — это подстановка $(1 \to 1,2 \to 3,3 \to 4,4 \to 2)$. Композицию перестановок σ' и σ'', при которой вначале применяется σ', а затем σ'', будем обозначать $\sigma'\sigma''$.

Перестановку σ на множестве $\{v_1, \dots, v_n\}$ можно задать в виде орграфа, в котором дуга ведёт из v_i в v_j, если $\sigma(v_i) = v_j$. В этом орграфе каждая вершина имеет ровно по одной входной и выходной дуге, то есть орграф распадается на непересекающиеся простые циклы. Они называются *циклами перестановки* σ. Например, у перестановки $(1 \to 1,2 \to 3,3 \to 4,4 \to 2)$ один цикл длины 1 и один

цикл длины 3. Часто перестановки записывают, перечисляя их циклы, и внутри каждого цикла перечисляя вершины в порядке их следования по циклу. Например, рассмотренная выше перестановка будет записана как $(1)(234)$.

Нетрудно проверить, что совокупность всех подстановок на множестве $\{1,2,\dots,n\}$ образует группу относительно композиции. Эта группа называется *симметрической группой* и обозначается $\mathbb{S}_n$. Очевидно, $|\mathbb{S}_n| = n!$

Если $(\mathbb{G},\circ)$ — группа, $\mathbb{H} \subseteq \mathbb{G}$ и $\mathbb{H}$ является группой относительно операции $\circ$, то $\mathbb{H}$ называется *подгруппой* группы $\mathbb{G}$. Обозначение: $\mathbb{H} \leq \mathbb{G}$.

Примеры подгрупп.

- При каждом фиксированном k все числа, делящиеся на k, образуют подгруппу в $(\mathbb{Z},+)$.
- Подстановки на множестве $\{1,2,\dots,n\}$, оставляющие элемент k неподвижным, образуют подгруппу в группе $\mathbb{S}_n$.

Теорема Кэли. Любая конечная группа порядка n изоморфна некоторой подгруппе группы $\mathbb{S}_n$.

Доказательство. Предъявим требуемый изоморфизм. Пусть $\mathbb{G} = \{g_1, g_2, \dots, g_n\}$. Каждому элементу $a \in \mathbb{G}$ сопоставим отображение σ_a на множестве $\mathbb{G}$:

$$\sigma_a(g_1) \coloneqq g_1 \circ a$$
$$\vdots$$
$$\sigma_a(g_n) \coloneqq g_n \circ a$$

Для каждого a отображение σ_a является перестановкой, т.к. при $i \neq j$ имеем $g_i \circ a \neq g_j \circ a$ (ср. альтернативное определение конечных групп). Очевидно также, что при $a \neq b$ имеем $\sigma_a \neq \sigma_b$, то есть рассматриваемое сопоставление элементам $\mathbb{G}$ перестановок является биекцией из $\mathbb{G}$ в $\{\sigma_{g_1}, \dots, \sigma_{g_n}\}$.

Пусть σ_a и σ_b — перестановки, сопоставленные элементам $a, b \in \mathbb{G}$. Посмотрим, как себя ведёт композиция этих перестановок $\sigma_a\sigma_b$. Пусть $g \in \mathbb{G}$. Имеем

$$(\sigma_a\sigma_b)(g) = \sigma_b(g \circ a) = (g \circ a) \circ b = \sigma_{a\circ b}(g).$$

Осталось показать, что $\{\sigma_{g_1}, \dots, \sigma_{g_n}\}$ — группа относительно операции композиции. Нейтральная перестановка у нас есть — это σ_e, где e — нейтральный элемент в $\mathbb{G}$. Обратная перестановка к σ_a — это σ_b, где элемент b обратен к a в $\mathbb{G}$. Действительно, тогда $\sigma_a\sigma_b(x) = x \circ a \circ b = x \circ e = x$.

2.4. Теорема Лагранжа

Пусть $(\mathbb{G},\circ)$ — группа. Для элемента $a \in \mathbb{G}$ и подмножества $S \subseteq \mathbb{G}$ введём обозначения

$$a \circ S \coloneqq \{a \circ s \mid s \in S\}$$

и

$$S \circ a \coloneqq \{s \circ a \mid s \in S\}.$$

Утверждение. Для любого $a \in G$ и любого $S \subseteq \mathbb{G}$ имеем

$$|a \circ S| = |S \circ a| = |S|.$$

Доказательство (здесь и далее в мультипликативных обозначениях). Пусть $S = \{a_1, \dots, a_m\}$, где $m \coloneqq |S|$. Зафиксируем любой элемент $a \in \mathbb{G}$ и любые i, j. Если $aa_i = aa_j$, то $a^{-1}aa_i = a^{-1}aa_j$, откуда $a_i = a_j$. Значит, все элементы $aa_1, aa_2 \dots, aa_m$ различны.

Пусть $\mathbb{H} \leq \mathbb{G}$ и $a \in \mathbb{G}$. Множество $a \circ \mathbb{H}$ называется *левым смежным классом элемента a по подгруппе* $\mathbb{H}$. Аналогично, множество $\mathbb{H} \circ a$ называется *правым смежным классом*. Для абелевых групп соответствующие левые и правые смежные классы совпадают.

Отметим, что если $a \in \mathbb{H}$, то и правый, и левый смежные классы a по $\mathbb{H}$ совпадают с самой подгруппой $\mathbb{H}$.

Примеры смежных классов.

- Множество чисел вида $7 + 3k$ образует смежный класс в абелевой группе $(\mathbb{Z}, +)$.
- Для фиксированных i, j совокупность перестановок множества $\{1,2, \dots, n\}$, меняющих друг с другом местами i и j, образует смежный класс в группе $\mathbb{S}_n$.

Утверждение. Различные левые смежные классы по одной и той же подгруппе не пересекаются. Это же справедливо и для правых смежных классов.

Доказательство. Пусть $\mathbb{H} \leq G$ и $a', a'' \in G$. Допустим, что $a'\mathbb{H} \cap a''\mathbb{H} \neq \emptyset$ и покажем, что тогда $a'\mathbb{H} = a''\mathbb{H}$. Если $a'\mathbb{H} \cap a''\mathbb{H} \ni b$, то существуют $c, d \in \mathbb{H}$, такие, что $b = a'c = a''d$.

Рассмотрим произвольный элемент $s \in a'\mathbb{H}$. По определению, $\exists h \in \mathbb{H}$ такой, что $s = a'h$. Имеем $s = a'h = a''(dc^{-1})h = a''(dc^{-1}h)$. То есть $s \in a''\mathbb{H}$. Получаем, что $a'\mathbb{H} \subseteq a''\mathbb{H}$.

Аналогично доказывается, что $a''\mathbb{H} \subseteq a'\mathbb{H}$. Отсюда $a'\mathbb{H} = a''\mathbb{H}$. *Утверждение доказано.*

Теорема Лагранжа о порядке подгруппы. Если $\mathbb{H} \leq \mathbb{G}$ и $|\mathbb{G}| < \infty$, то $|\mathbb{G}|$ делится на $|\mathbb{H}|$.

Доказательство. Очевидно, любой элемент $a \in \mathbb{G}$ принадлежит некоторому смежному классу $\mathbb{H}$, а именно, $a \in a\mathbb{H}$. Различные смежные классы по $\mathbb{H}$ не пересекаются, поэтому имеет место разбиение $\mathbb{G} = a_1\mathbb{H} \sqcup a_2\mathbb{H} \sqcup \dots \sqcup a_m\mathbb{H}$, где $a_i\mathbb{H}$ — различные смежные классы. Так как $|a_i\mathbb{H}| = |\mathbb{H}|$ для каждого i, то $|\mathbb{G}| = m \cdot |\mathbb{H}|$. *Теорема доказана.*

2.5. Теорема Силова

Теорема Силова, в определённом смысле обратная к теореме Лагранжа утверждает, что для широкого класса чисел, делящих порядок группы, существует подгруппа, имеющая в точности такую мощность.

Теорема Силова о существовании подгруппы. Пусть $\mathbb{G}$ — конечная группа. Для любого числа вида p^α, делящего $|\mathbb{G}|$, существует $\mathbb{H} \leq \mathbb{G}$, такая, что $|\mathbb{H}| = p^\alpha$. (Здесь p простое, а α произвольное натуральное.)

Доказательство. Пусть $\beta \coloneqq \max\{x \mid |\mathbb{G}| \text{ делится на } p^x\}$. Зафиксируем произвольное $\alpha \leq \beta$. Имеем $|\mathbb{G}| = p^\beta l$, где l не делится на p. Положив $M \coloneqq \{S \subseteq \mathbb{G} \mid |S| = p^\alpha\}$, получаем

$$|M| = \binom{p^\beta l}{p^\alpha} = \frac{p^\beta l \cdot (p^\beta l - 1) \cdot \dots \cdot (p^\beta l - p^\alpha + 1)}{1 \cdot 2 \cdot \dots \cdot p^\alpha} = p^{\beta-\alpha} l \cdot \prod_{k=1}^{p^\alpha - 1} \frac{p^\alpha(p^{\beta-\alpha} l - 1) + k}{k}.$$

При $k < p^\alpha$ и $m \in \mathbb{N}$ степень, с которой p входит в разложение числа k, равна степени, с которой p входит в разложение числа $(p^\alpha m + k)$. Поэтому в произведении справа число p входит в одинаковых степенях в числитель и знаменатель дробей. Стало быть, наибольшая степень числа p, на которую делится $|M|$, равна $(\beta - \alpha)$.

Для $S \subseteq \mathbb{G}$ и $g \in \mathbb{G}$ обозначим $Sg \coloneqq \{sg \mid s \in S\}$. Очевидно, если $S \in M$, то $Sg \in M$.

Орбитой множества S назовём множество $\mathrm{orb}(S) \coloneqq \{Sg \mid g \in \mathbb{G}\}$. Для любого $S \in M$ выполнено включение $S \in \mathrm{orb}(S) \subseteq M$.

Покажем, что если $\mathrm{orb}(S') \cap \mathrm{orb}(S'') \neq \emptyset$, то $\mathrm{orb}(S') = \mathrm{orb}(S'')$. Допустим, что $\mathrm{orb}(S') \cap \mathrm{orb}(S'') \ni S$, тогда

$$\exists a, b \in G: \quad S'a = S''b.$$

Отсюда $S' = S''ba^{-1}$. Пусть $T \in \mathrm{orb}(S')$, т.е. $T = S'c$ для некоторого c. Но тогда $T = S''(ba^{-1}c) \in \mathrm{orb}(S'')$. Итак, $\mathrm{orb}(S') \subseteq \mathrm{orb}(S'')$. Точно так же доказывается, что $\mathrm{orb}(S'') \subseteq \mathrm{orb}(S')$, и следовательно $\mathrm{orb}(S') = \mathrm{orb}(S'')$. Следовательно, всё множество M разбивается на непересекающиеся орбиты: $\exists S_1, \dots, S_r$ такие, что

$$M = \mathrm{orb}(S_1) \sqcup \dots \sqcup \mathrm{orb}(S_r).$$

Наибольшая степень p, на которую делится $|M|$, равна $(\beta - \alpha)$, поэтому

$$\exists i: \quad |\mathrm{orb}(S_i)| \text{ не делится на } p^{\beta-\alpha+1}.$$

Зафиксируем $S \in M$, такое, что

$$\mathrm{orb}(S) = \{T_1, T_2, \dots, T_n\},$$

где n не делится на $p^{\beta-\alpha+1}$.

Положим $\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\}$. Если $g_1, g_2 \in \mathbb{H}$, то $T_1(g_1 g_2) = (T_1 g_1)g_2 = T_1 g_2 = T_1$, то есть $g_1 g_2 \in \mathbb{H}$.

Если $g \in \mathbb{H}$, то $T_1 g^{-1} = (T_1 g)g^{-1} = T_1(gg^{-1}) = T_1 e = T_1$, то есть $g^{-1} \in \mathbb{H}$.

Отсюда $\mathbb{H}$ — подгруппа в $\mathbb{G}$. Рассмотрим произвольный правый смежный класс $\mathbb{H}a$ по подгруппе $\mathbb{H}$. Пусть $T_1 a = T_k$. Рассмотрим произвольный элемент $g \in \mathbb{H}a$. Т.к. $g = ha$ для некоторого $h \in \mathbb{H}$, то $T_1 g = T_1(ha) = (T_1 h)a = T_1 a = T_k$. Оказалось, что любой правый смежный класс по подгруппе $\mathbb{H}$ может быть представлен как

$$\{g \in G \mid T_1 g = T_k\}$$

для некоторого k. А значит, общее число различных смежных классов по $\mathbb{H}$ равно n. Отсюда

$$n \cdot |\mathbb{H}| = |\mathbb{G}| = p^\beta l \quad \Rightarrow \quad |\mathbb{H}| = \frac{p^\beta l}{n},$$

и, так как n не делится на $p^{\beta-\alpha+1}$, то $|\mathbb{H}|$ делится на p^α.

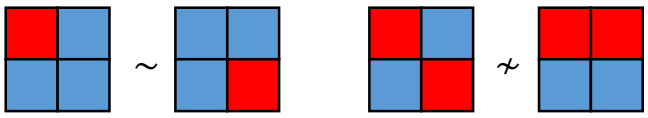
Достаточно теперь показать, что $|\mathbb{H}| \leq p^\alpha$. Возьмём произвольный $t \in T_1$. Для любого $h \in \mathbb{H}$ имеем $th \in T_1 h = T_1$. Отсюда $t\mathbb{H} \subseteq T_1$. Следовательно $|\mathbb{H}| = |t\mathbb{H}| \leq |T_1| = p^\alpha$.

Теорема доказана.

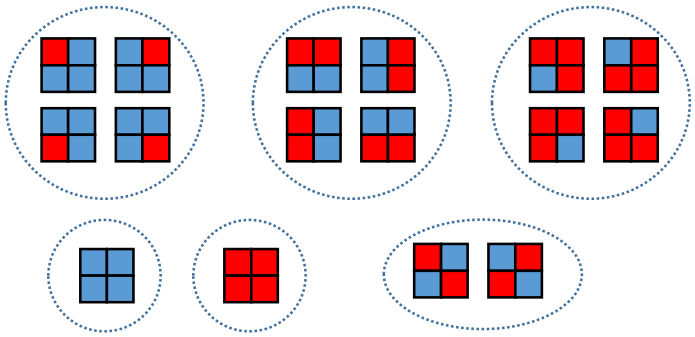
2.6. Теорема Редфилда—Пойи

2.6.1. Постановка задачи

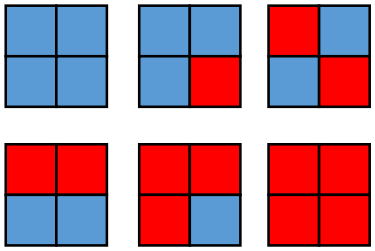
Рассмотрим такую задачу: сколькими способами можно раскрасить клетки доски 2×2 в красный и синий цвета? Раскраски считаются различными, если одну из другой нельзя получить поворотами доски:



Множество всевозможных раскрасок разбивается на классы эквивалентности, и нам нужно найти число этих классов.



Итак, раскрасить клетчатую доску 2×2 в красный и синий цвета можно шестью различными способами:



(На рисунке выше мы взяли по одной раскраске из каждого класса эквивалентности.)

Общая постановка задачи подсчёта числа раскрасок

- Дана *конфигурация* (клетчатая доска, таблица, многоугольник и т.д.), состоящая из отдельных *частей* (клеток, вершин/рёбер графа, …).
- Задано множество *цветов*, которые мы можем присваивать частям нашей конфигурации. *Раскраска* конфигурации — это присвоение каждому её элементу одного из цветов.
- Задана *группа перестановок* частей конфигурации. Две раскраски для нас *эквивалентны*, если они совпадают при какой-либо перестановке, принадлежащей группе.
- Нужно найти число классов эквивалентности.

Обозначения и термины

- $\mathbb{G}$ — группа перестановок частей конфигурации.
- Col — множество всевозможных раскрасок конфигурации ($|\mathrm{Col}| = \#\text{цветов}^{\#\text{частей}}$).
- Раскраска, переходящая сама в себя при перестановке π, называется *неподвижной* относительно π.
- Класс эквивалентности, в который входит раскраска, называется *орбитой* этой раскраски.

2.6.2. Лемма Бёрнсайда

Обозначим через $n_{\mathrm{stable}}(\pi)$ число раскрасок, неподвижных относительно π.

Лемма (Коши—Фробениуса—)Бёрнсайда. Число различных орбит раскрасок равняется

$$\frac{1}{|\mathbb{G}|} \cdot \sum_{\pi \in \mathbb{G}} n_{\mathrm{stable}}(\pi).$$

Доказательство. Пусть $\mathrm{Col}_1, \dots, \mathrm{Col}_m$ — все различные орбиты раскрасок. Пусть $\mathrm{Col}_i = \{c_1, \dots, c_r\}$ — произвольная из этих орбит. Положим

$$\mathbb{G}_{c_1} \coloneqq \{\pi \in \mathbb{G} \mid \pi \text{ переводит раскраску } c_1 \text{ саму в себя}\}.$$

Можно проверить, что $\mathbb{G}_{c_1}$ — подгруппа в $\mathbb{G}$. Она называется *стабилизатором* раскраски c_1.

Зафиксируем какую-нибудь раскраску c_j. Пусть $\pi' \in G$ — произвольная перестановка, переводящая c_1 в c_j. Докажем, что

$$\mathbb{G}_{c_1}\pi' = \{\sigma \in \mathbb{G} \mid \sigma \text{ переводит } c_1 \text{ в } c_j\}.$$

Пусть π — произвольная перестановка из $\mathbb{G}_{c_1}$. Тогда перестановка $\pi\pi'$ сначала действует как π (т.е. оставляет c_1 неподвижной), а затем как π', то есть переводит c_1 в c_j. Тем самым мы доказали вложенность

$$\mathbb{G}_{c_1}\pi' \subseteq \{\sigma \in \mathbb{G} \mid \sigma \text{ переводит } c_1 \text{ в } c_j\}.$$

Теперь докажем включение в обратную сторону. Пусть $\sigma \in \mathbb{G}$ и σ переводит c_1 в c_j. Тогда $\sigma(\pi')^{-1}$ переводит c_1 саму в себя, то есть $\sigma(\pi')^{-1} \in \mathbb{G}_{c_1}$. Отсюда $\sigma \in \mathbb{G}_{c_1}\pi'$.

Мы доказали, что для каждого j множество $\{\sigma \in \mathbb{G} \mid \sigma \text{ переводит } c_1 \text{ в } c_j\}$ суть смежный класс подгруппы $\mathbb{G}_{c_1}$. Отсюда вытекает равенство

$$\#\{\sigma \in \mathbb{G} \mid \sigma \text{ переводит } c_1 \text{ в } c_j\} = |\mathbb{G}_{c_1}|$$

для каждого $j \in \{1, \dots, r\}$. Отсюда следует, что $|\mathrm{Col}_i| \cdot |G_{c_1}| = |\mathbb{G}|$.

Из доказанного выше следует, что для любой орбиты Col_i и любой раскраски $c \in \mathrm{Col}_i$ выполнено равенство

$$\#\{\pi \in \mathbb{G} \mid \pi \text{ переводит } c \text{ саму в себя}\} = \frac{|\mathbb{G}|}{|\mathrm{Col}_i|}.$$

Для раскраски c и перестановки $\pi \in \mathbb{G}$ положим

$$\mathbb{1}_{\pi,c} := \begin{cases} 1, \text{ если } c \text{ неподвижна относительно } \pi \\ 0, \text{ иначе} \end{cases}$$

Имеем

$$\sum_{\pi\in\mathbb{G}} n_{\text{stable}}(\pi) = \sum_{\pi\in\mathbb{G}}\sum_{c\in\mathrm{Col}} \mathbb{1}_{\pi,c} = \sum_{c\in\mathrm{Col}}\sum_{\pi\in\mathbb{G}} \mathbb{1}_{\pi,c} = \sum_{i=1}^{m}\sum_{c\in\mathrm{Col}_i}\sum_{\pi\in\mathbb{G}} \mathbb{1}_{\pi,c}$$
$$= \sum_{i=1}^{m}\sum_{c\in\mathrm{Col}_i} \#\{\pi \in \mathbb{G} \mid \pi \text{ переводит } c \text{ саму в себя}\} = \sum_{i=1}^{m}\sum_{c\in\mathrm{Col}_i} \frac{|\mathbb{G}|}{|\mathrm{Col}_i|} = \sum_{i=1}^{m} |\mathbb{G}| = m \cdot |\mathbb{G}|.$$

Отсюда

$$m = \frac{1}{|\mathbb{G}|} \cdot \sum_{\pi\in\mathbb{G}} n_{\text{stable}}(\pi)\,,$$

что и требовалось. *Лемма Бёрнсайда доказана.*

2.6.3. Теорема Редфилда—Пойи

Теорема Редфилда—Пойи. Число различных орбит раскрасок конфигурации в цвета из множества $\{1, \dots, l\}$ равно

$$\frac{1}{|\mathbb{G}|} \cdot \sum_{\pi\in\mathbb{G}} l^{\#\text{циклов в } \pi}.$$

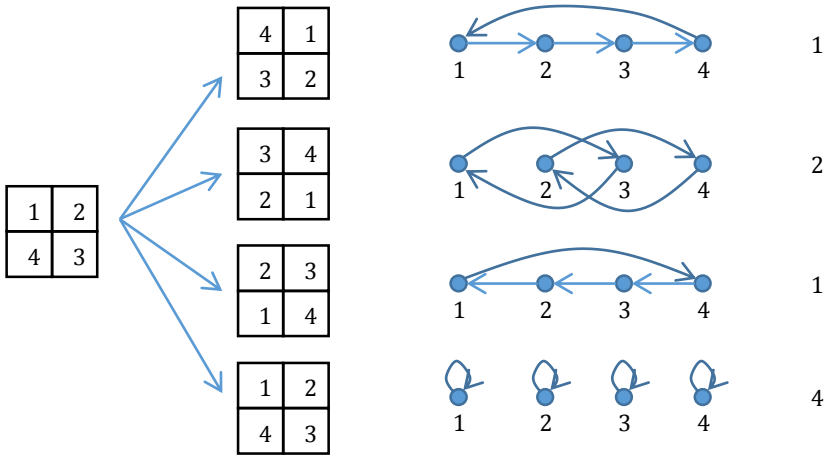
Доказательство. Заметим, что раскраска неподвижна относительно перестановки т. и т.т., когда части конфигурации, входящие в один и тот же цикл перестановки, окрашены одинаково. Поэтому количество раскрасок, неподвижных относительно перестановки π, равно $l^{\#\text{циклов в } \pi}$. Осталось применить лемму Бёрнсайда.

Следствие. Если в конфигурации n частей, то количество орбит раскрасок в не более чем l цветов при $l \to \infty$ асимптотически равно $\frac{l^n}{|\mathbb{G}|}$.

Доказательство. Заметим, что любой группе перестановок принадлежит тождественная перестановка; в ней n циклов, а в любой другой перестановке менее чем n циклов. По теореме Редфилда—Пойи, число различных орбит равно

$$\frac{1}{|\mathbb{G}|} \cdot \left(l^n + \sum_{\substack{\pi \in \mathbb{G} \\ \pi \text{ не тожд.}}} l^{\#\text{циклов в } \pi} \right) \leq \frac{1}{|\mathbb{G}|} \cdot (l^n + (|\mathbb{G}| - 1) \cdot l^{n-1}) \sim \frac{l^n}{|\mathbb{G}|}.$$

Пример применения теоремы Редфилда—Пойи. Сколькими способами можно раскрасить доску 2×2 в цвета из множества $\{1, \dots, l\}$, если раскраски, переходящие друг в друга при вращении квадрата, считаются одинаковыми? Сначала найдём количество циклов в перестановках клеток доски при вращениях:



Применив теорему Редфилда—Пойи, получаем

$$\#\text{раскрасок} = \frac{l^4 + l^2 + 2l}{4} \sim \frac{l^4}{4}.$$

2.7. Группы вычетов

В этом и следующих разделах часто будут возникать простые числа. Полезно помнить, что их достаточно много. Многие знают следующую широко известную теорему.

Теорема (постулат Бертрана). Для любого $n \in \mathbb{N}$ в интервале $[n, 2n]$ лежит хотя бы одно простое число.

На самом деле, при больших $\mathbb{N}$ можно дать куда лучшую оценку. Ниже приведён самый точный из известных на сегодняшний день асимптотических результатов о существовании простых чисел.

Теорема (Бейкер, Харман, Пинц). Для любого достаточно большого n в интервале $\left[n, n + n^{21/40}\right]$ лежит хотя бы одно простое число.

Введём нужные для дальнейшего обозначения. Для любых $n \in \mathbb{Z}$ и $m \in \mathbb{Z} \setminus \{0\}$ существуют и однозначно определены $k, r \in \mathbb{N}_0$, такие, что

$$n = k \cdot m + r,$$
$$r < m.$$

Число r — *остаток от деления* n *на* m, или *вычет числа* n *по модулю* m. Обозначение: $r = n \bmod m$.

Если $n_1 \bmod m = n_2 \bmod m$, то пишут $n_1 \equiv n_2 \pmod m$ и говорят, что n_1 и n_2 *равны по модулю* m. Мы ещё будем обозначать это так: $n_1 \overset{m}{=} n_2$.

Утверждение. Пусть $n_1 \overset{m}{=} n_2$ и $n_3 \overset{m}{=} n_4$. Тогда

$$n_1 + n_3 \overset{m}{=} n_2 + n_4,$$
$$n_1 - n_3 \overset{m}{=} n_2 - n_4,$$
$$n_1 n_3 \overset{m}{=} n_2 n_4.$$

Доказательство. По условию,

$$n_1 = k_1 \cdot m + r',$$
$$n_2 = k_2 \cdot m + r',$$
$$n_3 = k_3 \cdot m + r'',$$
$$n_4 = k_4 \cdot m + r''.$$

Отсюда

$$n_1 + n_3 = (k_1 + k_3) \cdot m + r' + r'' \overset{m}{=} r' + r'',$$
$$n_2 + n_4 = (k_2 + k_4) \cdot m + r' + r'' \overset{m}{=} r' + r''.$$

Следовательно, $n_1 + n_3 \overset{m}{=} n_2 + n_4$. Совершенно аналогично доказываются остальные равенства.

Утверждение. Если $n_1 \overset{m}{=} n_2$, то $n_1^k \overset{m}{=} n_2^k$ для любого k.

Доказательство можно провести индукцией по k с использованием предыдущего утверждения.

Вычисления по модулю можно легко производить даже с очень большими числами, если модуль небольшой.

Пример. Какому числу из $[0,10]$ равно по модулю 11 значение выражения $4^{100} \cdot 10^6 + 18^{85}$?

Решение:

$$4^{100} \cdot 10^6 + 18^{85} = (11+5)^{50} \cdot (11-1)^6 + (22-4)^{85} \overset{11}{=} 5^{50} \cdot (-1)^6 + (-4)^{85} = 25^{25} - 2^{10 \cdot 17}$$
$$= (22+3)^{25} - (93 \cdot 11 + 1)^{17} \overset{11}{=} 3^{25} - 1 = 243^5 - 1 = (2 \cdot 121 + 1)^5 - 1 \overset{11}{=} 0.$$

Утверждение. Множество чисел $\mathbb{Z}_m := \{0,1,\dots,m-1\}$ образует группу относительно операции $\bigoplus$. Через $\bigoplus$ обозначена операция *сложения по модулю* m, то есть $x \bigoplus y$ — это такое число $z \in \mathbb{Z}_m$, что $z \overset{m}{=} x + y$. Группу $\mathbb{Z}_m$ называют *аддитивной группой вычетов по модулю* m.

Пример. Если мы работаем в $\mathbb{Z}_5$, то $3 \bigoplus 2 = 0$ и $4 \bigoplus 4 = 3$. Операцию $\bigoplus$ будем обычно обозначать просто $+$.

Доказательство утверждения.

- Ассоциативность операции. Пусть $a \bigoplus (b \bigoplus c) = z'$ и $(a \bigoplus b) \bigoplus c = z''$. Тогда $z' \overset{m}{=} a + d$, где $d \overset{m}{=} b + c$, и следовательно $z' \overset{m}{=} a + b + c$. Аналогично, $z'' \overset{m}{=} a + b + c$. Так как $z' \overset{m}{=} z''$ и $z', z'' < m$, то $z' = z''$.

- Нейтральный элемент: 0.
- Существование обратных элементов. Для 0 обратный элемент 0. Для $a \neq 0$ обратным будет $(m - a)$, т.к. $a + (m - a) = m \overset{m}{=} 0$.

Утверждение доказано.

Если конечная группа $\mathbb{G}$ изоморфна группе $\mathbb{Z}_{|\mathbb{G}|}$, то $\mathbb{G}$ называется *циклической* группой. Также циклическими называют бесконечные группы, изоморфные группе $(\mathbb{Z}, +)$.

Примеры циклических групп:

- группа поворотов плоскости относительно начала координат на угол, кратный $\frac{2\pi}{m}$,
- группа чисел вида $\{n^a \mid a \in \mathbb{Z}\}$ относительно умножения (при фиксированном n).

Пусть $\mathbb{G}$ — группа с операцией $\circ$. Для каждого $k \in \mathbb{N}$ обозначим

$$a^{\circ k} \coloneqq \underbrace{a \circ a \circ \ldots \circ a}_{k \text{ раз}}.$$

По определению положим $a^{\circ 0} \coloneqq e$, где e — нейтральный элемент группы.

Порядком элемента $a \in \mathbb{G}$ называется такое *наименьшее* $k > 0$, для которого

$$a^{\circ k} = e,$$

где e — нейтральный элемент в $\mathbb{G}$. Обозначается порядок так: $\operatorname{ord} a$. Если такого k не существует, порядок элемента считается равным ∞.

Утверждение. У каждого элемента в *конечной* группе есть конечный порядок.

Доказательство. В последовательности $a, a \circ a, a \circ a \circ a, \ldots$ обязательно возникнет повторение: для $k > 0$ выполнится равенство

$$a^{\circ s} = a^{\circ (s+k)}.$$

Отсюда сразу следует, что $a^{\circ k} = e$. *Утверждение доказано.*

Утверждение. Пусть $a \in \mathbb{G}$ и $\operatorname{ord} a = r < \infty$. Тогда множество

$$\mathbb{H} \coloneqq \{a^{\circ k} \mid k \in [0, r)\}$$

является подгруппой группы $\mathbb{G}$ и образует циклическую группу, изоморфную $\mathbb{Z}_r$. Множество $\{a^{\circ k} \mid k \in [0, \operatorname{ord} a)\}$ называется подгруппой, *порождённой элементом* a, и обозначается $\langle a \rangle$.

Доказательство. Вначале докажем, что $\mathbb{H}$ является группой. Нейтральный элемент $e \in \mathbb{H}$. При $s \geq 1$ для элемента $a^{\circ s} \in \mathbb{H}$ обратным будет элемент $a^{\circ (r-s)}$. При этом $|\mathbb{H}| = r$, поскольку в силу определения порядка элемента, если $m < n$ и $a^{\circ m} = a^{\circ n}$, то $|m - n| \geq r$.

Остаётся показать, что $\mathbb{H}$ — циклическая подгруппа. Изоморфизм $\phi\colon \mathbb{H} \to \mathbb{Z}_r$ очевиден:

$$\forall k \in [0, r) \qquad \phi(a^{\circ k}) \coloneqq k.$$

Поскольку $a^{\circ m} \circ a^{\circ n} = a^{\circ \left((m+n) \bmod r\right)}$, имеем

$$\phi(a^{\circ m} \circ a^{\circ n}) = (m + n) \bmod r = \phi(a^{\circ m}) \oplus \phi(a^{\circ n}),$$

то есть ϕ сохраняет групповую операцию, что и требовалось.

Утверждение доказано.

Утверждение. Множество чисел

$$\mathbb{Z}_m^\times = \{k \in (0,m) \mid k \text{ взаимно просто с } m\}$$

образует группу относительно операции $\odot$. Через $\odot$ обозначена операция *умножения по модулю* m. По определению $x \odot y = z$, если $z \in \mathbb{Z}_m^\times$ и $z \overset{m}{=} x \cdot y$. Например, в $\mathbb{Z}_9^\times$ имеем $2 \odot 5 = 1$ и $4 \odot 4 = 7$. Операцию $\odot$ будем обычно обозначать просто $\cdot$. Группу $\mathbb{Z}_m^\times$ называют *мультипликативной группой вычетов по модулю* m.

Доказательство. Ассоциативность $\odot$ доказывается так же, как для $\oplus$. Нейтральный элемент: 1. Нетривиально только доказательство существования обратных элементов, которое мы сейчас и проведём. Пусть $a \in \mathbb{Z}_m^\times$ и $a \neq 1$. Так как $\mathbb{Z}_m^\times$ конечно, то в последовательности

$$a, \quad a \odot a, \quad a \odot a \odot a, \ldots$$

есть повторяющиеся элементы. То есть $a^{k+l} \overset{m}{=} a^k$ для некоторых $k, l \in \mathbb{N}$. Имеем

$$a^{k+l} - a^k \overset{m}{=} 0 \quad \Rightarrow \quad a^k(a^l - 1) \overset{m}{=} 0.$$

Так как a и m взаимно просты, то $a^l - 1 \overset{m}{=} 0$. Отсюда следует, что элемент $b \coloneqq a^{l-1} \bmod m$ будет обратным к a, поскольку $a \odot b \overset{m}{=} a^l \overset{m}{=} 1$.

Следствие. Для любого простого p множество $\mathbb{Z}_p \setminus \{0\}$ образует группу относительно умножения по модулю p.

2.7.1. Теоремы Ферма и Эйлера

Функция Эйлера — это функция натурального аргумента, определяемая так:

$$\varphi(m) \coloneqq \#\{k < m \mid m \text{ и } k \text{ взаимно просты}\} = |\mathbb{Z}_m^\times|.$$

Примеры.

- $\varphi(2^n) = 2^{n-1}$ для любого $n \in \mathbb{N}$,
- $\varphi(p) = p - 1$ для любого простого p,
- $\varphi(30) = \#\{1,7,11,13,17,19,23,29\} = 8$.

Теорема Эйлера—Ферма. Если $a, m \in \mathbb{N}$ — взаимно простые числа, то $a^{\varphi(m)} \overset{m}{=} 1$.

Доказательство. Пусть $b \coloneqq a \bmod m$. Достаточно доказать, что $b^{\varphi(m)} \overset{m}{=} 1$. Заметим, что $b \in \mathbb{Z}_m^\times$, и рассмотрим группу $\langle b \rangle$. Имеем $|\langle b \rangle| = \operatorname{ord} b$, $|\mathbb{Z}_m^\times| = \varphi(m)$. Поскольку $\langle b \rangle$ — подгруппа $\mathbb{Z}_m^\times$, то по теореме Лагранжа получаем $\varphi(m) = t \cdot \operatorname{ord} b$ для некоторого $t \in \mathbb{N}$. Отсюда

$$b^{\varphi(m)} = b^{t \cdot \operatorname{ord} b} = \left(b^{\operatorname{ord} b}\right)^t \quad \overset{m}{=} \quad 1.$$

Прямым следствием доказанной теоремы является следующее известное утверждение.

Малая теорема Ферма. Для любого простого p и для любого a имеем $a^p \overset{p}{=} a$.

С использованием теорем Эйлера и Ферма, вычисления по модулю становятся ещё эффективнее.
Пример. Какому числу из $[0,10]$ равно по модулю 11 значение выражения $4^{100} \cdot 10^6 + 18^{85}$?
Решение:

$$4^{100} \cdot 10^6 + 18^{85} \overset{11}{=} (4^{10})^{10} \cdot (-1)^6 + (-4)^{80+5} \overset{11}{=} 1 + ((-4)^8)^{10} \cdot (-4)^5 \overset{11}{=} 1 - 4^5 = 1 - 2^{10} \overset{11}{=} 0.$$

Для демонстрации взаимосвязей между разными областями дискретной математики приведём комбинаторное доказательство малой теоремы Ферма, использующее циклические слова. Это доказательство принадлежит Дейкстре.

Будем доказывать малую теорему Ферма в следующем эквивалентном виде: «для простого p и натурального a выполнено $a^p \overset{p}{=} a$». Рассмотрим множество W всех слов длины a в p-символьном алфавите, содержащих хотя бы две различные буквы. Очевидно, $|W| = a^p - a$. Пусть $W_{\text{ц}}$ — всевозможные циклические слова, соответствующие словам из W. Поскольку длина каждого слова из $W_{\text{ц}}$ равна простому числу p, а период этого слова должен делить длину, то период равен единице или p. Так как в словах из $W_{\text{ц}}$ встречается не менее двух букв, то период не может быть равен единице. Значит, каждое циклическое слово из $W_{\text{ц}}$ имеет период p и, следовательно, порождает ровно p обычных слов. Отсюда $|W| = p \cdot |W_{\text{ц}}|$, а стало быть, $a^p - a \overset{p}{=} 0$.

3. Поля и многочлены

3.1. Основное определение и примеры полей

В этом разделе мы введём понятие поля и укажем способ построения конечных полей.

Поле — это множество $\mathbb{F}$ с двумя бинарными ассоциативными *и коммутативными* операциями $+$ и $\cdot$, такими, что

- $\mathbb{F}$ является группой относительно $+$. Нейтральный элемент этой группы обозначается 0.
- $\mathbb{F} \setminus \{0\}$ является группой относительно $\cdot$. Нейтральный элемент этой группы обозначается 1.
- Операция $\cdot$ дистрибутивна относительно $+$:

$$\forall a, b, c \in \mathbb{F} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Полями являются, например, множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ относительно обычных сложения и умножения.

Полями не являются множества $\mathbb{N}, \mathbb{Z}$, а также множество $\mathbb{R}^{n \times n}$ относительно сложения и умножения матриц (объясните, почему). Кроме $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ есть и другие, более экзотические бесконечные поля, например, *поле дробно-рациональных функций*, т.е. множество

$$\left\{ f \mid f = \frac{A(x)}{B(x)} \right\},$$

где $A(x)$ и $B(x)$ — многочлены с целыми коэффициентами, и $B(x) \not\equiv 0$.

Конечные поля также существуют, как показывает следующее утверждение.

Утверждение. Для любого простого p множество $\mathbb{Z}_p$ образует поле относительно операций сложения и умножения по модулю p.

Доказательство. То, что $(\mathbb{Z}_p, \oplus)$ и $(\mathbb{Z}_p \setminus \{0\}, \odot)$ — группы, доказано ранее. Дистрибутивность умножения по модулю относительно сложения по модулю очевидна.

3.2. Два простых свойства полей

Используя лишь базовые аксиомы полей, можно выводить свойства нейтральных по сложению и умножению, которые очевидны в случае привычных нам числовых полей. На первый взгляд, в следующих двух утверждениях «доказывать нечего», но это ощущение пропадает, если вспомнить, например, что через 0 мы обозначаем не действительное число *нуль*, а нейтральный по сложению элемент произвольного поля. Точно так же, (-1) — это не целое число *минус единица*, а элемент, обратный по сложению к нейтральному по умножению элементу поля.

Утверждение. Если $\mathbb{F}$ поле, то для любого $a \in \mathbb{F}$ выполнено соотношение $a \cdot 0 = 0$.

Доказательство. Обозначим $z \coloneqq a \cdot 0$. Имеем

$$z + z = a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = z.$$

Отсюда

$$z = 0 + z = (-z) + z + z = (-z) + z = 0.$$

Утверждение. Если $\mathbb{F}$ поле, то для любого $a \in \mathbb{F}$ выполнено соотношение $(-1) \cdot a = -a$.

Доказательство. Обозначим $b \coloneqq (-1) \cdot a$. Получаем

$$b + a = b + 1 \cdot a = (-1) \cdot a + 1 \cdot a = \big((-1) + 1\big) \cdot a = 0 \cdot a = 0.$$

3.3. Альтернативные определения поля

3.3.1. Второе определение поля

Вспомнив, что группу можно определить как множество с ассоциативной операцией, в котором имеют решения простые уравнения, мы можем определить поле следующим образом. Поле — это множество $\mathbb{F}$ с двумя бинарными ассоциативными операциями $+$ и $\cdot$, и с двумя специальными элементами 0 и 1, такими, что

- $\forall a, b \quad a + b = b + a, \quad a \cdot b = b \cdot a$
- $\forall a, b, c \in \mathbb{F} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- $\forall a \in \mathbb{F} \quad 0 + a = a + 0 = a$
- $\forall a \in \mathbb{F} \setminus \{0\} \quad 1 \cdot a = a \cdot 1 = a$
- $\forall a, b \in \mathbb{F} \quad \exists x\colon \ a + x = b$
- $\forall a, b \in \mathbb{F} \setminus \{0\} \quad \exists x\colon \ a \cdot x = b$

3.3.2. Альтернативное определение для конечного поля

Основываясь на альтернативном определении конечных групп, мы можем получить следующее определение полей. Конечное поле — это множество $\mathbb{F} = \{a_1, \dots, a_n\}$ с бинарными ассоциативными коммутативными операциями $+$ и $\cdot$, такими, что

- $\forall a, b, c \in \mathbb{F} \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
- $\forall a$ все элементы $a + a_1, \ \dots, a + a_n$ различны (а стало быть, $\mathbb{F}$ образует группу относительно $+$, нейтральный элемент которой мы обозначим 0),
- $\forall a \in \mathbb{F} \setminus \{0\}$ все элементы $a \cdot a_1, \dots, a \cdot a_n$ различны.

3.4. Многочлены и поля на их основе

3.4.1. Определения и обозначения

Многочлен (*полином*) от переменных $x_1, \dots, x_m$ с коэффициентами из множества K — это конечная сумма *одночленов* (*мономов*) т.е. произведений вида

$$c \cdot x_{i_1}^{t_1} \cdot \dots \cdot x_{i_r}^{t_m},$$

где

$$\begin{aligned} &c \in K, \\ &t_1, \dots, t_m \in \mathbb{N}_0, \\ &i_1, \dots, i_r \in \{1, \dots, m\}. \end{aligned}$$

Если $r = 0$, то моном называется *свободным членом*.

Степень монома $T = c \cdot x_{i_1}^{t_1} \cdot \dots \cdot x_{i_r}^{t_m}$ — это величина

$$\deg T \coloneqq t_1 + \dots + t_m.$$

Степень полинома P определяется так:

$$\deg P \coloneqq \max\{\deg T \quad | \quad T \text{ — моном } P\}.$$

Степень *нулевого* (тождественно равного нулю) многочлена считается равной $-\infty$.

Степень монома $T = c \cdot x_{i_1}^{t_1} \cdot \ldots \cdot x_{i_r}^{t_m}$ *по переменной* x_k — это показатель, с которым x_k входит в произведение T. Обозначение: $\deg_{x_k} T$.

Степень полинома P *по переменной* x_k равна

$$\deg_{x_k} P \coloneqq \max\{\deg_{x_k} T \quad | \quad T \text{ — моном } P\}.$$

Если $P \equiv 0$, то полагаем $\deg_{x_k} P \coloneqq -\infty$.

Следующее утверждение доказывается прямой проверкой.

Утверждение. Если P' и P'' — многочлены, то

$$\deg(P' + P'') \le \max\{\deg P', \deg P''\},$$
$$\deg(P' \cdot P'') = \deg P' + \deg P'',$$

то же справедливо и для степеней по переменным:

$$\deg_{x_k}(P' + P'') \le \max\{\deg_{x_k} P', \deg_{x_k} P''\},$$
$$\deg_{x_k}(P' \cdot P'') = \deg_{x_k} P' + \deg_{x_k} P''.$$

Если коэффициенты многочлена P от переменных $x_1, \ldots, x_m$ берутся из некоторого множества K, то пишут $P \in K[x_1, \ldots, x_m]$. Если для любых $a, b \in K$ сумма $(a + b)$ и произведение $(a \cdot b)$ также лежат в K, то множество $K[x_1, \ldots, x_m]$ тоже замкнуто относительно сложения и умножения многочленов. Часто в качестве K рассматривают некоторое *поле*, и тогда обычно пишут $P \in \mathbb{F}[x_1, \ldots, x_m]$.

Многочлен $P \in \mathbb{F}[x]$, у которого коэффициент при мономе старшей степени равен 1, называется *нормированным*. Кратко будем называть нормированные многочлены *нормногочлеными*. Очевидно, любой многочлен можно получить из некоторого нормногочлена умножением на константу.

Доказательство следующего утверждение полностью аналогично доказательству теорему о делении натуральных чисел с остатком.

Утверждение. Для любых многочленов $P, Q \in \mathbb{F}[x]$ при $Q \not\equiv 0$ существуют и однозначно определены многочлены S и R, такие, что $P = Q \cdot S + R$ и $\deg R < \deg Q$. Многочлен R называется *остатком* от деления P на Q.

Если R — остаток от деления P на Q, будем писать $R = P \bmod Q$. Если $P_1 \bmod Q = P_2 \bmod Q$, то будем обозначать это $P_1 \equiv P_2 \pmod{Q}$ или $P_1 \overset{Q}{=} P_2$.

Нетрудно проверить, что сравнения по модулю многочленов ведут себя так же, как сравнения по модулю целых чисел.

Утверждение. Если $P_1 \overset{Q}{=} P_2$ и $P_3 \overset{Q}{=} P_4$, то

$$P_1 + P_3 \overset{Q}{=} P_2 + P_4,$$
$$P_1 \cdot P_3 \overset{Q}{=} P_2 \cdot P_4,$$
$$\forall k \in \mathbb{N} \quad (P_1)^k \overset{Q}{=} (P_2)^k.$$

Пример. Найдём остаток от деления многочлена

$$P \coloneqq (x^5 + 2x^3 + 4)^4 \cdot (x^3 + 3) + x$$

на многочлен $\mathrm{Q} \coloneqq x^2 + 2$, где все многочлены принадлежат $\mathbb{Z}_5[x]$.

Решение:

$$x^5 + 2x^3 + 4 = (x^2 + 2)x^3 + 4 \overset{Q}{=} 4 \overset{\mathbb{Z}_5}{=} -1,$$

$$x^3 + 3 = (x^2 + 2)x - 2x + 3 \overset{Q}{=} -2x + 3.$$

Отсюда $P \overset{Q}{=} (-1)^4 \cdot (-2x + 3) + x = -x + 3 = 4x + 3.$

Многочлен $P \in \mathbb{F}[x]$ называется *неприводимым/неразложимым/простым* (*над* $\mathbb{F}$), если не существует $Q, S \in \mathbb{F}[x]$, таких, что

$$P = Q \cdot S, \quad \deg Q \geq 1, \quad \deg S \geq 1.$$

Примеры.

- $x^2 + x + 1$ неприводим над $\mathbb{R}$, так как если бы его можно было разложить на множители, то у него были бы корни в $\mathbb{R}$.
- $P = x^4 + 2x^3 + 3x^2 + 2x + 1$ не является неприводимым над $\mathbb{R}$, так как $P = (x^2 + x + 1)^2$. Заметьте, что корней у P при этом всё же нет.
- $x^2 + x + 1$ неприводимый над $\mathbb{Z}_2$, так как ни 0, ни 1 не являются его корнями (если вычисления выполнять по модулю 2).
- $x^2 + x + 1$ не является неприводимым над $\mathbb{Z}_3$, так как $x^2 + x + 1 \overset{3}{=} x^2 + 4x + 4 = (x + 2)^2$.

Доказательство следующей теоремы полностью повторяет доказательство основной теоремы арифметики.

Теорема. Любой многочлен $P \in \mathbb{F}[x]$ может быть единственным образом (с точностью до перестановки сомножителей) представлен в виде $P = c \cdot P_1 \cdot \ldots \cdot P_k$, где $P_1, \ldots, P_k$ — простые (не обязательно различные) нормногочлены из $\mathbb{F}[x]$.

Также аналогичны фактам из арифметики следующие утверждения о многочленах.

Утверждение. Если $P_1 \cdot P_2$ делится на Q, и Q простой, то хотя бы один из многочленов P_1, P_2 делится на Q. Если P делится на различные простые многочлены Q_1 и Q_2, то P делится на $Q_1 \cdot Q_2$.

3.4.2. Конечные поля вычетов по модулю многочлена

Пусть p — простое число и пусть Q — простой многочлен из $\mathbb{Z}_p[x]$. Обозначим через $\mathbb{Z}_p[x]/Q$ множество всех многочленов из $\mathbb{Z}_p[x]$, степень которых строго меньше $\deg Q$. На множестве $\mathbb{Z}_p[x]/Q$ определим операции сложения и умножения:

$$P_1 \oplus P_2 \coloneqq (P_1 + P_2) \bmod Q,$$
$$P_1 \odot P_2 \coloneqq (P_1 \cdot P_2) \bmod Q.$$

Теорема. Множество $\mathbb{Z}_p[x]/Q$ является полем относительно введённых операций сложения и умножения многочленов по модулю Q.

Доказательство. Докажем, что множество $\mathbb{Z}_p[x]/Q$ удовлетворяет альтернативному определению конечного поля. Ассоциативность, коммутативность, дистрибутивность операций очевидна. Докажем, что $\forall P, P_1, P_2 \in \mathbb{Z}_p[x]/Q$ из $P_1 \neq P_2$, вытекает $P \oplus P_1 \neq P \oplus P_2$. Это так, поскольку

$$P \oplus P_1 = P \oplus P_2 \quad \Rightarrow \quad P + P_1 \overset{Q}{=} P + P_2 \quad \Rightarrow \quad P_1 \overset{Q}{=} P_2 \quad \Rightarrow \quad P_1 = P_2.$$

Таким образом, $\mathbb{Z}_p[x]/Q$ — группа относительно операции $\oplus$. Очевидным нейтральным элементом является тождественно нулевой многочлен. Осталось доказать, что $\forall P, P_1, P_2 \in \mathbb{Z}_p[x]/Q$ из $P_1 \neq P_2$ и $P \not\equiv 0$ следует $P \odot P_1 \neq P \odot P_2$. Докажем это в обратном порядке. Пусть $P \odot P_1 = P \odot P_2$, тогда

$$P \cdot P_1 \overset{Q}{=} P \cdot P_2 \quad \Rightarrow \quad P \cdot (P_1 - P_2) \overset{Q}{=} 0.$$

Т.к. Q простой, то либо P делится на Q, либо $(P_1 - P_2)$ делится на Q. По условию, $P \not\equiv 0$, а значит

$$(P_1 - P_2) \overset{Q}{=} 0 \quad \Rightarrow \quad P_1 \overset{Q}{=} P_2 \quad \Rightarrow \quad P_1 = P_2.$$

Теорема доказана.

3.5. Количество неприводимых нормированных многочленов над $\mathbb{Z}_p$

Чтобы доказать, что конечные поля вида $\mathbb{Z}_p[x]/Q$ существуют при любых простых p, нам нужно убедиться, что для каждого p существуют многочлены, неприводимые над $\mathbb{Z}_p$. Оказывается, неприводимые многочлены существуют для любого p и любой степени, не меньшей двух.

Пусть $f_1, f_2, \ldots$ — последовательность всех простых нормногочленов над $\mathbb{Z}_p$, в порядке неубывания их степеней. Обозначим $d_i \coloneqq \deg f_i$. По теореме, аналогичной основной теореме арифметики, любой нормногочлен f представляется единственным образом в виде $f = (f_{i_1})^{\alpha_{i_1}} \cdot \ldots \cdot (f_{i_s})^{\alpha_{i_s}}$, где $i_1 < i_2 < \cdots < i_s$ и $\alpha_{i_1}, \ldots, \alpha_{i_s} > 0$. Очевидно, выполнено соотношение $\deg f = \alpha_1 d_{i_1} + \cdots + \alpha_s d_{i_s}$.

Дополнив для удобства обозначений набор $(\alpha_{i_1}, \ldots, \alpha_{i_s})$ нулями, мы можем сформулировать следующее предложение: любой последовательности $(\alpha_1, \alpha_2, \ldots)$, такой, что $\sum_{i=1}^{\infty} \alpha_i d_i = k$, можно взаимно однозначно сопоставить нормногочлен степени k. А поскольку количество нормногочленов из $\mathbb{Z}_p[x]$ степени k равно p^k, мы получаем, что для любого k число решений уравнения

$$k = d_1 x_1 + d_2 x_2 + \cdots$$

в целых неотрицательных числах равно p^k.

Утверждение. Выполнено равенство

$$\prod_{i=1}^{\infty} \frac{1}{1 - t^{d_i}} = \frac{1}{1 - pt}.$$

Доказательство. Так как $(1 - t^{d_i})^{-1} = 1 + t^{d_i} + t^{2d_i} + t^{3d_i} + \cdots$, то

$$\prod_{i=1}^{\infty} (1 - t^{d_i})^{-1} = \prod_{i=1}^{\infty} \left(\sum_{x_i=0}^{\infty} t^{x_i d_i} \right) = \sum_{k=0}^{\infty} a_k t^k,$$

где a_k — количество решений уравнения $k = d_1 x_1 + d_2 x_2 + \cdots$ в целых неотрицательных числах. Но это значит, что $a_k = p^k$. Отсюда

$$\prod_{i=1}^{\infty} (1 - t^{d_i})^{-1} = \sum_{k=0}^{\infty} p^k t^k = \sum_{k=0}^{\infty} (pt)^k = \frac{1}{1 - pt}.$$

Утверждение доказано.

Пусть M_k — количество простых нормногочленов степени k. Тогда

$$\frac{1}{1 - pt} = \prod_{i=1}^{\infty} \frac{1}{1 - t^{d_i}} = \prod_{k=1}^{\infty} \left(\frac{1}{1 - t^k} \right)^{M_k}.$$

Прологарифмировав, получаем

$$\ln \frac{1}{1 - pt} = \sum_{k=1}^{\infty} M_k \ln \frac{1}{1 - t^k}.$$

Ряд Тейлора для функции $\ln((1 - x)^{-1})$ имеет вид $\sum_{j=1}^{\infty} \frac{x^j}{j}$, отсюда

$$\sum_{m=1}^{\infty}\frac{(pt)^m}{m}=\sum_{k=1}^{\infty}M_k\sum_{j=1}^{\infty}\frac{t^{kj}}{j}=\sum_{k,j=1}^{\infty}\frac{M_k}{j}\cdot t^{kj}=\sum_{n=1}^{\infty}\left(\sum_{k,j:\,k\cdot j=n}\frac{M_k}{j}\right)t^n=\sum_{n=1}^{\infty}\left(\sum_{k:\,k|n}\frac{M_k}{n/k}\right)t^n.$$

Для каждого n коэффициенты при t^n должны совпадать в левой и правой частях равенства. Поэтому

$$\frac{p^n}{n}=\sum_{k|n}\frac{M_k}{n/k}.$$

Окончательно получаем

$$p^n=\sum_{k|n}kM_k.$$

Заметим, что полученное соотношение с точностью до переименования величин совпадает с тем, что возникало в задаче подсчёта числа циклических слов фиксированной длины в конечном алфавите. Применяя «теоретико-числовую» теорему об обращении, получаем следующую теорему.

Теорема. Число нормногочленов степени n, неприводимых над $\mathbb{Z}_p$, совпадает с числом циклических слов в p-символьном алфавите, имеющих длину и период n, и равно

$$\frac{1}{n}\sum_{k|n}p^k\hat{\mu}(n/k)\,,$$

где $\hat{\mu}$ — функция Мёбиуса.

Очевидно, для любого $n\geq 2$ найдётся хотя бы одно циклическое слово длины и периода n, поэтому справедливо следующее утверждение.

Утверждение. При каждом p и при каждом $n\geq 2$ существует хотя бы один неприводимый над $\mathbb{Z}_p$ нормногочлен степени n.

Аналогично тому, как мы получали асимптотику числа циклических слов, можно доказать следующее утверждение.

Утверждение. Число нормногочленов степени n, неприводимых над $\mathbb{Z}_p$, при $n\to\infty$ асимптотически равно p^n/n.

Резюме.

- Многочлены похожи на числа: их можно делить с остатком, можно определить простые многочлены и доказать аналоги теорем из арифметики.
- Для любого простого p и любого $\alpha\in\mathbb{N}$ существует конечное поле порядка p^α. При $\alpha=1$ это просто $\mathbb{Z}_p$, а при $\alpha>1$ это множество многочленов из $\mathbb{Z}_p[x]$ степени $\leq\alpha-1$, сложение и умножение которых проводится по модулю некоторого простого многочлена Q, где $\deg Q=\alpha$.

Факты о конечных полях (без доказательства).

- Любое конечное поле изоморфно полю многочленов $\mathbb{Z}_p[x]/Q$ для некоторого простого числа p и многочлена Q, неприводимого над $\mathbb{Z}_p$.
- В любом конечном поле все ненулевые элементы образуют *циклическую* группу относительно умножения.

4. Алгебраические методы в дискретной математике

4.1. Теорема Алона и её применения

В этом разделе мы докажем теорему о многочленах, которая не имеет, на первый взгляд, никакого отношения к комбинаторике. Однако некоторые весьма трудные задачи этой теореме оказываются подвластны, и ниже мы это покажем.

4.1.1. Теорема Алона

Утверждение. Пусть $P \in \mathbb{F}[x_1, \dots, x_m]$ и $\tilde{P} \in \mathbb{F}[x_i]$ — произвольные ненулевые многочлены. Тогда существуют $Q, R \in \mathbb{F}[x_1, \dots, x_m]$, такие, что $P = \tilde{P} \cdot Q + R$, и $\deg_{x_i} R < \deg_{x_i} \tilde{P}$.

Доказательство. Во всех мономах P, куда x_i входит в степени больше $\deg_{x_i} R$, заменяем эту степень, выразив её через $\tilde{P}$. По сути, это «деление столбиком», в котором мы рассматриваем P как многочлен от x_i с коэффициентами из $\mathbb{F}[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m]$.

Пример. Пусть $P \coloneqq x_1^5 x_2^8 x_4 + x_1^2 + x_1 x_3$ и $\tilde{P} \coloneqq x_1^2 + 3x_1$. Тогда

$$\begin{aligned} P &= x_1^3 x_2^8 x_4 \cdot \left(\tilde{P} - 3x_1\right) + \left(\tilde{P} - 3x_1\right) + x_1 x_3 = \left(x_1^3 x_2^8 x_4 + 1\right) \cdot \tilde{P} - 3x_1^4 x_2^8 x_4 - 3x_1 + x_1 x_3 \\ &= \left(x_1^3 x_2^8 x_4 + 1\right) \cdot \tilde{P} - 3x_1^2 x_2^8 x_4 \left(\tilde{P} - 3x_1\right) - 3x_1 + x_1 x_3 \\ &= \left(x_1^3 x_2^8 x_4 - 3x_1^2 x_2^8 x_4 + 1\right) \cdot \tilde{P} + 9x_1^3 x_2^8 x_4 - 3x_1 + x_1 x_3 (\dots) \cdot \tilde{P} + 9x_1 x_2^8 x_4 \left(\tilde{P} - 3x_1\right) \\ &- 3x_1 + x_1 x_3 = (\dots) \cdot \tilde{P} - 27x_1^2 x_2^8 x_4 - 3x_1 + x_1 x_3 \\ &= (\dots) \cdot \tilde{P} - 27x_2^8 x_4 \left(\tilde{P} - 3x_1\right) - 3x_1 + x_1 x_3 = \underbrace{(\dots)}_{Q} \cdot \tilde{P} + \underbrace{81 x_1 x_2^8 x_4 - 3x_1 + x_1 x_3}_{R}. \end{aligned}$$

Теорема. Пусть $P \in \mathbb{F}[x_1, \dots, x_m]$ — произвольный полином, и пусть $x_1^{t_1} \cdot \dots \cdot x_m^{t_m}$ — моном старшей степени, то есть $\sum_i t_i = \deg P$. Пусть $S_1, \dots, S_m \subseteq \mathbb{F}$ — произвольные множества, такие, что $|S_i| \geq t_i + 1$ для всех i. Тогда найдутся такие $s_1 \in S_1, \dots, s_m \in S_m$, что $P(s_1, \dots, s_m) \neq 0$.

Доказательство. Индукция по $\deg P$. Если $\deg P = 1$, то P — линейная форма:

$$P(x_1, \dots, x_m) = c_0 + \sum_i c_i x_i.$$

Если, например, $c_1 \neq 0$, то $|S_1| \geq 2$ и, как бы ни были фиксированы $x_2 \leftarrow s_2, \dots, x_m \leftarrow s_m$, уравнение $P(x_1, s_2, \dots, s_m) = 0$ имеет не более одного корня. Значит, найдётся $s_1 \in S_1$, для которого $P(s_1, s_2, \dots, s_m) \neq 0$.

Пусть $\deg P > 1$, и для многочленов меньшей степени утверждение теоремы выполнено. Б.о.о. будем считать, что $t_1 > 0$. Зафиксируем произвольное $s \in S_1$ и поделим с остатком P на $(x_1 - s)$:

$$P = (x_1 - s) \cdot Q + R,$$

где $Q \not\equiv 0$ и $\deg_{x_1} R < \deg_{x_1} (x_1 - s) = 1$, то есть R *не зависит от* x_1.

Если найдётся набор $s_2 \in S_2, \dots, s_m \in S_m$, такой, что $R(s_2, \dots, s_m) \neq 0$, то $P(s, s_2, \dots, s_m) \neq 0$, что и требовалось.

Остаётся разобрать случай, когда

$$\forall s_2 \in S_2, \dots, \forall s_m \in S_m \quad R(s_2, \dots, s_m) = 0.$$

Т.к. в P один из мономов степени $\deg P$ имеет вид $x_1^{t_1} \cdot \dots \cdot x_m^{t_m}$, то в Q один из мономов степени $\deg Q$ имеет вид $x_1^{t_1 - 1} \cdot \dots \cdot x_m^{t_m}$. По предположению индукции, найдутся такие $s_1 \in S_1 \setminus \{s\}$, $s_2 \in S_2, \dots, s_m \in S_m$, для которых $Q(s_1, \dots, s_m) \neq 0$. Для таких $s_1, \dots, s_m$ получаем $P(s_1, \dots, s_m) = (s_1 - s) \cdot Q(s_1, \dots, s_m) \neq 0$. Все случаи разобраны, и теорема доказана.

4.1.2. Теорема Коши—Давенпорта

Пусть $A, B \subseteq \mathbb{G}$, где $\mathbb{G}$ — абелева группа. Обозначим

$$A + B \coloneqq \{a + b \mid a \in A, b \in B\}.$$

Как можно оценить $|A + B|$, если известны $|A|$ и $|B|$? Пример простой оценки сверху:

$$|A + B| \leq \min\{|G|, |A| \cdot |B|\}.$$

Нижняя оценка даётся следующей теоремой.

Теорема (Коши, Давенпорт). Если $A, B \subseteq \mathbb{Z}_p$, где p — простое число, то

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

Доказательство. Утверждение теоремы тривиально при $|A| = 1$ или $|B| = 1$. Далее везде будем предполагать, что $|A|, |B| \geq 2$.

Сначала рассмотрим лёгкий случай $|A| + |B| > p$. Для любого $c \in \mathbb{Z}_p$ имеем

$$|A| + |c - B| = |A| + |B| > p,$$

а значит $A \cap (c - B) \neq \emptyset$, и найдутся $a \in A$ и $b \in B$, такие, что $a = c - b$. Отсюда $c \in A + B$. Т.к. c брался произвольным, получаем $A + B = \mathbb{Z}_p$.

Пусть теперь $|A| + |B| \leq p$. Допустим, что $|A + B| < |A| + |B| - 1$, и придём к противоречию. Рассмотрим многочлен

$$P(x, y) \coloneqq \prod_{c \in A+B} (x + y - c) \in \mathbb{Z}_p[x, y].$$

Обозначим $n \coloneqq |A + B| \leq p - 2$. Раскрыв скобки в определении P, видим, что

$$\operatorname{coef}_{x^{|A|-1}y^{n-|A|+1}} P \quad = \quad \frac{n!}{(|A|-1)!(n-|A|+1)!} \bmod p \quad \neq 0,$$

то есть моном $x^{|A|-1}y^{n-|A|+1}$ входит в многочлен с ненулевым коэффициентом, причём степень монома равна степени многочлена. По теореме Алона, должны найтись $a \in A$ и $b \in B$, такие, что $P(a, b) \neq 0$. Но такого не может быть по построению P.

4.1.3. Покрытие вершин гиперкуба гиперплоскостями

Нетрудно видеть, что все вершины гиперкуба в пространстве любой размерности можно покрыть, проведя всего две гиперплоскости. А сколько плоскостей нужно, чтобы покрыть все, *кроме одной*, вершины гиперкуба? Оказывается, в этом случае требуемое число гиперплоскостей намного больше.

Теорема (Алон, Фюреди). Наименьшее число гиперплоскостей, достаточное, чтобы покрыть все, кроме одной, вершины гиперкуба в $\mathbb{R}^n$, равно n.

Доказательство. Б.о.о. будем считать, что у нас гиперкуб $\{0,1\}^n$, и что вершина, которую мы не покрываем $(0,0,\dots,0)$. Сразу отметим, что n гиперплоскостей достаточно — например, такие:

$$\begin{aligned} x_1 - 1 &= 0 \\ x_2 - 1 &= 0 \\ &\vdots \\ x_n - 1 &= 0 \end{aligned}$$

Сложная часть — доказать, что меньшим числом гиперплоскостей не обойтись. Докажем это от противного. Допустим, мы обошлись m гиперплоскостями, $m < n$. Пусть их уравнения такие:

$$\begin{aligned} \langle \boldsymbol{a}_1, \boldsymbol{x} \rangle - b_1 &= 0 \\ &\vdots \\ \langle \boldsymbol{a}_m, \boldsymbol{x} \rangle - b_m &= 0 \end{aligned}$$

Отметим, что $b_1, \dots, b_m \neq 0$, т.к. ни одна из гиперплоскостей не должна покрывать точку $(0,0,\dots,0)$.

Рассмотрим многочлен

$$P(x_1, \dots, x_n) \coloneqq \prod_{j=1}^{m}\left(b_j - \langle \boldsymbol{a}_j, \boldsymbol{x}\rangle\right) - \left(\prod_{j=1}^{m} b_j\right)\cdot\left(\prod_{i=1}^{n}(1-x_i)\right).$$

Заметим, что этот многочлен обнуляется на всех вершинах гиперкуба:

- во-первых,

$$P(0,\dots,0) = \prod_{j=1}^{m}(b_j) - \left(\prod_{j=1}^{m} b_j\right)\cdot\left(\prod_{i=1}^{n} 1\right) = 0,$$

- во-вторых, для любой точки $(\alpha_1, \dots, \alpha_n) \in \{0,1\}^n \setminus \{(0,\dots,0)\}$

$$P(\alpha_1, \dots, \alpha_n) = \prod_{j=1}^{m}(0) - \left(\prod_{j=1}^{m} b_j\right)\cdot 0 = 0.$$

С другой стороны, поскольку $\deg P = n$ и

$$\operatorname{coef}_{x_1\cdot x_2\cdot\dots\cdot x_n} P = (-1)^{n+1}\prod_{j=1}^{m} b_j \neq 0,$$

то, по теореме Алона, должны найтись $\alpha_1 \in \{0,1\}, \dots, \alpha_n \in \{0,1\}$, для которых $P(\alpha_1, \dots, \alpha_n) \neq 0$ — противоречие.

4.1.4. Регулярные подграфы в регулярных графах

Общая постановка многих задач в теории графов выглядит так: в данном графе с известными свойствами выделить подграф с требуемыми свойствами (максимальную клику, компоненту связности с максимальным числом вершин и т.д.). Задача из этой же серии: во всяком ли k-регулярном графе существует $(k-1)$-регулярный подграф? Ответ на поставленный вопрос положительный при $k \leq 4$ и отрицательный при $k \geq 5$. При $k \leq 3$ это простое упражнение, а при $k \geq 4$ — трудная теорема (доказана В.А. Ташкиновым в ’1984 г.).

Более общий вопрос: во всяком ли k-регулярном графе существует k'-регулярный подграф (где $k' < k$)? Известно, например, что для любых нечётных k и k' ответ на вопрос положительный. В этом разделе мы докажем теорему о существовании регулярных подграфов при ослаблении условия «строгой» регулярности до «почти регулярности» (то есть рассматриваются графы, у которых степени вершин близки, но необязательно равны).

Через $\Delta(G)$ будем обозначать максимальную степень вершин графа G. Через V и E обозначим соответственно множества вершин и рёбер графа, а через $d(v)$ — степень вершины v.

Теорема (Алон, Фридланд, Калаи). Пусть p — простое число. Пусть $G = (V, E)$ — мультиграф (без петель), удовлетворяющий условиям $\Delta(G) \leq 2p-1$ и $\frac{1}{|V|}\sum_{v\in V} d(v) > 2p-2$. Тогда в G есть p-регулярный подграф.

Отметим, что условия теоремы, если не считать простоту числа p, являются достаточно естественными: требуется, чтобы в графе максимальная степень вершин совсем незначительно превосходила среднюю степень. В этом случае степени вершин распределены «не слишком неравеномерно», и естественно ожидать наличие регулярного подграфа.

Доказательство теоремы. Каждому $e \in E$ сопоставим переменную x_e. Рассмотрим многочлен от переменных $\{x_e\}_{e\in E}$ с коэффициентами из $\mathbb{Z}_p$:

$$P \coloneqq \prod_{v\in V}\left(1-\left(\sum_{e\in E:\, e\ni v} x_e\right)^{p-1}\right)-\prod_{e\in E}(1-x_e).$$

Обозначим первое из произведений через Q. Из условия, $2\cdot|E| = \sum_{v\in V} d(v) > (2p-2)\cdot|V|$, отсюда $\deg Q \le (p-1)\cdot|V| < |E|$. Следовательно, $\deg P = |E|$. При этом, $\operatorname{coef}_{\prod_{e\in E} x_e} P = (-1)^{|E|+1} \neq 0$. Значит, по теореме Алона, найдётся набор значений $\boldsymbol{\alpha} = (\alpha_e)_{e\in E} \in \{0,1\}^{|E|}$, такой, что $P(\boldsymbol{\alpha}) \neq 0$. При этом для любого $v \in V$ имеем

$$\sum_{e\in E:\, e\ni v} \alpha_e \overset{p}{=} 0,$$

иначе, по малой теореме Ферма, получилось бы $\left(\sum_{e\in E:\, e\ni v}\alpha_e\right)^{p-1} \overset{p}{=} 1 \quad\Rightarrow\quad P(\boldsymbol{\alpha}) = 0$ (в $\mathbb{Z}_p$).

Кроме того, видно, что $\boldsymbol{\alpha} \neq \mathbf{0}$. Взяв те рёбра G, для которых $\alpha_e = 1$, и все вершины G, получим непустой остовный подграф G'. В подграфе G' степень каждой вершины v равна $\sum_{e\in E:\, e\ni v}\alpha_e \overset{p}{=} 0$, а значит, эта степень равна нулю или p. Выбросив из G' вершины нулевой степени, получим искомый p-регулярный подграф.

4.2. Проблема Заранкевича

К. Заранкевич поставил в 1950-х годах следующий вопрос: каково максимальное число единиц в $m \times m$-матрице, не содержащей $a \times a$-подматриц, состоящих из единиц. Точные значения $Z_a(m)$ известны лишь в немногих частных случаях. Простейший нетривиальный случай, когда $a = 2$, мы и рассмотрим далее. Хотя по своей постановке задача дискретная (и может быть переформулирована в терминах двудольных графов), в её решении важную роль играет алгебраический подход.

4.2.1. Верхняя оценка $Z_2(m)$

Теорема. Имеет место неравенство

$$Z_2(m) \le m\cdot\left(\tfrac{1}{2}+\sqrt{m-\tfrac{3}{4}}\right).$$

Доказательство. 2×2-подматрицы из единиц назовём *плохими*. Пусть X — $m\times m$-матрица без плохих подматриц, содержащая ровно $Z_2(m)$ единиц. Строки X — это двоичные вектора длины m, обозначим их $X_1, \dots, X_m$. Оценим скалярный квадрат вектора $X_1+\dots+X_m$. С одной стороны,

$$\begin{aligned}\langle X_1+\dots+X_m, X_1+\dots+X_m\rangle &= \sum_i \langle X_i, X_i\rangle + \sum_{i\neq j}\langle X_i, X_j\rangle = Z_2(m) + \sum_{i\neq j}\langle X_i, X_j\rangle \le Z_2(m) + \sum_{i\neq j} 1\\ &= Z_2(m) + m(m-1).\end{aligned}$$

С другой стороны, обозначив координаты вектора $(X_1+\dots+X_m)$ через $s_1, \dots, s_m$, получаем

$$\langle X_1+\dots+X_m, X_1+\dots+X_m\rangle = \sum_{i=1}^{m} s_i^2\,.$$

Заметим, что s_i равно числу единиц в i-м столбце матрицы X, поэтому $\sum_{i=1}^m s_i = Z_2(m)$. Отсюда, по неравенству Коши—Буняковского,

$$\sum_{i=1}^{m} s_i^2 \ge \sum_{i=1}^{m}\left(\frac{Z_2(m)}{m}\right)^2 = \frac{\left(Z_2(m)\right)^2}{m}.$$

В итоге получаем

$$\frac{\left(Z_2(m)\right)^2}{m} \le Z_2(m) + m(m-1).$$

Отсюда

$$\big(Z_2(m)\big)^2 - m \cdot Z_2(m) - m^2(m-1) \le 0.$$

Решив это неравенство относительно $Z_2(m)$, получим требуемое. *Теорема доказана.*

4.2.2. Нижняя оценка $Z_2(m)$

Пусть p — простое число. Рассмотрим множество $T \coloneqq \{(x,y,z) \mid x,y,z \in \mathbb{Z}_p\} \setminus \{(0,0,0)\}$. Тройки $(x,y,z), (x',y',z') \in T^3$ назовём *эквивалентными*, если $(x',y',z') = (\lambda x, \lambda y, \lambda z)$ для некоторого ненулевого λ. Пусть $T_1, \dots, T_m$ — все различные классы эквивалентности множества T. Так как $|T| = p^3 - 1$, и для каждой тройки $(x,y,z) \in T$ есть ровно $(p-1)$ эквивалентных ей троек, то

$$m = \frac{p^3-1}{p-1} = p^2 + p + 1.$$

Заметим, что если найдутся ортогональные тройки $(x,y,z) \in T_i$ и $(u,v,w) \in T_j$, такие, что

$$ux + vy + wz = 0 \pmod p,$$

то и любая пара троек из T_i и T_j будет ортогональна. В этом случае скажем, что T_i и T_j *ортогональны*, и обозначим это так: $T_i \perp T_j$.

Пусть $i \ne j$ и пусть (a_i, b_i, c_i) и (a_j, b_j, c_j) — произвольные тройки из T_i и T_j соответственно. Найдём количество множеств T_k, таких, что одновременно $T_k \perp T_i$ и $T_k \perp T_j$. Для этого должна найтись тройка $(x,y,z) \in T_k$, такая, что

$$\begin{cases} a_i x + b_i y + c_i z = 0 \\ a_j x + b_j y + c_j z = 0 \end{cases}$$

В силу того, что тройки коэффициентов уравнений принадлежат разным классам T_i и T_j (а значит, линейно независимы), матрица записанной выше системы имеет ранг 2. Поэтому множество решений системы суть подпространство размерности 1 трёхмерного координатного пространства $\mathbb{Z}_p^3$. Из этого следует, что T_k единственное.

Рассмотрим теперь матрицу $X = \{x_{i,k}\}_{i,k=1}^{m}$, в которой

$$x_{i,k} \coloneqq \mathbb{1}_{T_i \perp T_k}.$$

Заметим, что в этой матрице нет плохих подматриц, иначе оказалось бы, что нашлись $i \ne j$ и $k \ne l$, для которых T_k и T_l ортогональны одновременно T_i и T_j.

Осталось найти число единиц в матрице X. Пусть T_i фиксировано, и пусть $(a,b,c) \in T_i$. Посчитаем число троек (x,y,z), ортогональных тройке (a,b,c), то есть таких, что $ax + by + cz = 0$. Множество решений этого уравнения образует двумерное подпространство в $\mathbb{Z}_p^3$, и, стало быть, имеет мощность p^2. Значит, число ненулевых решений уравнения равно $p^2 - 1$. Тогда

$$\#\{k \mid T_k \perp T_i\} = \frac{p^2-1}{p-1} = p + 1.$$

То есть в каждой строке матрицы X ровно $(p+1)$ единиц, и всего единиц в матрице

$$(p+1)(p^2+p+1).$$

Мы построили матрицу X размерности (p^2+p+1), в которой $(p+1)(p^2+p+1)$ единиц и которая не содержит плохих подматриц, а значит

$$Z_2(p^2+p+1) \ge (p+1)(p^2+p+1).$$

Посмотрим, как это соотносится с полученной ранее верхней оценкой $Z_2(m) \le m \cdot \left(\frac{1}{2} + \sqrt{m - \frac{3}{4}}\right)$. Правая часть указанной оценки при $m = p^2+p+1$ равна

$$(p^2+p+1) \cdot \left(\frac{1}{2} + \sqrt{(p^2+p+1) - \frac{3}{4}}\right) = (p^2+p+1)\left(\frac{1}{2} + \frac{2p+1}{2}\right) = (p^2+p+1)(p+1).$$

То есть построенная матрица X оптимальна: при той же размерности больше единиц мы в ней расставить не смогли бы. Таким образом, справедлива следующая теорема.

Теорема. Для любого простого числа p имеем

$$Z_2(p^2+p+1) = (p+1)(p^2+p+1).$$

Следствие. При $m \to \infty$ имеет место асимптотика

$$Z_2(m) \sim m^{3/2}.$$

Доказательство. Верхняя оценка следует из соотношений

$$Z_2(m) \leq m\left(\frac{1}{2}+\sqrt{m-\frac{3}{4}}\right) \sim m^{3/2}.$$

Осталось доказать нижнюю оценку. Согласно теореме Бейкера—Хармана—Пинца, найдётся простое число

$$p \in \left[\sqrt{m}-1-\left(\sqrt{m}-1\right)^{21/40}, \sqrt{m}-1\right].$$

Для такого p, согласно теореме, найдётся матрица X', размер которой $p^2+p+1 < m$, без плохих подматриц, содержащая

$$(p^2+p+1)(p+1) > p^3 \gtrsim m^{3/2}$$

единиц. Остаётся дополнить X' нулями до матрицы размера в точности $m \times m$.

Замечание. На самом деле, все построения, с которыми мы работали при доказательстве нижней оценки чисел Заранкевича, могут быть проведены не с $\mathbb{Z}_p$, а с любым конечным полем. Поэтому равенство $Z_2(m) = m\left(\frac{1}{2}+\sqrt{m-\frac{3}{4}}\right)$ выполнено для всех m, представимых в виде q^2+q+1, где q — натуральная степень простого числа.