Прикладная алгебра

Лекции для III потока, 5-й семестр 2013/2014 уч. года

Гуров Сергей Исаевич

Факультет Вычислительной математики и кибернетики,
МГУ имени М.В. Ломоносова
Кафедра Математических методов прогнозирования
комн. 530, 682
e-mail: *sgur@cs.msu.ru*

Литература


Воронин В.П. Дополнительные главы дискретной математики. — М.: ф-т ВМК МГУ, 2002. http://padabum.com/d.php?id=10281


Гуров С.И. Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры. — М.: Либроком, 2013.


Журавлёв Ю.И., Флёров Ю.А., Вялый М.Н. Дискретный анализ. Основы высшей алгебры. — М.: МЗ Пресс, 2007.


Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. — М.: Мир, 1988.


Нефедов В.Н., Осипова В.А. Курс дискретной математики. М.: Изд-во МАИ, 1992.


Ромащенко А.Е., Румянцев А.Ю., Шень А. Заметки по теории кодирования. — М.: МЦНМО, 2011.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Поле $GF(p)$

- $\mathbb{Z}$ — евклидово кольцо целых чисел (без делителей нуля + деление с остатком).
- p — простое число.
- $(p) = \{np \mid n \in \mathbb{Z}\} = p\mathbb{Z} = \{0, \pm p, \pm 2p, \ldots\}$ — *идеал*
- $\mathbb{Z}/p\mathbb{Z}$ — кольцо вычетов по модулю этого идеала: $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$ — классы остатков от деления на p:

$$\begin{aligned} \overline{0} &= 0 + p\mathbb{Z}\,, \\ \overline{1} &= 1 + p\mathbb{Z}\,, \\ &\ldots \\ \overline{p-1} &= (p-1) + p\mathbb{Z}\,. \end{aligned}$$

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{p-1}.$$

Поскольку p — простое, то $\mathbb{Z}/p\mathbb{Z}$ — поле.
Это простейшее *поле Галуа*, обозначение — $\mathbb{F}_p$ или $GF(p)$.
Все операции в поле $\mathbb{F}_p$ — по $\mod p$.

$\mathbb{F}_3$ и $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{F}_3$ и $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}/4\mathbb{Z}$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем их:
$1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots$

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем их: $1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots$. В конечном поле всегда найдётся первое k такое, что $\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 1$. Тогда

$$k = \text{порядок аддитивной группы поля } \Bbbk =$$

$$= \textit{характеристика поля } \Bbbk \stackrel{\text{def}}{=} \operatorname{char} \Bbbk$$

Характеристика поля

Пусть $\Bbbk$ — произвольное поле, 1 — единица $\Bbbk$. Складываем их: $1 = 1\,, \quad 2 = 1 + 1\,, \quad \ldots$. В конечном поле всегда найдётся первое k такое, что $\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 1$. Тогда

$$k = \text{порядок аддитивной группы поля } \Bbbk =$$

$$= \textit{характеристика поля } \Bbbk \stackrel{\text{def}}{=} \operatorname{char} \Bbbk$$

Значение k порождает идеал $\overline{k} = (\operatorname{char} \Bbbk)$ в $\mathbb{Z}$.

$\mathbb{Z}/(\operatorname{char} \Bbbk)$ — поле iff k — простое число, *подполе* $\Bbbk$.

Если все суммы $\underbrace{1 + \ldots + 1}_{k}$ различны, то $\operatorname{char} \Bbbk = 0$.

Примеры: $\mathbb{Q}$, $\mathbb{R}$.

Может ли бесконечное поле иметь положительную характеристику?

Может ли бесконечное поле иметь положительную характеристику?

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — множество многочленов $P(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_0, \ldots, a_n \in \Bbbk$ от x с коэффициентами из $\Bbbk$.

Может ли бесконечное поле иметь положительную характеристику?

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — множество многочленов $P(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_0, \ldots, a_n \in \Bbbk$ от x с коэффициентами из $\Bbbk$.
2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$.

Может ли бесконечное поле иметь положительную характеристику?

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — множество многочленов $P(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_0, \ldots, a_n \in \Bbbk$ от x с коэффициентами из $\Bbbk$.
2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$. В нём

   Элементы — "дроби" P/Q (если $Q \neq 0$), где $P, Q \in \Bbbk[x]$.

   Умножение — $P/Q \cdot U/V = (PU)/(QV)$.

   Эквивалентность — $P_1/Q_1 = P_2/Q_2$, если $P_1 Q_2 = P_2 Q_1$.

   Сложение — дроби можно приводить к общему знаменателю и складывать:
   $$P/Q + U/v = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV).$$

   Включение — Поскольку $\Bbbk[x] \subset \Bbbk(x)$, то каждый многочлен P отождествляется с $P/1$.

Может ли бесконечное поле иметь положительную характеристику?

$\Bbbk$ — произвольное (конечное или бесконечное) поле. Построим:

1. $\Bbbk[x]$ — множество многочленов $P(x) = a_0 + a_1 x + \ldots + a_n x^n$, $a_0, \ldots, a_n \in \Bbbk$ от x с коэффициентами из $\Bbbk$.
2. $\Bbbk(x)$ — поле рациональных функций над $\Bbbk$. В нём

   Элементы — "дроби" P/Q (если $Q \neq 0$), где $P, Q \in \Bbbk[x]$.

   Умножение — $P/Q \cdot U/V = (PU)/(QV)$.

   Эквивалентность — $P_1/Q_1 = P_2/Q_2$, если $P_1 Q_2 = P_2 Q_1$.

   Сложение — дроби можно приводить к общему знаменателю и складывать:
   $$P/Q + U/v = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV).$$

   Включение — Поскольку $\Bbbk[x] \subset \Bbbk(x)$, то каждый многочлен P отождествляется с $P/1$.

Если в качестве $\Bbbk$ взять конечное поле $\mathbb{F}_p$, то $\mathbb{F}_p(x)$ — бесконечное поле с характеристикой p.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Сильное упрощение вычислений в поле положительной характеристики

Лемма

В поле характеристики $p > 0$ выполнено тождество

$$(a + b)^p = a^p + b^p.$$

Сильное упрощение вычислений в поле положительной характеристики

Лемма

В поле характеристики $p > 0$ выполнено тождество

$$(a+b)^p = a^p + b^p.$$

Доказательство

В любом коммутативном кольце верна формула для бинома

$$(a+b)^p = a^p + C_p^1 a^{p-1} b + \ldots + C_p^{p-1} a b^{p-1} + b^p.$$

Но при $i = 1, \ldots, p-1$ числитель $C_p^i = \frac{p!}{i!(p-i)!}$ делятся на p, а знаменатель — нет, $\therefore C_p^i \equiv_p 0$.

Сильное упрощение вычислений в поле положительной характеристики

Лемма

В поле характеристики $p > 0$ выполнено тождество

$$(a + b)^p = a^p + b^p.$$

Доказательство

В любом коммутативном кольце верна формула для бинома

$$(a + b)^p = a^p + C_p^1 a^{p-1} b + \ldots + C_p^{p-1} a b^{p-1} + b^p.$$

Но при $i = 1, \ldots, p - 1$ числитель $C_p^i = \frac{p!}{i!(p-i)!}$ делятся на p, а знаменатель — нет, $\therefore C_p^i \equiv_p 0$.

Следствие

В поле характеристики $p > 0$ справедливо $(a + b)^{p^n} = a^{p^n} + b^{p^n}$.

Мультпликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\} = \{1, \ldots, p-1\}$ — *мультпликативная группа поля* $\mathbb{F}_p$.

Мультпликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\} = \{1, \ldots, p-1\}$ — *мультпликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$ *по умножению.*

Мультпликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\} = \{1, \ldots, p-1\}$ — *мультпликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$ *по умножению.*

$\mathbb{F}_p^*$ содержит *примитивный элемент* α —

- *порядок* α равен $p-1$, т.е. $\alpha^{p-1} = 1$ и $\alpha^i \neq 1$ для $0 < i < p-1$.
- любой ненулевой элемент $\beta \in \mathbb{F}_p^*$ является некоторой степенью примитивного элемента: $\beta = \alpha^i,\ i = 0, 1, \ldots, q-1$.

Мультпликативная группа и примитивный элемент поля $\mathbb{F}_p$

$\mathbb{F}_p^* \stackrel{\text{def}}{=} \mathbb{F}_p \setminus \{0\} = \{1, \ldots, p-1\}$ — *мультпликативная группа поля* $\mathbb{F}_p$.

Утверждение

$\mathbb{F}_p^*$ — *циклическая группа порядка* $p-1$ *по умножению.*

$\mathbb{F}_p^*$ содержит *примитивный элемент* α —

- *порядок* α равен $p-1$, т.е. $\alpha^{p-1} = 1$ и $\alpha^i \neq 1$ для $0 < i < p-1$.
- любой ненулевой элемент $\beta \in \mathbb{F}_p^*$ является некоторой степенью примитивного элемента: $\beta = \alpha^i,\ i = 0, 1, \ldots, q-1$.

Утверждение

Группа $\mathbb{F}_p^*$ *имеет* $\varphi(p-1)$ *примитивных элементов.*

Функция Эйлера

$\varphi(n)$ — *функция Эйлера* т.е. количество чисел ряда из интервала $[1, \ldots, n-1]$, взаимно простых с n:

$$\varphi(1) = 1 \text{ (по определению)}, \varphi(2) = 1, \varphi(3) = \varphi(4) = 2,$$
$$\varphi(5) = 4, \varphi(6) = |\{1, 5\}| = 2, \ldots$$

Функция Эйлера

$\varphi(n)$ — *функция Эйлера* т.е. количество чисел ряда из интервала $[1, \ldots, n-1]$, взаимно простых с n:

$$\varphi(1) = 1 \text{ (по определению)}, \varphi(2) = 1, \varphi(3) = \varphi(4) = 2,$$
$$\varphi(5) = 4, \varphi(6) = |\{1, 5\}| = 2, \ldots$$

Свойства:

- $\varphi(n) \geqslant n - 1$ и $\varphi(p) = p - 1$, если p — простое;
- $\varphi(n^m) = n^{m-1}\varphi(n-1)$, т.е. $\varphi(p^m) = p^{m-1}(p-1)$, если p — простое;
- если m и n взаимно просты, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ (т.е. $\varphi(n)$ — *мультпликативная функция*);
- в общем случае $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}$, где $d = (m, n)$.

Пример

$$\varphi(15) =$$

Функция Эйлера

$\varphi(n)$ — *функция Эйлера* т.е. количество чисел ряда из интервала $[1, \ldots, n-1]$, взаимно простых с n:

$$\varphi(1) = 1 \text{ (по определению)}, \varphi(2) = 1, \varphi(3) = \varphi(4) = 2,$$
$$\varphi(5) = 4, \varphi(6) = |\{1, 5\}| = 2, \ldots$$

Свойства:

- $\varphi(n) \geqslant n - 1$ и $\varphi(p) = p - 1$, если p — простое;
- $\varphi(n^m) = n^{m-1}\varphi(n-1)$, т.е. $\varphi(p^m) = p^{m-1}(p-1)$, если p — простое;
- если m и n взаимно просты, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ (т.е. $\varphi(n)$ — *мультпликативная функция*);
- в общем случае $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}$, где $d = (m, n)$.

Пример

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = (3-1)(5-1) = 8.$$

Как найти примитивные элементы поля $\mathbb{F}_p$?

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $(p-1)$ —

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $(p-1)$ —

известно — элемент $\alpha \in \mathbb{F}_p$ будет примитивным iff $\alpha^{\frac{p-1}{q}} \not\equiv_p 1$ для каждого простого $q \mid (p-1)$.

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $(p-1)$ —

известно — элемент $\alpha \in \mathbb{F}_p$ будет примитивным iff $\alpha^{\frac{p-1}{q}} \not\equiv_p 1$ для каждого простого $q \mid (p-1)$.

неизвестно — эффективного алгоритма нахождения примитивного элемента не найдено (используют вероятностные алгоритмы).

Как найти примитивные элементы поля $\mathbb{F}_p$?

Если примарное разложение $(p-1)$ —

известно — элемент $\alpha \in \mathbb{F}_p$ будет примитивным iff $\alpha^{\frac{p-1}{q}} \not\equiv_p 1$ для каждого простого $q \mid (p-1)$.

неизвестно — эффективного алгоритма нахождения примитивного элемента не найдено (используют вероятностные алгоритмы).

Если найден один примитивный элемент, остальные находятся возведением его в степени, взаимно простые с числом $p-1$.

Неприводимые многочлены

Утверждение

Кольцо многочленов $\Bbbk[x]$ над полем $\Bbbk$ — евклидово.

Теорема

Каждый элемент евклидова кольца однозначно с точностью до перестановок разлагается в произведение простых элементов. и делителей единицы.

Простые (неразложимые) элементы $\Bbbk[x]$ — *неприводимые многочлены*.

Вопросы для полей $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ и $\mathbb{F}_p$:

1. какие многочлены над ними неприводимы?
2. как находить неприводимые многочлены?

Свойства корней многочленов

Утверждение

Остаток от деления многочлена f *на многочлен первой степени* $(x-a)$ *равен* $f(a)$. *В частности,* f *делится на* $(x-a)$ *iff* a *является корнем* f, *т. е.* $f(a)=0$.

Свойства корней многочленов

Утверждение

Остаток от деления многочлена f на многочлен первой степени $(x-a)$ равен $f(a)$. В частности, f делится на $(x-a)$ iff a является корнем f, т. е. $f(a)=0$.

Доказательство

Разделим f с остатком на $x-a$. Остаток должен иметь степень 0, т.е. $f(x)=q\cdot(x-a)+b$, откуда $f(a)=b$.

Основная теорема алгебры

Лемма

Многочлен степени n имеет не более n корней. Если два многочлена степени не выше n как функции различны, то их значения совпадают не более чем в n точках.

$\Rightarrow$ Указанные многочлены «сильно отличаются один от другого».

Это свойство многочленов лежит в основе многих их применений в комбинаторике и в теоретической информатике.

Теорема (основная теорема алгебры)

Всякий многочлен положительной степени над полем $\mathbb{C}$ имеет корень.

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$

Неприводимые многочлены:

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$

Неприводимые многочлены:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$

Неприводимые многочлены:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

в поле $\mathbb{R}$ —

1. многочлены 1-й степени,
2. многочлены 2-й степени с отрицательным дискриминантом;

Неприводимые многочлены над $\mathbb{C}$, $\mathbb{R}$ и $\mathbb{Q}$

Неприводимые многочлены:

в поле $\mathbb{C}$ — только многочлены 1-й степени;

в поле $\mathbb{R}$ —

1. многочлены 1-й степени,
2. многочлены 2-й степени с отрицательным дискриминантом;

в поле $\mathbb{Q}$ — существуют неприводимые многочлены произвольной степени (надо показать).
Вопрос о приводимости многочлена сводится к вопросу о разложении на множители многочлена с целыми коэффициентами.

Критерий Эйзенштейна — достаточное условие неприводимости многочленов над $\mathbb{Q}$

Теорема (критерий Эйзенштейна)

Если для многочлена $a_n x_n + \ldots + a_1 x + a_0$ с целыми коэффициентами существует такое простое p, что (1) $p \nmid a_n$, $p \mid a_i$ при $i = 0, 1, \ldots, n-1$ и (2) $p^2 \nmid a_0$, то этот многочлен неприводим.

Критерий Эйзенштейна — достаточное условие неприводимости многочленов над $\mathbb{Q}$

Теорема (критерий Эйзенштейна)

Если для многочлена $a_n x_n + \ldots + a_1 x + a_0$ с целыми коэффициентами существует такое простое p, что (1) $p \nmid a_n$, $p \mid a_i$ при $i = 0, 1, \ldots, n-1$ и (2) $p^2 \nmid a_0$, то этот многочлен неприводим.

Пример

$2x^4 - 6x^3 + 15x^2 + 21$ неприводим по критерию Эйзенштейна $(p = 3)$.

Критерий Эйзенштейна — достаточное условие неприводимости многочленов над $\mathbb{Q}$

Теорема (критерий Эйзенштейна)

Если для многочлена $a_n x_n + \ldots + a_1 x + a_0$ с целыми коэффициентами существует такое простое p, что (1) $p \nmid a_n$, $p \mid a_i$ при $i = 0, 1, \ldots, n-1$ и (2) $p^2 \nmid a_0$, то этот многочлен неприводим.

Пример

$2x^4 - 6x^3 + 15x^2 + 21$ неприводим по критерию Эйзенштейна ($p = 3$).

Пример (существование над $\mathbb{Q}$ неприводимых многочленов любой степени)

Многочлен $x^n - 2$ для всякого $n > 0$ неприводим над $\mathbb{Q}$ по критерию Эйзенштейна для $p = 2$.

Неприводимые многочлены над $\mathbb{F}_p$ — основной для нас случай

Пример ($p = 2$)

Дано: поле $\mathbb{F}_2 = \langle \{0, 1\}, +_{\mathrm{mod}\,2}, \cdot_{\mathrm{mod}\,2} \rangle$.

Требуется: найти все неприводимые многочлены степеней 2, 3, 4 над ним.

Неприводимые многочлены над $\mathbb{F}_p$ — основной для нас случай

Пример ($p = 2$)

Дано: поле $\mathbb{F}_2 = \langle \{0, 1\}, +_{\mathrm{mod}\,2}, \cdot_{\mathrm{mod}\,2} \rangle$.

Требуется: найти все неприводимые многочлены степеней 2, 3, 4 над ним.

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$.

Ищем неприводимый многочлен в виде $x^2 + ax + 1$.

Неприводимые многочлены над $\mathbb{F}_p$ — основной для нас случай

Пример ($p = 2$)

Дано: поле $\mathbb{F}_2 = \langle \{0, 1\}, +_{\bmod 2}, \cdot_{\bmod 2} \rangle$.
Требуется: найти все неприводимые многочлены степеней 2, 3, 4 над ним.

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$.
Ищем неприводимый многочлен в виде $x^2 + ax + 1$. Таких многочленов всего два: x и $x + 1$, а делимость на первый мы уже исключили, то осталось исключить делимость на $x + 1$. Делаем замену $y = x + 1$ $(x = y + 1)$: $(y + 1)^2 + a(y + 1) + 1 = y^2 + ay + (1 + a + 1)$, свободный член должен быть $\neq 0$.

Неприводимые многочлены над $\mathbb{F}_p$ — основной для нас случай

Пример ($p = 2$)

Дано: поле $\mathbb{F}_2 = \langle \{0, 1\}, +_{\bmod 2}, \cdot_{\bmod 2} \rangle$.
Требуется: найти все неприводимые многочлены степеней 2, 3, 4 над ним.

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$.
Ищем неприводимый многочлен в виде $x^2 + ax + 1$. Таких многочленов всего два: x и $x + 1$, а делимость на первый мы уже исключили, то осталось исключить делимость на $x + 1$. Делаем замену $y = x + 1$ $(x = y + 1)$: $(y + 1)^2 + a(y + 1) + 1 = y^2 + ay + (1 + a + 1)$, свободный член должен быть $\neq 0$.
$\therefore$ над $\mathbb{F}_2$ существует единственный неприводимый многочлен степени 2 — $x^2 + x + 1$.

Неприводимые многочлены над $\mathbb{F}_p$...

Третья степень: $x^3 + ax^2 + bx + 1$ (почему свободный член не равен нулю?)

Исключаем (как сделано ранее) делимость на $x + 1$ — получаем условие $a + b \neq 0$, т.е.

$$\left[\begin{array}{l} a = 0,\ b = 1\,, \\ a = 1,\ b = 0\,. \end{array}\right.$$

Неприводимые многочлены над $\mathbb{F}_p$...

Третья степень: $x^3 + ax^2 + bx + 1$ (почему свободный член не равен нулю?)

Исключаем (как сделано ранее) делимость на $x + 1$ — получаем условие $a + b \neq 0$, т.е.

$$\left[\begin{array}{l} a = 0,\ b = 1\,, \\ a = 1,\ b = 0\,. \end{array}\right.$$

$\therefore$ над $\mathbb{F}_2$ существует два неприводимых многочлена степени 3 —

$$x^3 + x^2 + 1\,,$$
$$x^3 + x + 1\,.$$

Неприводимые многочлены над $\mathbb{F}_p$...

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$

Исключение делимости на $x + 1$ приводит к условию $a + b + c = 1$, т.е. имеется 4 варианта, которые дают 3 решения:

a	b	c	многочлен	
0	0	1	$x^4 + x + 1$	
0	1	0	$x^4 + x^2 + 1$	— приводимый
1	0	0	$x^4 + x^3 + 1$	
1	1	1	$x^4 + x^3 + x^2 + x + 1$	

Откуда взялся ещё один приводимый многочлен?

Неприводимые многочлены над $\mathbb{F}_p$...

Четвёртая степень: $x^4 + ax^3 + bx^2 + cx + 1$

Исключение делимости на $x + 1$ приводит к условию $a + b + c = 1$, т.е. имеется 4 варианта, которые дают 3 решения:

a	b	c	многочлен	
0	0	1	$x^4 + x + 1$	
0	1	0	$x^4 + x^2 + 1$	— приводимый
1	0	0	$x^4 + x^3 + 1$	
1	1	1	$x^4 + x^3 + x^2 + x + 1$	

Откуда взялся ещё один приводимый многочлен?

В таблице указаны многочлены, у которых нет делителей степени 1. Но многочлен 4-й степени может разлагаться в произведение двух неприводимых многочленов 2-й степени:

$$x^4 + x^2 + 1 = (x^2 + x + 1)^2.$$

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \langle \{0, 1, 2\}, +_3, \cdot_3 \rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \langle \{0,1,2\}, +_3, \cdot_3 \rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$x \qquad 2x$$
$$x+1 \qquad 2x+1$$
$$x+2 \qquad 2x+2$$

Какие из них неприводимы?

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \langle \{0,1,2\}, +_3, \cdot_3 \rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$x \qquad 2x$$
$$x+1 \qquad 2x+1$$
$$x+2 \qquad 2x+2$$

Какие из них неприводимы? Все!

Неприводимые многочлены над $\mathbb{F}_3$

Поле $\mathbb{F}_3 = \langle \{0,1,2\}, +_3, \cdot_3 \rangle \Rightarrow$ кольцо многочленов $\mathbb{F}_3[x]$.
Многочлены порядка 1:

$$x \qquad 2x$$
$$x+1 \qquad 2x+1$$
$$x+2 \qquad 2x+2$$

Какие из них неприводимы? Все!

Неприводимые многочлены порядка 2 в $\mathbb{F}_3[x]$:

$$x^2+1 \qquad 2x^2+x+1$$
$$x^2+x+2 \qquad 2x^2+2x$$
$$x^2+2x+2$$
$$x^2+2$$

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

Доказательство

— отложим пока.

Вопрос

Как в $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Существование и нахождение неприводимых многочленов

Теорема (о существовании неприводимых многочленов)

Для любых натурального n и простого p над $\mathbb{F}_p$ существует неприводимый многочлен степени n.

Доказательство

— отложим пока.

Вопрос

Как в $\mathbb{F}_p[x]$ найти неприводимый многочлен?

Ответ: нет эффективных алгоритмов 

(из таблиц, пребором...)

Построение конечных полей

— с использованием неприводимых многочленов.

1. Выбираем простое p и фиксируем поле
$$\mathbb{F}_p = \langle \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}, +_{\mathrm{mod}\ p}, \cdot_{\mathrm{mod}\ p} \rangle.$$
2. Образуем кольцо $\mathbb{F}_p[x]$ многочленов над ним.
3. Выбираем натуральное n и неприводимый многочлен n-й степени $P(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x]$.
4. Идеал $(P(x))$ порождает фактормножество $\mathbb{F}_p[x]/(P(x))$, элементы которого суть совокупность $\{R(x)\}$ остатков от деления многочленов $f \in \mathbb{F}_p[x]$ на $P(x)$:
$$f(x) = Q(x) \cdot P(x) + R(x)\,.$$

Построение конечных полей

— с использованием неприводимых многочленов.

1. Выбираем простое p и фиксируем поле
$$\mathbb{F}_p = \langle \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}, +_{\mathrm{mod}\ p}, \cdot_{\mathrm{mod}\ p} \rangle.$$
2. Образуем кольцо $\mathbb{F}_p[x]$ многочленов над ним.
3. Выбираем натуральное n и неприводимый многочлен n-й степени $P(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{F}_p[x]$.
4. Идеал $(P(x))$ порождает фактормножество $\mathbb{F}_p[x]/(P(x))$, элементы которого суть совокупность $\{R(x)\}$ остатков от деления многочленов $f \in \mathbb{F}_p[x]$ на $P(x)$:
$$f(x) = Q(x) \cdot P(x) + R(x)\,.$$

Утверждение

Множество $\{R(x)\}$ является полем Галуа $GF(p^n)$.

Построение конечных полей...

Доказательство

1. *кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(P(x))$ — *максимальный* $\Rightarrow \{R(x)\}$ — *поле;*
2. $|\{R(x)\}|$ = *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $|\{R(x)\}| = p^n$.

Построение конечных полей...

Доказательство

1. *кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(P(x))$ — *максимальный* $\Rightarrow \{R(x)\}$ — *поле;*
2. $|\{R(x)\}|$ = *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $|\{R(x)\}| = p^n$.

Поле Галуа $\{R(x)\}$ называется
расширением n-й степени поля $\mathbb{F}_p$ и обозначается $\mathbb{F}_p^n$.

Вопрос

Почему в обозначении $\mathbb{F}_p^n$ *не используется многочлен* $P(x)$, *с помощью которого построено поле?*

Построение конечных полей...

Доказательство

1. *кольцо многочленов* $\mathbb{F}_p[x]$ *евклидово, идеал* $(P(x))$ — *максимальный* $\Rightarrow \{R(x)\}$ — *поле;*
2. $|\{R(x)\}| =$ *число многочленов над* $\mathbb{F}_p$ *степени не выше* $n-1$, *т.е.* $|\{R(x)\}| = p^n$.

Поле Галуа $\{R(x)\}$ называется
расширением n-й степени поля $\mathbb{F}_p$ и обозначается $\mathbb{F}_p^n$.

Вопрос

Почему в обозначении $\mathbb{F}_p^n$ *не используется многочлен* $P(x)$, *с помощью которого построено поле?*

Теорема

Любое конечное поле изоморфно какому-нибудь полю Галуа $\mathbb{F}_p^n$.

Пример: построение поля $\mathbb{F}_3^2$

Выберем неприводимый многочлен в $\mathbb{F}_3[x]$: x^2+1.
Искомое поле есть $\mathbb{F}_3^2 =$

$$= \mathbb{F}_3[x]/(x^2+1) = \{0,\ 1,\ 2,\ x,\ x+1,\ x+2,\ 2x,\ 2x+1,\ 2x+2\}.$$

Можно составить таблицу сложения и умножения в этом поле.
Например (применяем обычные правила с учётом $x^2 \equiv_3 2$):

$$\begin{aligned} (x+1)+(x+2) &= 2x, & (x)\cdot(2x) &= 1, \\ (2x+1)+(x) &= 1, & (2x+1)\cdot(x) &= x+1. \end{aligned}$$

Построение поля $\mathbb{F}_3^2$...

Заметим, что

$$\begin{aligned}(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\ (x+1)^2 &= 2x, & (x+1)^6 &= x,\\ (x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\ (x+1)^4 &= 2, & (x+1)^8 &= 1.\end{aligned}$$

Это значит, что $\alpha = x+1$ — примитивный элемент мультипликативной группы $\mathbb{F}_3^{2*}$.

Построение поля $\mathbb{F}_3^2$...

Заметим, что

$$\begin{aligned}(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\ (x+1)^2 &= 2x, & (x+1)^6 &= x,\\ (x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\ (x+1)^4 &= 2, & (x+1)^8 &= 1.\end{aligned}$$

Это значит, что $\alpha = x+1$ — примитивный элемент мультипликативной группы $\mathbb{F}_3^{2*}$.

Вопрос

Что будет, если при построении поля вместо x^2+1 взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен? Например, $2x^2+x+1$?

Построение поля $\mathbb{F}_3^2$...

Заметим, что

$$\begin{aligned}(x+1)^1 &= x+1, & (x+1)^5 &= 2x+2,\\ (x+1)^2 &= 2x, & (x+1)^6 &= x,\\ (x+1)^3 &= 2x+1, & (x+1)^7 &= x+2,\\ (x+1)^4 &= 2, & (x+1)^8 &= 1.\end{aligned}$$

Это значит, что $\alpha = x+1$ — примитивный элемент мультипликативной группы $\mathbb{F}_3^{2*}$.

Вопрос

Что будет, если при построении поля вместо x^2+1 взять другой неприводимый в $\mathbb{F}_3[x]$ многочлен? Например, $2x^2+x+1$?

Ответ: получится поле, изоморфное построенному.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Векторное пространство: определение

Определение

Абстрактным векторным пространством над полем $\Bbbk = \{\alpha, \ldots\}$ называется двухосновная алгебраическая система $\mathcal{V} = \langle V, \Bbbk; +, \cdot \rangle$, где

- $V = \{0, v, \ldots\}$ — произвольное множество,
- $+$ — бинарная операция сложения над V: $V \times V \xrightarrow{+} V$,
- $\cdot$ — бинарная операция умножения элемента («числа») из $\Bbbk$ на элемент («вектор») из V: $\Bbbk \times V \xrightarrow{\cdot} V$,

причём операции $+$ и $\cdot$ удовлетворяют следующим аксиомам:

L1: V — коммутативная группа по сложению, 0 — её нейтральный элемент.

L2: $\alpha \cdot (v_1 + v_2) = \alpha \cdot v_1 + \alpha \cdot v_2$, $(\alpha_1 + \alpha_2) \cdot v = \alpha_1 \cdot v + \alpha_2 \cdot v$, (дистрибутивность $\cdot$ относительно $+$),

L3: $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$ (композиция умножений на два элемента поля совпадает с умножением их произведение, «ассоциативность» операций умножения поля и $\cdot$),

L4: $1 \cdot v = v$ (унитальность).

Координатное пространство

Пример

Пусть $V = \Bbbk^n$ — множество последовательностей длины n, составленных из элементов поля $\Bbbk$. Сложение и умножение на число определяются покомпонентно.

Получившаяся структура — векторное пространство.

Его называют *n-мерным координатным пространством* над полем $\Bbbk$.

Лемма

Поле $\Bbbk$ *характеристики* $p > 0$ *есть векторное пространство над* $\mathbb{F}_p$.

Лемма

Поле $\Bbbk$ характеристики $p > 0$ есть векторное пространство над $\mathbb{F}_p$.

Доказательство

сложение — *наследуется операция сложения в поле $\Bbbk$;*

умножение — *подмножество*

$$F = \{0, 1, 1+1, \ldots, \underbrace{1+\ldots+1}_{p-1}\} \subseteq \Bbbk$$

есть подполе, изоморфное $\mathbb{F}_p$, что позволяет заменять при умножении «числа» из $\mathbb{F}_p$ на соответствующие элементы из F;

аксиомы векторного пространства — *выполняются в силу свойств арифметических операций в поле $\Bbbk$.*

Лемма

Поле $\Bbbk$ характеристики $p > 0$ есть векторное пространство над $\mathbb{F}_p$.

Доказательство

сложение — *наследуется операция сложения в поле $\Bbbk$;*

умножение — *подмножество*

$$F = \{0, 1, 1+1, \ldots, \underbrace{1+\ldots+1}_{p-1}\} \subseteq \Bbbk$$

есть подполе, изоморфное $\mathbb{F}_p$, что позволяет заменять при умножении «числа» из $\mathbb{F}_p$ на соответствующие элементы из F;

аксиомы векторного пространства — *выполняются в силу свойств арифметических операций в поле $\Bbbk$.*

Следствие

Конечное поле (как векторное пространство) состоит из p^n элементов, p — простое, n — натуральное.

Поля Галуа как кольца вычетов или векторные пространства

Конечную АС $\mathbb{F}_p^n$ с элементами-многочленами

$$M = \{ a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \} \subset \mathbb{F}_p[x]$$

можно рассматривать как

- факторкольцо вычетов по модулю некоторого неприводимого многочлена $f(x)$ степени n над полем $\mathbb{F}_p$:

$$\mathbb{F}_p^n = \langle \mathbb{F}_p / (f(x)); +_p, \cdot_p \rangle;$$

или как

- n-мерное координатное пространство над полем $\mathbb{F}_p$:

$$\mathbb{F}_p^n = \langle M, \mathbb{F}_p; +_p, \cdot_p \rangle.$$

Базис в $\mathbb{F}_p^n$

Теорема

Элементы $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ *образуют базис* $\mathbb{F}_p^n$.

Базис в $\mathbb{F}_p^n$

Теорема

Элементы $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ *образуют базис* $\mathbb{F}_p^n$.

Доказательство

Любой остаток представим в виде линейной комбинации указанных векторов:

$$\overline{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}} = a_0\overline{1} + a_1\overline{x} + \ldots + a_{n-1}\overline{x^{n-1}}.$$

$$\overline{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}} = a_0\overline{1} + a_1\overline{x} + \ldots + a_{n-1}\overline{x^{n-1}}.$$

И обратно, пусть $b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x^{n-1}} = 0$.
Это означает, что многочлен $g = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$ *делится на многочлен* n*-й степени* $f(x)$. *Поскольку при умножении многочленов их степени складываются, это возможно лишь при* $g = 0$.
$\therefore$ *система* $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ *линейно независима.*

Расширение поля $\mathbb{R}$

Замечание

Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы не только в случае конечных полей.

Расширение поля $\mathbb{R}$

Замечание

Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы не только в случае конечных полей.
Например,

- рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$;
- возьмём неприводимый многочлен $x^2 + 1 \in \mathbb{R}[x]$;
- построим поле как факторкольцо $\mathbb{R}[x]/(x^2 + 1)$.

Расширение поля $\mathbb{R}$

Замечание

Построение поля с помощью вычетов по модулю некоторого неприводимого многочлена и аналоги доказанных теорем справедливы не только в случае конечных полей.
Например,

- рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$;
- возьмём неприводимый многочлен $x^2 + 1 \in \mathbb{R}[x]$;
- построим поле как факторкольцо $\mathbb{R}[x]/(x^2 + 1)$.

Получилось векторное пространство над $\mathbb{R}$, его базис — $\overline{1}, \overline{x}$ и каждый элемент можно представить в виде $a\overline{1} + b\overline{x}$.
Полученное поле изоморфно полю комплексных чисел $\mathbb{C}$: изоморфизм задаётся соответствием

$$\overline{1} \mapsto 1, \quad \overline{x} \mapsto i\,.$$

Подполя $\mathbb{F}_p^n$

Лемма

Если поле $\mathbb{F}_p^n$ содержит подполе $\mathbb{F}_p^k$, то $k \mid n$.

Доказательство

Если поле $\Bbbk_1$ содержится в поле $\Bbbk_1 \subset \Bbbk_2$, то элементы $\Bbbk_2$ можно умножать на элементы из $\Bbbk_1$, а результаты складывать. Поэтому поле $\Bbbk_2$ является векторным пространством над полем $\Bbbk_1$ размерности d. Значит, в нем $|\Bbbk_1|^d$ элементов. Таким образом $p^n = (p^k)^d$, что и означает делимость n на k.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Минимальный многочлен

Рассмотрим поле $\mathbb{F}_p^n$, а в нём — какой-нибудь элемент β и будем интересоваться многочленами, для которых этот элемент является корнем.

Определение

Многочлен $m(x)$ называется *минимальной функцией* (или *минимальным многочленом, м.м.*) *для* β, если $m(x)$ — нормированный многочлен (со старшим коэффициентом 1) минимальной степени, для которого β является корнем.

Другими словами, должны выполняться три свойства:

1. $m(\beta) = 0$;
2. $\deg f(x) < \deg m(x) \Rightarrow f(\beta) \neq 0$;
3. коэффициент при старшей степени в $m(x)$ равен 1.

Минимальные многочлены: пример построения

Рассмотрим $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, где $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ — неприводимый многочлен. Тогда для класса вычетов $\overline{x} \in \mathbb{F}_p^n$ многочлен $a_n^{-1} a(x)$ — минимальный.

Минимальные многочлены: пример построения

Рассмотрим $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, где $a(x) = a_0 + a_1 x + \ldots + a_n x^n$ — неприводимый многочлен. Тогда для класса вычетов $\overline{x} \in \mathbb{F}_p^n$ многочлен $a_n^{-1} a(x)$ — минимальный.

1. $a_0\overline{1} + a_1\overline{x} + \ldots + a_n\overline{x}^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} = \overline{0}$ т.е. $\overline{x}$ — корень $a(x)$, но тогда $\overline{x}$ является корнем и $a_n^{-1} a(x)$.
2. Предположим, что существует многочлен $b_0 + b_1 x + \ldots + b_{n-1} x^{n-1}$, для которого

$$b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x}^{n-1} = b_0\overline{1} + b_1\overline{x} + \ldots + b_{n-1}\overline{x^{n-1}} = \overline{0}.$$

Это равенство задает линейную зависимость между классами $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$, которые образуют базис поля как векторного пространства над $\mathbb{F}_p$.
Поэтому $b_0 = b_1 = \ldots = b_{n-1} = 0$.

Свойства минимальных многочленов

Утверждение

Минимальные многочлены неприводимы.

Свойства минимальных многочленов

Утверждение

Минимальные многочлены неприводимы.

Доказательство

Пусть $m(x)$ *— м.м. и* $m(x) = m_1(x)m_2(x)$.
Имеем

$$m(\beta) = 0 \Rightarrow \left[\begin{array}{l} m_1(\beta) = 0 \\ m_2(\beta) = 0 \end{array} \right. .$$

Но $\deg m_1 < m(x)$ *и* $\deg m_2 < m(x)$, *что противоречит минимальности* $m(x)$.

Свойства минимальных многочленов...

Утверждение

Пусть $m(x)$ *— м.м. для* β*, и* $f(\beta) = 0$*. Тогда* $f(x)$ *делится на* $m(x)$*.*

Свойства минимальных многочленов...

Утверждение

Пусть $m(x)$ — м.м. для β, и $f(\beta) = 0$. Тогда $f(x)$ делится на $m(x)$.

Доказательство

Разделим $f(x)$ на $m(x)$ с остатком:

$$f(x) = u(x)m(x) + v(x)\,, \quad \deg v < \deg m\,.$$

Подставляя в это равенство β, получаем

$$0 = f(\beta) = u(\beta)m(\beta) + v(\beta) = v(\beta)\,,$$

т.е. β — корень $v(x)$, что противоречит минимальности $m(x)$.

Свойства минимальных многочленов...

Следствие

Для каждого β есть ровно одна минимальная функция.

Свойства минимальных многочленов...

Следствие

Для каждого β есть ровно одна минимальная функция.

Доказательство

Действительно, пусть минимальных функций две.
Они взаимно делят друг друга, а значит, различаются на обратимый множитель (константу).
Поскольку минимальная функция нормирована, эта константа равна 1, т. е. функции совпадают.

Свойства минимальных многочленов...

Утверждение

Для каждого $\beta \in \mathbb{F}_p$ существует минимальная функция и ее степень не превосходит n.

Свойства минимальных многочленов...

Утверждение

Для каждого $\beta \in \mathbb{F}_p$ существует минимальная функция и ее степень не превосходит n.

Доказательство

Рассмотрим следующие элементы поля $\mathbb{F}_p$: $1, \beta, \beta^2, \ldots, \beta^n$, их $n+1$ штука, а размерность $\mathbb{F}_p^n$ как векторного пространства над $\mathbb{F}_p$ равна n. Значит, эти элементы линейно зависимы, т.е. существуют такие коэффициенты $c_0, \ldots, c_n$, что

$$c_0 + c_1\beta + \ldots + c_n\beta_n = 0\,.$$

т.е. β — корень многочлена $f(x) = c_0 + c_1 x + \ldots + c_n x^n$. Минимальной функцией для β будет некоторый нормированный неприводимый делитель $f(x)$.

Многочлены над конечным полем: свойства

Теорема

Любой ненулевой элемент поля $\mathbb{F}_p^n$ *является корнем многочлена* $x^{p^n-1}-1$, *т.е.*

$$x^{p^n-1}-1 = (x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1}),$$

где $\{\beta_1,\ldots,\beta_{p^n-1}\} = \mathbb{F}_p^{n*} = \mathbb{F}_p^n \setminus \{0\}$.

Многочлены над конечным полем: свойства

Теорема

Любой ненулевой элемент поля $\mathbb{F}_p^n$ *является корнем многочлена* $x^{p^n-1}-1$, *т.е.*

$$x^{p^n-1}-1 = (x-\beta_1)\cdot\ldots\cdot(x-\beta_{p^n-1}),$$

где $\{\beta_1,\ldots,\beta_{p^n-1}\} = \mathbb{F}_p^{n*} = \mathbb{F}_p^n \setminus \{0\}$.

Доказательство

$\mathbb{F}_p^{n*}$ — *группа по умножению порядка* p^n-1.
Порядок любого элемента $\alpha \in \mathbb{F}_p^{n*}$ *(т.е. порядок циклической подгруппы* $\langle\alpha\rangle$*) по теореме Лагранжа делит порядок группы. Пусть* $\deg\alpha = k$, *тогда* $p^n-1 = kq$ *и* $\alpha^k = 1$, *поэтому*

$$\alpha^{p^n-1}-1 = \alpha^{kq}-1 = (\alpha^k)^q-1 = 1^q-1 = 0.$$

Многочлены над конечным полем: свойства...

Следствие

Все элементы поля $\mathbb{F}_p^n$, не исключая нуля, являются корнями многочлена $x^{p^n} - x$.

Многочлены над конечным полем: свойства...

Следствие

Все элементы поля $\mathbb{F}_p^n$, не исключая нуля, являются корнями многочлена $x^{p^n} - x$.

Доказательство

Вынесем x за скобку:

$$x^{p^n} - x = x\left(x^{p^n-1} - 1\right).$$

У правого множителя корнями будут все ненулевые элементы, а у левого — 0.

Многочлены над конечным полем: свойства...

Теорема

$(x^n - 1) \vdots (x^m - 1) \Leftrightarrow n \vdots m.$

Доказательство

Пусть $n = mk$. *Сделаем замену:* $x^m = y$, *тогда* $x^n - 1 = y^k - 1$ *и* $x^m - 1 = y - 1$. *Делимость очевидна, поскольку 1 является корнем* $y^k - 1$.

Предположим, что $n \not\vdots m$, *т.е.* $n = km + r$, $0 < r < m$, *тогда*

$$x^n - 1 = \frac{x^r(x^{mk} - 1)(x^m - 1)}{x^m - 1} + x^r - 1 =$$

$$= \frac{x^r(x^{mk} - 1)}{x^m - 1}(x^m - 1) + x^r - 1\,.$$

Многочлены над конечным полем: свойства...

Последнее выражение задает результат деления $x^n - 1$ *на* $x^m - 1$ *с остатком, поскольку* $x^{mk} - 1$ *делится на* $x^m - 1$ *по доказанному выше.*
Остаток $x^r - 1 \neq 0$ *в силу сделанных предположений.*
$\therefore x^n - 1$ *не делится на* $x^m - 1$.

Многочлены над конечным полем: свойства...

Последнее выражение задает результат деления $x^n - 1$ на $x^m - 1$ с остатком, поскольку $x^{mk} - 1$ делится на $x^m - 1$ по доказанному выше.
Остаток $x^r - 1 \neq 0$ в силу сделанных предположений.
$\therefore$ $x^n - 1$ не делится на $x^m - 1$.

Эта теорема дает нам возможность раскладывать многочлены $x^n - 1$ при составных n.
Например, разложим $x^{15} + 1$ в поле характеристике 2 (где $+1 = -1$):

$$x^{15} + 1 = (x^3 + 1)(x^{12} + x^9 + x^6 + x^3 + 1), \quad (3 \mid 15).$$

Продолжить это разложение помогает следующая теорема.

Многочлены над конечным полем...

Теорема

Все неприводимые многочлены n-й степени над $\mathbb{F}_p$ являются делителями $x^{p^n} - x$.

Многочлены над конечным полем...

Теорема

Все неприводимые многочлены n-й степени над $\mathbb{F}_p$ являются делителями $x^{p^n} - x$.

Доказательство

Если $n = 1$, то нужно проверить, что $x - a \mid x^p - x$, где $a \in \mathbb{F}_p$. Это очевидно при $a = 0$, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1$.

При $n > 1$ строим по неприводимому многочлену $f(x)$ степени n поле $\mathbb{F}_p^n$. Тогда многочлен $f(x)$ имеет в $\mathbb{F}_p^n$ корень $\overline{x}$, а нормированный $f(x)$ является минимальной функцией для него. Кроме того, $\overline{x}$ является корнем уравнения $x^{p^n-1} - 1$.

По свойствам м.м., $x^{p^n-1} - 1$ делится на $f(x)$.

Многочлены над конечным полем...

Используя эту теорему, мы можем завершить разложение

$$x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\,,$$

перебирая неприводимые многочлены из $\mathbb{F}_2^4$
(т.к. $x(x^{15}+1) = x^{2^4}+x$).

Теорема

Любой неприводимый делитель многочлена $x^{p^n-1}-1$ имеет степень, не превосходящую n.

Многочлены над конечным полем...

Используя эту теорему, мы можем завершить разложение

$$x^{15}+1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1),$$

перебирая неприводимые многочлены из $\mathbb{F}_2^4$
(т.к. $x(x^{15}+1) = x^{2^4}+x$).

Теорема

Любой неприводимый делитель многочлена $x^{p^n-1}-1$ имеет степень, не превосходящую n.

Доказательство

Пусть φ — неприводимый многочлен степени k, который является делителем $x^{p^n}-x$. Кратные φ образуют максимальный идеал в кольце $\mathbb{F}_p[x]$, поэтому кольцо вычетов по этому идеалу является полем.

Многочлены над конечным полем...

Поле можно рассматривать как векторное пространство над $\mathbb{F}_p$ *с базисом* $\left\{\overline{1}, \overline{x}, \ldots, \overline{x^{k-1}}\right\}$. *Обозначим* $\overline{x} = \alpha$. *Поскольку* $x^{p^n} - x$ *делится на* φ, *то в кольце вычетов по модулю идеала* (φ) *получаем* $\alpha^{p^n} - \alpha = 0$.

Любой элемент построенного поля выражается через базис: $\beta = \sum_{i=0}^{k-1} a_i \alpha^i$. *Возведя обе части этого равенства в степень* p^n, *получим*

$$\begin{aligned}\beta^{p^n} &= (a_0 + a_1\alpha + \ldots + a_{k-1}\alpha^{k-1})^{p^n} = \\ &= a_0^{p^n} + a_1^{p^n}\alpha^{p^n} + \ldots + a_{k-1}^{p^n}(\alpha^{k-1})^{p^n} = \\ &= a_0 + a_1\alpha + \ldots + a_{k-1}\alpha^{k-1} = \beta\,.\end{aligned}$$

Отсюда $\beta^{p^n} - \beta = 0$, *т.е.* β *— корень уравнения* $x^{p^n} - x = 0$. *Но у него не более* p^n *различных корней, а в построенном нами поле —* p^k *элементов. Каждый элемент поля является корнем,* $\therefore n > k$.

Многочлены над конечным полем...

Утверждение

Пусть $\beta \in \mathbb{F}_p^n$ *имеет порядок* l, *а его м.м.* $m(x)$ *имеет степень* k.

Тогда (a) $p^k - 1 \vdots l$, *а если* $r < k$, *то (b)* $(p^r - 1) \not\vdots l$.

Многочлены над конечным полем...

Утверждение

Пусть $\beta \in \mathbb{F}_p^n$ *имеет порядок* l, *а его м.м.* $m(x)$ *имеет степень* k.

Тогда (a) $p^k - 1 \vdots l$, *а если* $r < k$, *то (b)* $(p^r - 1) \not\vdots l$.

Доказательство

a) По неприводимому многочлену k*-й степени* $m(x)$ *строим поле из* p^k *элементов. Все его ненулевые элементы, в том числе и* β, *являются корнями уравнения* $x^{p^k-1} - 1 = 0$, *т.е.* $\beta^{p^k-1} - 1 = 0$ *и* $\beta^{p^k-1} = 1$.

b) Пусть $(p^r - 1) \vdots l$ *и* $r < k$. *Тогда* β *— корень уравнения* $x^{p^r} - 1 = 0$, *а т.к.* $m(x)$ *— м.м. для* β, *то* $(x^{p^r} - 1) \vdots m(x)$ *(было доказано). Мы нашли неприводимый делитель многочлена* $x^{p^r} - 1$ *степени* k, *но* $k > r$, *что противоречит доказанному ранее.*

Многочлены над конечным полем...

Следующая теорема нужна нам для того, чтобы раскладывать многочлены на множители.

Теорема

Пусть $\beta \in \mathbb{F}_p^n$ — корень неприводимого многочлена $\varphi(x)$ степени n с коэффициентами из $\mathbb{F}_p$. Тогда $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ все различны и исчерпывают список корней этого многочлена.

Т. е. чтобы получить все корни неприводимого многочлена, достаточно найти один из них и возводить его последовательно в степень p.

Многочлены над конечным полем...

Следующая теорема нужна нам для того, чтобы раскладывать многочлены на множители.

Теорема

Пусть $\beta \in \mathbb{F}_p^n$ — корень неприводимого многочлена $\varphi(x)$ степени n с коэффициентами из $\mathbb{F}_p$. Тогда $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ все различны и исчерпывают список корней этого многочлена.

Т. е. чтобы получить все корни неприводимого многочлена, достаточно найти один из них и возводить его последовательно в степень p.

Доказательство

Вначале докажем, что если β — корень $\varphi(x)$, то β^p — тоже корень.

Многочлены над конечным полем...

Как было показано выше, $a^p = a$ *для всех* $a \in \mathbb{F}_p$. *Поэтому для любого многочлена* $f(x)$ *с коэффициентами из* $\mathbb{F}_p$ *выполняется равенство*

$$(f(x))^p = f(x^p)\,. \qquad (*)$$

Действительно, возведение в степень p *сохраняет операции сложения и умножения. Поэтому*

$$(a_0 + a_1 x + \ldots + a_k x^k)^p = a_0^p + a_1^p x^p + a_2^p x^{2p} + \ldots + a_k^p x^{kp} = \\ = a_0 + a_1 (x^p) + a_2 (x^p)^2 + \ldots + a_k (x^p)^k.$$

Если $\varphi(\beta) = 0$, *то и* $\varphi(\beta)^p = 0$. *Из* $(*)$ *получаем, что и* $\varphi(\beta^p) = 0$. *Итак, мы доказали, что* $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ *— корни многочлена* $\varphi(x)$.

Многочлены над конечным полем...

Осталось доказать, что они все различны, тогда из доказанного ранее будет следовать, что мы нашли все корни многочлена $\varphi(x)$.

Предположим, что $\beta^{p^l} = \beta^{p^k}$, *причем без ограничения общности* $l \leqslant k$. *Мы знаем, что* $\beta^{p^n} = \beta$. *С другой стороны, поскольку*

$$\beta^{p^n} = \beta^{p^k \cdot p^{n-k}} = \left(\beta^{p^k}\right)^{p^{n-k}} = \left(\beta^{p^l}\right)^{p^{n-k}} = \beta^{p^{n-k+l}},$$

то β *— корень уравнения* $x^{p^{n-k+l}-1} - 1 = 0$. *Из ранее доказанного получаем* $n - k + l \geqslant n$, *так что* $l \geqslant k$. *Другими словами,* $l = k$ *и все выписанные выше корни различны.*

Многочлены над конечным полем: решение уравнений

Пример

Рассмотрим $\mathbb{F}_2$ и неприводимый над этим полем многочлен $x^4 + x^3 + 1$. Найдем его корни в расширении $\mathbb{F}_2^4$.

Один корень получаем немедленно: $\overline{x}$.

По только что доказанной теореме можно выписать остальные: $\overline{x^2}$, $\overline{x^4} = \overline{x^3 + 1}$, $\overline{x^8} = \overline{x^6 + 1} = \overline{x^3 + x^2 + x}$.

Многочлены над конечным полем: решение уравнений

Пример

Рассмотрим $\mathbb{F}_2$ и неприводимый над этим полем многочлен $x^4 + x^3 + 1$. Найдем его корни в расширении $\mathbb{F}_2^4$.

Один корень получаем немедленно: $\overline{x}$.

По только что доказанной теореме можно выписать остальные: $\overline{x^2}$, $\overline{x^4} = \overline{x^3 + 1}$, $\overline{x^8} = \overline{x^6 + 1} = \overline{x^3 + x^2 + x}$.

Покажем, что $\alpha = x^2$ действительно корень $x^4 + x^3 + 1 = 0$.

Подставляем:

$$x^4 + x^3 + 1 \,|_{x=\alpha} = x^{4\cdot 2} + x^{4+2} + 1 \,|_{x^4 = x^3+1} =$$
$$= (x^3 + 1)^2 + (x^3 + 1)x^2 + 1 = (x^6 + 1) + x^5 + x^2 + 1 =$$
$$= x^6 + x^5 + x^2 = x^2(x^4 + x^3 + 1) = x^2 \cdot 0 = 0.$$

Как решать уравнения, когда корней нет

Как решать уравнения, когда корней нет

Для решения уравнения

$$f(x) = 0\,, \qquad (*)$$

где f — неприводимый многочлен степени n, над полем $\mathbb{F}_p$ нужно построить поле $\mathbb{F}_p[x]/(f)$.

Корни $(*)$ в этом поле: $\overline{x}$, $\overline{x^2}$, $\ldots$, $\overline{x^{p^{n-1}}}$.

В общем случае для решения уравнения нужно уметь раскладывать многочлен на неприводимые множители.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Мультипликативная группа расширения поля

Пример (поле $\mathbb{F}_2^4$)

Поле $\mathbb{F}_2^4$ можно строить с помощью любого из трех неприводимых многочленов (но пока не доказано).
Удобнее всего это сделать, если взять многочлен $f = x^4 + x + 1$ (почему?).
Будем задавать элементы расширения наборами коэффициентов многочлена, который получается в остатке при делении на f, записывая их в порядке возрастания степеней.
Порождающим является элемент $\alpha = x$, который записывается как $(0, 1, 0, 0)$.
Вычислим степени α, сведя результаты в таблицу.

Мультипликативная группа поля $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4+x+1)$

степень α	1	x	x^2	x^3
$\alpha =$	(0,	1,	0,	0)
$\alpha^2 =$	(0,	0,	1,	0)
$\alpha^3 =$	(0,	0,	0,	1)
$1+\alpha = \alpha^4 =$	(1,	1,	0,	0)
$\alpha+\alpha^2 = \alpha^5 =$	(0,	1,	1,	0)
$\alpha^2+\alpha^3 = \alpha^6 =$	(0,	0	1,	1)
$\alpha^3+\alpha+1 = \alpha^3+\alpha^4 = \alpha^7 =$	(1,	1,	0	1)
$1+\alpha^2 = \alpha+1+\alpha^2+\alpha = \alpha^8 =$	(1,	0,	1,	0)
$\alpha+\alpha^3 = \alpha^9 =$	(0,	1,	0,	1)
$\alpha^2+1+\alpha = \alpha^2+\alpha^4 = \alpha^{10} =$	(1,	1,	1,	0)
$\alpha+\alpha^2+\alpha^3 = \alpha^{11} =$	(0,	1,	1,	1)
$1+\alpha+\alpha^2+\alpha^3 = \alpha^2+\alpha^3+\alpha^4 = \alpha^{12} =$	(1,	1,	1,	1)
$1+\alpha^2+\alpha^3 = \alpha+\alpha^2+\alpha^3+\alpha^4 = \alpha^{13} =$	(1,	0,	1,	1)
$1+\alpha^3 = \alpha+\alpha^3+\alpha^4 = \alpha^{14} =$	(1,	0,	0,	1)
$1 = \alpha+\alpha^4 = \alpha^{15} =$	(1,	0,	0,	0)

Имея такую таблицу, очень просто производить умножение:

$$(x^3 + x + 1) \cdot (x^2 + x + 1) = x^2,$$
$$(1, 1, 0, 1) \cdot (1, 1, 1, 0) = (0, 0, 1, 0) \quad - (+_{\mathrm{mod}\,2}),$$
$$\alpha^7 \alpha^{10} = \alpha^{17} = \alpha^2.$$

Лемма

Пусть m — максимальный порядок элемента в конечной абелевой группе G. Тогда порядок любого элемента G делит m.

Теперь можно вернуться к вопросу о существовании

а) конечного поля $\mathbb{F}_q$ размера q, показав, что всегда $q = p^n$;
б) неприводимого многочлена степени n над $\mathbb{F}_p$.

(везде p — простое, n — натуральное).

Пути доказательства

Это можно сделать двумя способами.

- а) $\Rightarrow$ б) доказать существование поля из p^n элементов, откуда вывести существование неприводимого многочлена степени n над $\mathbb{F}_p$;
- б) $\Rightarrow$ а) установить существование неприводимого многочлена f степени n над $\mathbb{F}_p$, откуда уже следует существование поля из p^n как факторкольца по идеалу (f).

Мы пойдём вторым путём.

Существование неприводимого многочлена степени n над полем $\mathbb{F}_p$

Для нормированных многочленов выполняется аналог основной теоремы арифметики: *каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов.*

Существование неприводимого многочлена степени n над полем $\mathbb{F}_p$

Для нормированных многочленов выполняется аналог основной теоремы арифметики: *каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов.*

Действительно:

- *разложение в евклидовом кольце однозначно (с точностью до умножения на обратимые элементы — делители);*
- *в случае кольца многочленов над полем обратимые элементы — это константы (многочлены степени 0);*
- *выбор старшего коэффициента устраняет произвол в выборе сомножителей.*

Число неприводимых нормированных многочленов d_n

Лемма (о числе d_n)

Пусть d_n — число неприводимых нормированных многочленов степени n над полем $\mathbb{F}_p$. Тогда

$$\sum_{m|n} m \cdot d_m = p^n.$$

Доказательство

Занумеруем $i = 1, \ldots, d_n$ все неприводимые нормированные многочлены степени n и сопоставим им формальную переменную $f_{i,n}$. Тогда произвольному нормированному многочлену степени n однозначно сопоставлен моном произведения этих переменных

$$f_{i_1,n_1}^{s_1} \cdot \ldots \cdot f_{i_r,n_r}^{s_r}, \quad \text{причем} \sum_{j=1}^{r} n_j, s_j = n\,.$$

Число неприводимых нормированных многочленов d_n...

Доказательство

Поэтому все нормированные многочлены перечисляются формальным бесконечным произведением

$$\prod_{i,n}\left(\sum_{k=0}^{\infty} f_{i,n}^k\right) = \sum f_{i_1,n_1}^{s_1} \cdot \ldots \cdot f_{i_r,n_r}^{s_r}$$

(раскрыты скобки и бесконечное произведение записано в виде формального ряда; это равенство — это другой способ сказать, что каждый нормированный многочлен однозначно разлагается в произведение неприводимых нормированных).
Сделаем замену переменных $f_{i,n} = t^n$, *которая делает все многочлены одной степени неразличимыми. Приведение подобных в правой части равенства даст ряд от переменной* t.

Число неприводимых нормированных многочленов d_n...

Доказательство

Коэффициент при t^n в этом ряде равен числу нормированных многочленов степени n, которое равно p^n. Действительно, нормированный многочлен степени n однозначно задается своими коэффициентами $a_0, \ldots, a_{n-1}$ (т.к. старший коэффициент равен 1). В левой части равенства все неприводимые многочлены степени n дадут одинаковый множитель (сумму бесконечной геометрической прогрессии со знаменателем t^n). Равенство превращается в

$$\prod_n \left(\sum_{k=0}^{\infty} f^{nk} \right)^{d_n} = \sum_{n=0}^{\infty} p^n t^n.$$

По формуле для суммы бесконечной геометрической прогрессии

$$\prod_n \frac{1}{(1-t^n)^{d_n}} = \frac{1}{1-p^t}.$$

Число неприводимых нормированных многочленов d_n...

Доказательство

Прологарифмируем:

$$\sum_n d_n \ln(1 - t^n) = \ln(1 - pt)\,.$$

Продифференцируем по t:

$$\sum_n d_n \frac{nt^{n-1}}{1 - t^n} = \frac{p}{1 - pt}\,.$$

Снова воспользуемся суммой геометрической прогрессии:

$$\sum_{n,k} d_n n t^{n-1} t^{nk} = \sum_s p^{s+1} t^s.$$

Число неприводимых нормированных многочленов d_n...

Доказательство

Косметические преобразования:

$$\sum_{n,k} n d_n t^{n(k+1)} = \sum_{s} p^s t^s.$$

Равенство коэффициентов при одинаковых степенях t в левой и правой части и есть утверждение леммы.

Важные замечания

Замечание (Доказательство теоремы о существовании неприводимых полиномов)

Из данной леммы следует неравенство $nd_n \leqslant p^n$. Простая оценка

$$nd_n = \sum_{k|n,\, k<n} kd_k \geqslant p^n - \sum_{k=0}^{n-1} p^k = p^n - \frac{p^n - 1}{p - 1} > 0 \ .$$

доказывает, что $d_n>0$, а это означает, что существует хотя бы один неприводимый многочлен степени n.

Замечание

Из данной леммы вытекает, что при $n \to \infty$ имеем $d_n \sim p^n/n$. Таким образом, примерно, $1/n$-я часть всех многочленов степени n над полем из p элементов неприводима.

Важные

Докажем вторую часть основной теоремы о конечных полях: любые два поля с одинаковым числом элементов изоморфны.

Теорема

Пусть m — минимальная функция элемента $\alpha \in \mathbb{F}_p^n$ и d — её степень. Тогда поле $\mathbb{F}_p[x]/(m)$ изоморфно подполю $\mathbb{F}_p^d$, порожденному степенями α.

Доказательство

Степени α принадлежат d-мерному пространству с базисом $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$, которое является подполем поля $\mathbb{F}_p^n$, поскольку замкнуто относительно сложения и умножения и содержит 0 и 1.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Кольцо $\mathbb{F}_p/(f)$

В приложениях часто используется кольцо $\mathbb{F}_p/(f)$ по модулю главного идеала не обязательно неприводимого многочлена $f \in \mathbb{F}_p[x]$.

Если f неприводим, то $\mathbb{F}_p/(f)$ — поле и этот случай уже рассмотрен.

Кольцо $\mathbb{F}_p/(f)$

В приложениях часто используется кольцо $\mathbb{F}_p/(f)$ по модулю главного идеала не обязательно неприводимого многочлена $f \in \mathbb{F}_p[x]$.

Если f неприводим, то $\mathbb{F}_p/(f)$ — поле и этот случай уже рассмотрен.

В любом случае вычеты образуют векторное пространство над $\mathbb{F}_p$ многочленов степени не выше $\deg f$.

$$
\begin{aligned}
\mathbb{F}_p[x] &= \{0, 1, \ldots, x, x+1, \ldots, f, \ldots\};\\
(f) = \overline{f} &= \{t \cdot f\},\ t \in \mathbb{F}_p[x];\\
\mathbb{F}_p/(f) &= \{\overline{f}, \overline{g}, \overline{h}, \ldots\},\ \deg g, \deg h, \ldots < \deg f;\\
\overline{g} &= \{t \cdot f + g\};\\
\overline{h} &= \{t \cdot f + h\};\\
&\ldots\\
\overline{g} + \overline{f} &= \overline{g},\ \ \overline{g} \cdot \overline{f} = \overline{f}.
\end{aligned}
$$

Нормированный делитель в порождающего элемента идеала

Теорема

Пусть φ — непривидимый нормированный многочлен, который делит f: $\varphi \mid f$. Тогда совокупность всех вычетов, кратных φ, образует идеал в кольце классов вычетов по модулю f и φ — единственный нормированный многочлен минимальной степени в этом идеале.

Доказательство

Итак, $(f) = tf, t, s \in \mathbb{F}_p[x]$, $\deg f \geqslant \deg \varphi = k$

$$\varphi = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + 1 \cdot x^k, \quad f = \varphi^* \varphi;$$

$$I_\varphi \stackrel{\text{def}}{=} s\varphi \subseteq (f) = t\varphi^*\varphi \Leftrightarrow \deg s \geqslant \deg \varphi.$$

Нормированный делитель...

Проверим, что I_φ — идеал. $\overline{g} = \{s\varphi\}$, $\overline{h} = \{r\varphi\}$; $s, r \in \mathbb{F}_p[x]$.

1.
$$\left\{ \begin{array}{l} \overline{g} \in I_\varphi, \\ \overline{h} \leqslant \overline{g}. \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \{s\varphi\},\ \deg s \geqslant \deg \varphi \\ \{r\varphi\},\ \deg r \geqslant \deg s. \end{array} \right. \Rightarrow$$
$$\Rightarrow \Rightarrow$$
$$\Rightarrow\ \deg r \geqslant \deg \varphi \ \Rightarrow\ \overline{h} \in I_\varphi$$

2. $\overline{g}, \overline{h} \in I_\varphi \ \Leftrightarrow\ \deg s, \deg r \geqslant \deg \varphi.$
$$\overline{g} + \overline{h} = \{s\varphi\} + \{r\varphi\} = \{(s+r)\varphi\};$$
$$\deg(s+r) \geqslant \deg \varphi \ \Rightarrow\ \overline{g} + \overline{h} \in I_\varphi.$$

Нормированный делитель...

Покажем, что в I_φ *нет других, кроме*

$$\varphi = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + x^k$$

нормированных многочленов степени, меньшей $k = \deg \varphi$.
Пусть $\psi = b_0 + b_1 x + \ldots + b_{m-1} x^{m-1} + x^m \in I_\varphi$, $m \leqslant k$. *Тогда:*

$$\psi \in I_\varphi \Rightarrow \varphi \mid \psi \Rightarrow \begin{cases} m \geqslant k, \ \text{т.е. } k = m \\ b_i = a_i, \ i = 0, 1, \ldots, m-1 \end{cases} \Rightarrow \psi = \varphi.$$

Подыдеал как векторное пространство

Теорема

Пусть φ — неприводимый нормированный делитель многочлена $f \in \mathbb{F}_p[x]$ отличный от f, $\deg f = n$, $\deg \varphi = k$. Тогда идеал (φ) — векторное пространство размерности $n - k$.

Доказательство

Подыдеал как векторное пространство

Теорема

Пусть φ — неприводимый нормированный делитель многочлена $f \in \mathbb{F}_p[x]$ отличный от f, $\deg f = n$, $\deg \varphi = k$. Тогда идеал (φ) — векторное пространство размерности $n - k$.

Доказательство

Без доказательства.

Циклическое пространство: определение

- Пусть F — n-мерное векторное пространство (над каким-то полем).
- Фиксируем некоторый базис F.
- Тогда
  $F \cong F^n = \{ (a_0, \ldots, a_{n-1}) \}$, $a_i \in F$, $i = 0, 1, \ldots, n-1$ — т.е. координатное пространство.

Определение

Подпространство координатного пространства F^n называется *циклическим*, если вместе с набором $(a_0, \ldots, a_{n-1})$ оно содержит циклический сдвиг этого набора, т.е. набор $(a_{n-1}, a_0, \ldots, a_{n-2})$.

Кольцо классов вычетов по модулю многочлена $x^n - 1$

В кольце $\mathbb{F}_p/(x^n - 1)$, рассматриваемом как векторное пространство над полем $\mathbb{F}_p$, есть базис $\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$.

Циклический сдвиг координат в этом базисе равносилен умножению на x:

$$\overline{(a_0 + a_1 x + \ldots + a_{n-1}x^{n-1})} \cdot \overline{x} =$$
$$= \overline{(a_0 x + a_1 x^2 + \ldots + a_{n-1}x^n)} =$$
$$= \overline{(a_{n-1} + a_0 x + a_1 x^2 + \ldots + a_{n-2}x^{n-1})}.$$

Подпространство $\mathbb{F}_p/(x^n-1)$

Теорема

Подпространство $I \subseteq \mathbb{F}_p/(x^n-1)$ является циклическим iff I — идеал в $\mathbb{F}_p/(x^n-1)$.

Подпространство $\mathbb{F}_p/(x^n-1)$

Теорема

Подпространство $I \subseteq \mathbb{F}_p/(x^n-1)$ является циклическим iff I — идеал в $\mathbb{F}_p/(x^n-1)$.

Доказательство

- *Если подпространство I — идеал, то оно замкнуто относительно умножения на $\overline{x}$, а это умножение и есть циклический сдвиг.*

Подпространство $\mathbb{F}_p/(x^n-1)$

Теорема

Подпространство $I \subseteq \mathbb{F}_p/(x^n-1)$ является циклическим iff I — идеал в $\mathbb{F}_p/(x^n-1)$.

Доказательство

- *Если подпространство I — идеал, то оно замкнуто относительно умножения на $\overline{x}$, а это умножение и есть циклический сдвиг.*
- *Пусть I — циклическое подпространство I и $g \in I$.*
  Тогда $g \cdot \overline{x}$, $g \cdot \overline{x^2}$, ... — циклические сдвиги, т.е. также принадлежат I.
  Значит, $g \cdot \overline{f} \in I$ для любого многочлена f. Поэтому I — идеал.

Разложение $x^n - 1$ на неприводимые множители

Разложим многочлен $x^n - 1$ на неприводимые над $\mathbb{F}_p$ множители:

$$x^n - 1 = f_1^{a_1}(x) \cdot f^{a_2}(x) \cdot \ldots \cdot f_s^{a_s}(x).$$

По китайской теореме об остатках кольцо классов вычетов по модулю многочлена $x^n - 1$ изоморфно прямой сумме колец классов вычетов по модулю многочленов $f_i^{a_i}(x)$:

$$\mathbb{F}_p[x]/(x^n - 1) \cong f_1^{a_1}(x) \oplus f^{a_2}(x) \oplus \ldots \oplus f_s^{a_s}(x).$$

Иногда такое разложение оказывается полезным.

Примитивные корни

Любой многочлен из $\mathbb{F}_p[x]$ разлагается на линейные множители в поле характеристики p.

Будем разлагать в поле $\mathbb{F}_q$ характеристики p многочлен $x^n - 1$.

- В $\mathbb{F}_q$ выполняется равенство $x^{kp} - 1 = (x^k - 1)^p$, поэтому интересен случай, когда n взаимно просто с p: тогда у многочлена $x^n - 1$ кратных корней нет (он взаимно прост со своей производной nx^{n-1}).
- Равенство $x^n = 1$ означает, что порядок элемента x в мультипликативной (цикличной!) группе $\mathbb{F}_q^*$ делит n.

$\therefore$ корни уравнения $x^n - 1 = 0$ образуют подгруппу в $\mathbb{F}_q^*$ (*группа корней из единицы степени* n), и эта подгруппа также циклическая; её порождающие элементы называются *примитивными корнями степени* n.

Количество и степени неприводимых делителей $x^n - 1$

Подгруппа порядка n в циклической группе существует тогда и только тогда, когда n делит порядок циклической группы $\Rightarrow$ необходимое и достаточное условие того, что поле $\mathbb{F}_q$ содержит группу корней из единицы степени n: *n должно быть делителем $q - 1$*.

Чтобы вернуться от разложения $x^n - 1$ на линейные множители в поле $\mathbb{F}_q$ к разложению на неприводимые множители в поле $\mathbb{F}_p$, нужно понять, какие корни из единицы будут входить в неприводимый делитель $f(x)$.

Было установлено: если уравнение $f(x) = 0$ имеет корень β, то и β^p, β^{p^2} и т.д. также будут корнями $f(x)$.

$\therefore$ количество и степени неприводимых делителей $x^n - 1$ можно найти, разбив вычеты по модулю n на орбиты отображения $t \mapsto p^t \mod n$.

Разложение многочлена $x^{15}-1$ над полем $\mathbb{F}_2$

Пример

Рассмотрим ещё раз разложение многочлена $x^{15}-1$ над $\mathbb{F}_2$. Относительно умножения на 2 вычеты по модулю 15 разбиваются на такие орбиты:

$$\{\overline{0}\},\ \{\overline{1},\overline{2},\overline{4},\overline{8}\},\ \{\overline{3},\overline{6},\overline{12},\overline{9}\},\ \{\overline{5},\overline{10}\},\ \{\overline{7},\overline{14},\overline{13},\overline{11}\}$$

$(1\cdot 2=2,\ 2\cdot 2=4,\ 4\cdot 2=8,\ 8\cdot 2=16\equiv_{15}=1$ и т.д.$)$.

Поэтому $x^{15}-1$ разлагается в произведение одного неприводимого многочлена степени 1, одного неприводимого многочлена степени 2 и трех неприводимых многочленов степени 4 (разложение было раньше):

$$x^{15}+1 = \\ =(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Разложение многочлена $x^{23} - 1$ над полем $\mathbb{F}_2$

Пример

Рассмотрим разложение многочлена $x^{23} - 1$ над $\mathbb{F}_2$. Относительно умножения на 2 вычеты по модулю 23 разбиваются на три орбиты:

$$\{\overline{0}\}, \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{9}, \overline{18}, \overline{13}, \overline{3}, \overline{6}, \overline{12}\},$$
$$\{\overline{5}, \overline{10}, \overline{20}, \overline{17}, \overline{11}, \overline{22}, \overline{21}, \overline{19}, \overline{15}, \overline{7}, \overline{14}\}$$
$$(18 \cdot 2 = 36 \equiv_{23} 13)$$

Поэтому $x^{23} - 1$ разлагается в произведение одного неприводимого многочлена степени 1 и двух неприводимых многочленов степени 11.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Задача

Решить уравнение $4x = 1$ *в поле* $\mathbb{Z}/(101)$.

Решение

Задача

Решить уравнение $4x = 1$ *в поле* $\mathbb{Z}/(101)$.

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$

Задача

Решить уравнение $4x = 1$ *в поле* $\mathbb{Z}/(101)$.

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$
2. *Можно решать уравнение* $4x + 101y = 1$ *в целых числах расширенным алгоритмом Евклида.*
   Решение: $4 \cdot 76 + 101 \cdot (-3) = 1.$
   Расширенный алгоритм Евклида применяется для решения уравнений
   $$ax + by = \text{НОД}(a, b)$$
   и систем таких уравнений в целых числах.

Задача

Решить уравнение $4x = 1$ *в поле* $\mathbb{Z}/(101)$.

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$
2. *Можно решать уравнение* $4x + 101y = 1$ *в целых числах расширенным алгоритмом Евклида.*
   Решение: $4 \cdot 76 + 101 \cdot (-3) = 1.$
   Расширенный алгоритм Евклида применяется для решения уравнений
   $$ax + by = \text{НОД}(a, b)$$
   и систем таких уравнений в целых числах.

Замечание

$x = -126$ — тоже решение: $4 \cdot (-126) = -504 \equiv_{101} 1$...

Задача (Теорема Вильсона)

Доказать, что $(p-1)! \equiv_p -1$ *для простого* p.

Задача (Теорема Вильсона)

Доказать, что $(p-1)! \equiv_p -1$ *для простого* p.

Решение

$p = 2$: — *утверждение тривиально.*

Задача (Теорема Вильсона)

Доказать, что $(p-1)! \equiv_p -1$ *для простого* p.

Решение

$p = 2$: — *утверждение тривиально.*

$p > 2$: *Элементы* $\mathbb{F}_p$ *являются корнями уравнения* $x^{p-1} - 1 = 0$ *и других корней у этого уравнения нет (многочлен степени* $p-1$ *имеет не больше* $p-1$ *корня).*

По теореме Виета их произведение равно свободному члену -1.

Задача

Найти $x \equiv_{17} 1^{2006} + 2^{2006} + \ldots + 16^{2006}$.

Задача

Найти $x \equiv_{17} 1^{2006} + 2^{2006} + \ldots + 16^{2006}$.

Решение

- $\mathbb{F}_{17}^* = \{1, 2, \ldots, 16\} = \langle 3 \rangle$:
  $3^1 = 1$, $3^2 = 9$, $3^3 = 27 \equiv_{17} 10$, $30 \equiv_{17} 13$, $39 \equiv_{17} 5$...;
- $G = \{1^{2006}, 2^{2006}, \ldots, 16^{2006}\}$ — *циклическая подгруппа порядка* k *группы* $\mathbb{F}_{17}^*$.

- *Элементы* G — *корни уравнения*

$$x^k - 1 = 0 \qquad (*)$$

- *Их сумма по теореме Виета есть коэффициент при* x^{k-1} *в* $(*)$, *т.е. 0.*

Задача

Производная многочлена $f \neq 0$ над полем характеристики p тождественно равна 0.

Доказать, что этот многочлен приводимый.

Задача

Производная многочлена $f \neq 0$ над полем характеристики p тождественно равна 0.
Доказать, что этот многочлен приводимый.

Решение

- *производная монома $(x^n)' = nx^{n-1}$ тождественно равна 0 iff $p \mid n$;*
- $f' = 0 \Rightarrow$ *показатели степеней всех мономов многочлена f делятся на p;*
- *поэтому $f(x) = g(x^p) = g^p(x)$.*

Задача

Доказать, что любая функция $f : \mathbb{F}_p^n \to \mathbb{F}_p^n$ *может быть представлена многочленом.*

Задача

Доказать, что любая функция $f : \mathbb{F}_p^n \to \mathbb{F}_p^n$ *может быть представлена многочленом.*

Решение

Можно, например, использовать интерполяционный многочлен Лагранжа:

$$f(x) = \sum_{\alpha \in \mathbb{F}_p^n} f(a) \frac{\prod_{b \in \mathbb{F}_p^n \setminus \{a\}} (x - b)}{\prod_{b \in \mathbb{F}_p^n \setminus \{a\}} (a - b)}.$$

Задача

Многочлен $x^5 + x^3 + x^2 + 1$ *разложить на неприводимые множители над полем вычетов по модулю 2.*

Задача

Многочлен $x^5 + x^3 + x^2 + 1$ *разложить на неприводимые множители над полем вычетов по модулю 2.*

Решение

1. $f(x) = x^5 + x^3 + x^2 + 1$, $f(1) = 0 \Rightarrow 1$ — *корень* f.
2. *Делим* f *на* $x = 1$, *получаем* $x^4 + x^3 + x + 1 = f_1(x)$.
3. $f_1(1) = 0 \Rightarrow 1$ — *корень* f_1; $\frac{f_1}{x+1} = x^3 + 1 = f_2(x)$.
4. $f_2(1) = 0 \Rightarrow 1$ — *корень* f_2; $\frac{f_2}{x+1} = x^2 + x + 1$.
5. *Многочлен* $x^2 + x + 1$ *неприводим.*

Ответ: $x^5 + x^3 + x^2 + 1 = (x+1)^3(x^2 + x + 1)$.

Задача

Многочлен $f = x^3 + 2x^2 + 4x + 1$ *разложить на неприводимые множители над полем* $\mathbb{F}_5$.

Задача

Многочлен $f = x^3 + 2x^2 + 4x + 1$ *разложить на неприводимые множители над полем* $\mathbb{F}_5$.

Решение

1. $f(2) = 2^3 + 2 \cdot 2^2 + 4 \cdot 2^2 + 1 = 25 \equiv_5 0$, $(x - 2) \equiv_5 (x + 3)$.
2. $$\begin{array}{rr|r} x^3 + 2x^2 + 4x + 1 & & x + 3 \\ \cline{3-3} x^3 + 3x^2 & & x^2 + 4x + 2 \\ \cline{1-1} 4x^2 + 4x & & \\ 4x^2 + 2x & & \\ \cline{1-1} 2x + 1 & & \\ 2x + 1 & & \\ \cline{1-1} 0 & & \end{array}$$
3. *Многочлен* $f_1 = x^2 + 4x + 2$ *неприводим в* $\mathbb{F}_5$.

Ответ: $x^3 + 2x^2 + 4x + 1 = (x + 3)(x^2 + 4x + 2)$.

Задача

Многочлен $f(x) = x^4 + x^3 + x + 2$ *разложить на неприводимые множители над полем вычетов по модулю 3.*

Задача

Многочлен $f(x) = x^4 + x^3 + x + 2$ *разложить на неприводимые множители над полем вычетов по модулю 3.*

Решение

1. $0, 1, 2$ — *не корни* $f(x) \Rightarrow f(x)$ *линейных делителей не содержит.*
2. *Неприводимые многочлены над* $\mathbb{F}_3$ *степени 2:*

$$x^2 + 1,$$
$$x^2 + x + 2,$$
$$x^2 + 2x + 2.$$

3. *Подбором получаем:* $f(x) = (x^2 + 1)(x^2 + x + 2)$.

Ответ: $(x^2 + 1)(x^2 + x + 2)$.

Задача

Многочлен $x^4 + 3x^3 + 2x^2 + x + 4$ *разложить на неприводимые множители над полем вычетов по модулю 5.*

Задача

Многочлен $x^4 + 3x^3 + 2x^2 + x + 4$ разложить на неприводимые множители над полем вычетов по модулю 5.

Решение

1. *Убеждаемся, что многочлен $f(x) = x^4 + 3x^3 + 2x^2 + x + 4$ не имеет линейных делителей.*
2. *Перебирая неприводимые многочлены степени 2 над $\mathbb{F}_5$, получаем*

$$f(x) = (x^2 + x + 1)(x^2 + 2x + 4).$$

Задача

Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x.

Задача

Разложить на неприводимые множители над полем вычетов по модулю 2 все нормированные многочлены второй степени от x.

Решение

$$f_1 = x^2 = x \cdot x,$$
$$f_2 = x^2 + 1 = (x+1)^2,$$
$$f_3 = x^2 + x = x \cdot (x+1),$$
$$f_4 = x^2 + x + 1 - \textit{неприводим}.$$

Задача

Разложить на неприводимые множители над полем вычетов до модулю 2 все нормированные многочлены третьей степени от x.

Задача

Разложить на неприводимые множители над полем вычетов до модулю 2 все нормированные многочлены третьей степени от x.

Решение

$$f_1 = x^3,$$
$$f_2 = x^3 + 1 = (x+1)(x^2+x+1),$$
$$f_3 = x^3 + x = x(x+1)^2,$$
$$f_4 = x^3 + x^2 = x^2(x+1),$$
$$f_5 = x^3 + x + 1 - \textit{неприводим},$$
$$f_6 = x^3 + x^2 + 1 - \textit{неприводим},$$
$$f_7 = x^3 + x^2 + x = x(x^2+x+1),$$
$$f_8 = x^3 + x^2 + x + 1 = (x+1)^3.$$

Задача

Найти все нормированные многочлены второй степени от x, неприводимые над полем вычетов по модулю 3.

Задача

Найти все нормированные многочлены второй степени от x, неприводимые над полем вычетов по модулю 3.

Решение

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0.$

$$f_1 = x^2 + 1,$$
$$f_2 = x^2 + x + 2,$$
$$f_3 = x^2 + 2x + 2.$$

Задача

Найти все нормированные многочлены третьей степени от x, неприводимые над полем вычетов по модулю 3.

Задача

Найти все нормированные многочлены третьей степени от x, неприводимые над полем вычетов по модулю 3.

Решение

Должно быть: $f(0) \neq 0,\ f(1) \neq 0,\ f(2) \neq 0.$

$$f_1 = x^3 + 2x + 1,$$
$$f_2 = x^3 + 2x + 2,$$
$$f_3 = x^3 + x^2 + 2,$$
$$f_4 = x^3 + 2x^2 + 1,$$
$$f_5 = x^3 + x^2 + x + 2,$$
$$f_6 = x^3 + x^2 + 2x + 1,$$
$$f_7 = x^3 + 2x^2 + x + 1,$$
$$f_8 = x^3 + 2x^2 + 2x + 2.$$

Задача

1. *Проверить, что* $F = \mathbb{F}_7[x]/(x^2 + x - 1)$ *является полем.*
2. *Выразить обратный к* $1 - x$ *в* F *в базисе* $\{\overline{1}, \overline{x}\}$.

Задача

1. *Проверить, что* $F = \mathbb{F}_7[x]/(x^2 + x - 1)$ *является полем.*
2. *Выразить обратный к* $1 - x$ *в* F *в базисе* $\{\overline{1}, \overline{x}\}$.

Решение

1. $f(x) = x^2 + x - 1$, $f(0) = 6$, $f(1) = 1$, $f(2) = 5$, $f(3) = 4$, $f(4) = 6$, $f(5) = 1$, $f(6) = 6 \Rightarrow$
   многочлен $f(x)$ *— неприводим в* $\mathbb{F}_7$ *и* F *— поле* $(= \mathbb{F}_7^2)$.
2. $$\mathbb{F}_7^2 = \{ ax + b \mid a, b \in \mathbb{F}_7,\ x^2 = 1 - x = 6x + 1 \}$$
   $$(ax + b) \cdot (6x + 1) = \ldots = (2a + 6b)x + (6a + b) = 1$$
   $$\begin{cases} 6a + b = 1 \\ a + 3b = 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$
   Проверка: $(6x + 1)(x + 2) = 6x^2 + 13x + 2 = 1 + 7x = 1.$

Задача

Найти порядок элемента $x + x^2$ *в мультипликативной группе*

1. *поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$;
2. *поля* $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

Задача

Найти порядок элемента $x + x^2$ в мультипликативной группе

1. *поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$;
2. *поля* $\mathbb{F}_2[x]/(x^4 + x^3 + 1)$.

Решение

$x + x^2 = x(x + 1)$

1. $x^4 = x + 1$

$$(x^2 + x)^2 = x^4 + x^2 = x^2 + x + 1,$$
$$(x^2 + x)^3 = x(x + 1)(x^2 + x + 1) = x(x^3 + 1) =$$
$$= x^4 + x = x + 1 + x = 1.$$

Ответ: 3.

2. $x^4 = x^3 + 1$

$$
\begin{aligned}
(x^2+x)^2 &= x^4 + x^2 = x^3 + x^2 + 1,\\
(x^2+x)^3 &= x(x+1)(x^3+x^2+1) = x(x^4+x^2+x+1) =\\
&= x(x^3+x^2+x) = x^4 + x^3 + x^2 = x^2 + 1,\\
(x^2+x)^4 &= (x^2+x)(x^2+x)^3 = (x^2+x)(x^2+1) =\\
&= x^4 + x^2 + x^3 + x = x^3 + 1 + x^2 + x^3 + x =\\
&= x^2 + x + 1,\\
&\dots
\end{aligned}
$$

Задача

Найти количество неприводимых многочленов

1. *степени 7 над полем* $\mathbb{F}_2$;
2. *степени 6 над полем* $\mathbb{F}_5$;
3. *степени 24 над полем* $\mathbb{F}_3$.

Задача

Найти количество неприводимых многочленов

1. *степени 7 над полем* $\mathbb{F}_2$;
2. *степени 6 над полем* $\mathbb{F}_5$;
3. *степени 24 над полем* $\mathbb{F}_3$.

Задача

Чему равно произведение всех ненулевых элементов поля $\mathbb{F}_2^6$*?*

Задача

Чему равно произведение всех ненулевых элементов поля $\mathbb{F}_2^6$*?*

Решение

Все ненулевые элементы поля $\mathbb{F}_2^6$ *являются корнями уравнения*

$$x^{2^6-1} - 1 = x^{63} - 1 = 0\,. \qquad (*)$$

По теореме Виета их произведение равно свободному члену, т.е. $-1 \equiv_2 1$.

Задача

Чему равна сумма всех элементов поля $\mathbb{F}_{37}$.

Задача

Чему равна сумма всех элементов поля $\mathbb{F}_{37}$.

Решение

Все элементы поля $\mathbb{F}_2^6$ *являются корнями уравнения*

$$x^{37} - x = 0\,. \qquad (*)$$

По теореме Виета их сумма равна коэффициенту перед x^{36}, *т.е.* *0*.

Задача

Найти наименьшее поле характеристики 2, в котором многочлен $x^{19} - 1$ разлагается на линейные множители.

Задача

Найти наименьшее поле характеристики 2, в котором многочлен $x^{19} - 1$ *разлагается на линейные множители.*

Решение

$$x^{19} - 1 = (x+1)^{19}$$

Нужно найти наименьшее k *такое, что* $19 \mid (2^k - 1)$ *или* $2^k \equiv_{19} 1$ *или* $2^k = m \cdot 19 + 1$.
Такое k *нужно искать среди делителей* $19 - 1 = 18$.
Так как $29 = 2 \cdot 16^2 = 2 \cdot 9 = -1 (\mathrm{mod}\ 19)$, *а* $2^6 = 4 \cdot 2^4 = -12 (\mathrm{mod}\ 19)$, *то ни один собственный делитель 18 не подходит.*
Итого:

$$2^{18} = 19 \cdot 13797 + 1.$$

Ответ: $\mathbb{F}_{18}$.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач
5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация
6. Алгебраические решётки
   - Решётки

Две задачи

Есть набор сообщений $S_1, \ldots, S_t$, которые нужно передать по каналу связи.
Сообщения передаются в виде *кодовых слов* из нулей и единиц.

Две задачи

Есть набор сообщений $S_1, \ldots, S_t$, которые нужно передать по каналу связи.
Сообщения передаются в виде *кодовых слов* из нулей и единиц.
Ограничимся случаями, когда:

1. все сообщения кодируются словами одинаковой длины;
2. ошибки при передаче могут только изменять значения некоторых битов.

Две задачи

Есть набор сообщений $S_1, \ldots, S_t$, которые нужно передать по каналу связи.
Сообщения передаются в виде *кодовых слов* из нулей и единиц.
Ограничимся случаями, когда:

1. все сообщения кодируются словами одинаковой длины;
2. ошибки при передаче могут только изменять значения некоторых битов.

Задача (основная): построить код минимальной длины, позволяющий восстановить сообщение, содержащее не более r ошибок.

Две задачи

Есть набор сообщений $S_1, \ldots, S_t$, которые нужно передать по каналу связи.
Сообщения передаются в виде *кодовых слов* из нулей и единиц.
Ограничимся случаями, когда:

1. все сообщения кодируются словами одинаковой длины;
2. ошибки при передаче могут только изменять значения некоторых битов.

Задача (основная): построить код минимальной длины, позволяющий восстановить сообщение, содержащее не более r ошибок.

Задача (вспомогательная): даны

- n — длина кода,
- r — максимально допустимое число ошибок;

Требуется найти максимальное число k сообщений, которое можно передать.

Метрика на бинарных наборах

Точное решение вспомогательной задачи известно лишь для случаев

- $n = 2m - 1$, $r = 1$ и
- $n = 23$, $r = 3$.

Будем решать вспомогательную задачу приближённо.

Метрика на бинарных наборах

Точное решение вспомогательной задачи известно лишь для случаев

- $n = 2m - 1,\ r = 1$ и
- $n = 23,\ r = 3.$

Будем решать вспомогательную задачу приближённо.

Норма $\|\gamma\|$ — число единичных координат в $\widetilde{\gamma}$.
Метрика (вспоминаем, что это такое) на множестве бинарных наборов — Хемингово расстояние ($\oplus$ — сумма по $\bmod 2$):

$$\rho(\widetilde{\alpha}, \widetilde{\beta}) \;=\; \|\widetilde{\alpha} \oplus \widetilde{\beta}\|.$$

Шар Хэмминга с центром в $\widetilde{\alpha}$ и радиусом r —

$$S_r(\widetilde{\alpha}) \stackrel{\text{def}}{=} \{\, \widetilde{\beta} \mid \rho(\widetilde{\alpha}, \widetilde{\beta}) \leqslant r \,\}.$$

Групповые коды

Бóльшая часть теории кодирования построена на т.н. *линейных* или *групповых кодах* — кодах, образующих группу относительно $\oplus$.

Групповые коды

Бóльшая часть теории кодирования построена на т.н. *линейных* или *групповых кодах* — кодах, образующих группу относительно $\oplus$.

Утверждение

Устойчивая совокупность кодовых слов $C = \{\widetilde{\alpha}^1, \ldots, \widetilde{\alpha}^q\}$ *образует группу по сложению относительно операции* $\oplus$.

Групповые коды

Бóльшая часть теории кодирования построена на т.н. *линейных* или *групповых кодах* — кодах, образующих группу относительно $\oplus$.

Утверждение

Устойчивая совокупность кодовых слов $C = \{\widetilde{\alpha}^1, \ldots, \widetilde{\alpha}^q\}$ *образует группу по сложению относительно операции* $\oplus$.

Доказательство

Устойчивость: *для любых кодовых слов* $\widetilde{\alpha}^i, \widetilde{\alpha}^j \in C$ *выполняется* $\widetilde{\alpha}^i \oplus \widetilde{\alpha}^j = \widetilde{\alpha}^t \in C$, $1 \leqslant t \leqslant q$ — *предполагается;*

Ассоциативность: *свойство операции* $\oplus$*;*

Существование 0: $\widetilde{\alpha} \oplus \widetilde{\alpha} = (0, \ldots, 0) \stackrel{\text{def}}{=} \widetilde{0}$;

Противоположные элементы: $\neg(\widetilde{\alpha}) = \widetilde{\alpha}$ — *см. выше.*

Минимальное расстояние между кодовыми словами

Теорема

Минимальное расстояние между кодовыми словами обладает свойством

$$\min_{\widetilde{\alpha}\neq\widetilde{\beta}} \rho\left(\widetilde{\alpha},\widetilde{\beta}\right) = \min_{\widetilde{\gamma}\neq\widetilde{0}} \| \widetilde{\gamma} \| .$$

Минимальное расстояние между кодовыми словами

Теорема

Минимальное расстояние между кодовыми словами обладает свойством

$$\min_{\widetilde{\alpha}\neq\widetilde{\beta}} \rho\left(\widetilde{\alpha},\widetilde{\beta}\right) = \min_{\widetilde{\gamma}\neq\widetilde{0}} \| \widetilde{\gamma} \| .$$

Доказательство

$\rho\left(\widetilde{\alpha},\widetilde{\beta}\right) = \| \widetilde{\alpha} \oplus \widetilde{\beta} \| = \| \widetilde{\gamma} \|$, *причем* $\widetilde{\gamma} \neq \widetilde{0}$ *при* $\widetilde{\alpha} \neq \widetilde{\beta}$.

Отсюда получаем оценку

$$\min_{\widetilde{\alpha}\neq\widetilde{\beta}} \rho\left(\widetilde{\alpha},\widetilde{\beta}\right) \geqslant \min_{\widetilde{\gamma}\neq\widetilde{0}} \| \widetilde{\gamma} \| .$$

Эта оценка достигается, например, при $\widetilde{\beta} = \widetilde{0}$.

Кодовое расстояние

Определение

Минимальное расстояние между словами кода называется *кодовым расстоянием*.

Утверждение

Множество C *образует код с исправлением не более* r *ошибок, если* $S_r(\widetilde{\alpha}) \cap S_r(\widetilde{\beta}) = \varnothing$ *для всех* $\widetilde{\alpha}, \widetilde{\beta} \in C$ *таких, что* $\widetilde{\alpha} \neq \widetilde{\beta}$.

Кодовое расстояние

Определение

Минимальное расстояние между словами кода называется *кодовым расстоянием*.

Утверждение

Множество C образует код с исправлением не более r ошибок, если $S_r(\widetilde{\alpha}) \cap S_r(\widetilde{\beta}) = \varnothing$ для всех $\widetilde{\alpha}, \widetilde{\beta} \in C$ таких, что $\widetilde{\alpha} \neq \widetilde{\beta}$.

Доказательство

Если при передаче сообщения $\widetilde{\alpha}$ сделано не более r ошибок, то набор останется в шаре $S_r(\widetilde{\alpha})$.

Если шары не пересекаются, по любой точке данного шара восстанавливается его центр.

Плотная упаковка шаров в булев куб

Следствие

У кода, исправляющего r ошибок, кодовое расстояние не меньше $2r + 1$.

Чтобы построить код максимального размера, исправляющий r ошибок, нужно вложить в множество всех бинарных наборов E^n (булев куб) максимальное число непересекающихся шаров Хэмминга радиуса r.

Вопрос: При каких n и r в куб E^n можно уложить непересекающиеся шары радиуса r «без остатка»?

Ответ: Такое возможно лишь в двух случаях:

1. $n = 2^m - 1$, $r = 1$;
2. $n = 23$, $r = 3$.

Количество кодовых слов

Теорема (Хэмминга)

При $2r < n$ максимальное число k кодовых слов находится в пределах

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}} \leqslant k \leqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}}.$$

Количество кодовых слов

Теорема (Хэмминга)

При $2r < n$ максимальное число k кодовых слов находится в пределах

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}} \leqslant k \leqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}}.$$

Доказательство

k есть максимальное число непересекающихся шаров радиуса r, помещающихся в кубе E^n.

Шар радиуса r содержит точки: сам центр и все точки с одной, двумя, ..., r измененными координатами; т.е. всего $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots, \binom{n}{r}$ штук.

Так как шары не пересекаются, получаем верхнюю оценку.

Продолжение доказательства

Для оценки снизу построим негрупповой код:

1. *берем произвольную точку* E^n *и строим вокруг неё шар радиуса* $2r$*;*
2. *берем произвольную точку вне построенного шара и строим вокруг неё шар радиуса* $2r$*;*
3. *и т.д., каждая новая точка выбирается вне построенных шаров.*

Имеем:

- *шары, возможно, пересекаются, но каждый шар занимает* $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}$ *точек, и, следовательно, шаров не менее*
$$\frac{2^n}{\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{2r}};$$
- *шары радиуса* r *с центрами в выбранных точках не пересекаются.*

Случай $n = 2^m - 1$, $r = 1$

Покажем, что в данном случае $k = \frac{2^n}{1+n}$, т.е. верхняя оценка в теореме Хэмминга достигается.

Построим код, а потом определим его кодовое расстояние.

Рассмотрим таблицу:

$$
\left.
\begin{array}{ll}
100\ldots000 & 1100\ldots000 \\
010\ldots000 & 1010\ldots000 \\
001\ldots000 & 1001\ldots000 \\
\ldots & \ldots \\
000\ldots100 & 1111\ldots101 \\
000\ldots010 & 1111\ldots110 \\
000\ldots001 & 1111\ldots111
\end{array}
\right\} 2^m-(m+1)
$$

$\underbrace{\qquad\qquad}_{2^m-(m+1)}$ $\underbrace{\qquad\qquad}_{m}$

Слева — единичная матрица порядка $2^m - (m+1)$, справа — все бинарные наборы длины m, содержащие не менее двух единиц.

Случай $n = 2^m - 1$, $r = 1$: код Хэмминга

Просуммируем всевозможные совокупности строк этой таблицы, получив всего $2^{2^m-(m+1)}$ наборов. Заметим, что

$$2^{2^m-(m+1)} = \frac{2^{2^m-1}}{2^m} = \frac{2^n}{n+1}.$$

Легко видеть, что если суммируем

две строки — в левой части будет две единицы, а в правой — хотя бы одна;

не менее трёх строк — в левой части будет не менее трех единиц;

т.е. всегда $\rho(\widetilde{\alpha}, \widetilde{\beta}) > 3$

и шары радиуса 1 с центрами в этих наборах не пересекаются.

Случай $n = 2^m - 1$, $r = 1$: код Хэмминга длины 7 ($m = 3$)

Пример

Составим таблицу для кода Хэмминга длины 7:

1	0	0	0	1	1	0
0	1	0	0	1	0	1
0	0	1	0	0	1	1
0	0	0	1	1	1	1

Складывая по $\mathrm{mod}\,2$ произвольные совокупности строк, получаем 16 различных бинарных слов. Ими можно закодировать 16 сообщений —
например, 10 цифр|разделитель|$=|+|-|\times|\div$.

При передаче сообщений с помощью кода Хэмминга можно исправить одну ошибку.

Случай $n = 23$, $r = 3$

В этом случае верхняя граница числа вложенных шаров радиуса 3 в куб 23-мерный единичный куб

$$\frac{2^{23}}{1 + 23 + \frac{23 \cdot 22}{2} + \frac{23 \cdot 22 \cdot 21}{6}} = \frac{2^{23}}{2048} = \frac{2^{23}}{2^{11}} = 2^{12} = 4096$$

достигается — имеем плотную упаковку, как и в ранее рассмотренных случаях.

Других пар n и r, удовлетворяющих условию

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}} \text{ — целое}$$

неизвестно.

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач

5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация

6. Алгебраические решётки
   - Решётки

Циклические коды: определение

Определение

Код C называется *циклическим*, если он инвариантен относительно циклических сдвигов: из того, что набор $(\alpha_0, \ldots, \alpha_{n-1}) \in C$, следует, что и всякий набор $(\alpha_s, \alpha_{s+1}, \ldots, \alpha_{n-1}, \alpha_0, \ldots, \alpha_{s-1}) \in C$.

Ранее рассматривались было показано:

- В кольце $\mathbb{F}_p/(x^n - 1)$, рассматриваемом как векторное пространство над полем $\mathbb{F}_p$, есть базис $\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$. Циклический сдвиг координат в этом базисе равносилен умножению на x.
- Теорема: *Подпространство $I \subseteq \mathbb{F}_p/(x^n - 1)$ является циклическим iff I — идеал в $\mathbb{F}_p/(x^n - 1)$.*

Циклические коды: построение

Поэтому построить циклический код можно так:

- рассмотрим многочлен $x^n - 1$ и выберем некоторый его делитель $\varphi(x)$;
- в кольце $\mathbb{F}_2[x]/(x^n - 1)$ образуем идеал $(\varphi(x))$.

Оказывается, при удачном выборе $\varphi(x)$ коэффициенты многочленов, принадлежащих этому идеалу, будут давать хороший код.
Есть только несколько конструкций циклических кодов с хорошими параметрами.

Вопрос о кодовом расстоянии произвольного циклического кода чрезвычайно труден.

Циклические коды: пример построения

Пример

Пусть $n = 7$. Разложение на неприводимые множители:

$$x^7 - 1 = (1 + x)(1 + x^2 + x^3)(1 + x + x^3).$$

Циклические коды: пример построения

Пример

Пусть $n = 7$. Разложение на неприводимые множители:

$$x^7 - 1 = (1 + x)(1 + x^2 + x^3)(1 + x + x^3).$$

В качестве φ возьмем последний множитель, $\deg \varphi = 3$. Умножая его на степени x (циклически сдвигая 3 раза) получим базис в подпространстве, которое является кодом:

$$\begin{aligned}(1101000) &\leftrightarrow \varphi \\ (0110100) &\leftrightarrow \varphi \cdot x \\ (0011010) &\leftrightarrow \varphi \cdot x^2 \\ (0001101) &\leftrightarrow \varphi \cdot x^3\end{aligned}$$

Можно проверить, что кодовое расстояние для этого кода равно 3.

Раздел I

Раздел II

- Коды БЧХ

4 Теория перечисления Пойа
- Действие группы на множестве
- Применение леммы Бернсайда для решения комбинаторных задач

5 Частично упорядоченные множества
- Частично упорядоченные множества
- Операции над ч.у. множествами
- Линеаризация

6 Алгебраические решётки
- Решётки

Коды БЧХ — коды длины $n = 2^k - 1$

Рассмотрим коды длины $n = 2^k - 1$.
Рассматриваемый далее способ построения «хорошего» кода, исправляющего «много» ошибок предложили Радж Чандра Боуз и Двайджендра Камар Рей-Чоудхури в 1959 г. и независимо Алексис Хоквингем в 1960 г.

Поэтому коды, которые мы рассмотрим, называются *кодами Боуза-Чоудхури-Хоквингема* или *БЧХ-кодами* (BCH, Bose-Chaudhuri-Hocquenghem) — это класс циклических кодов, исправляющих кратные (2 и более) ошибки.
Теоретически коды БЧХ могут исправлять произвольное количество ошибок, но при этом существенно увеличивается длина кодового слова (что приводит к уменьшению скорости передачи данных и усложнению приемо-передающей аппаратуры).

Коды Хэмминга — частный случай БЧХ-кодов.

Уточнение описанной выше схемы при $n = 2^k - 1$ —

— конкретизирующей выбор идеала.

1. Строим поле $\mathbb{F}_2^n = \mathbb{F}_2/(f)$, f — неприводимый многочлен.
2. Элементы $\mathbb{F}_2^{n*}$ образуют циклическую группу по умножению.
3. Выберем порождающий элемент $\alpha \in \mathbb{F}_2^{n*}$ и рассмотрим его степени
$$\alpha,\ \alpha^2,\ \ldots,\ \alpha^{2r},$$
где r — число ошибок, которые нужно уметь исправлять.
4. В разложении многочлена $x^n - 1$ выберем такие неприводимые многочлены, чтобы каждая из указанных степеней была корнем одного из них.
φ есть результат перемножения этих многочленов.
Коды — коэффициенты многочленов из идеала (φ).

Оказывается (далее будет доказано), что это гарантирует исправление r ошибок.

Построение кода БЧХ, исправляющего 3 ошибки

Пример ($k = 4$, многочлен для разложения: $x^{15} - 1$)

Пусть нужен код, исправляющий $r = 3$ ошибки. Значит, нужно найти многочлены, корнями которых являются первые $2r = 6$ степеней порождающего элемента α.

	если многочлен имеет корень	то он имеет корни
1	α	α^2, α^4, α^8
2	α^3	α^6, α^{12}, α^9 $(= \alpha^{24})$
3	α^5	α^{10}

По трём наборам корней построим три многочлена, два — 4-й степени и один — 2-й. Перемножив их, получим многочлен 10-й степени.

Идеал по модулю этого многочлена будет 5-мерным пространством.

Сколько элементов содержит идеал (φ)?

- $\varphi =$ произведение некоторых неприводимых многочленов-делителей $x^n - 1$.
- Каждый делитель имеет, как минимум, 2 корня из совокупности $\{\alpha, \ldots, \alpha^{2r}\}$, т.е. их требуется не более r штук.
- Если делитель имеет корнями s элементов $\{\alpha^m, \alpha^{2m}, \ldots, \alpha^{2^s m}\}$, то $2^s \leqslant n = 2^k - 1$, т.е. степень каждого делителя не более $k = \log_2(n+1)$.
- $\deg\varphi \leqslant rk = r\log_2(n+1)$.
- Идеал, порожденный φ, имеет размерность $n - \deg\varphi$.
- $|(\varphi)| \leqslant 2^{n - r\log_2(n+1)} = \frac{2^n}{(n+1)^r}$.

Ясно, что эта оценка далека от точности.

Сколько элементов содержит идеал (φ)?

- $\varphi =$ произведение некоторых неприводимых многочленов-делителей $x^n - 1$.
- Каждый делитель имеет, как минимум, 2 корня из совокупности $\{\alpha, \ldots, \alpha^{2r}\}$, т.е. их требуется не более r штук.
- Если делитель имеет корнями s элементов $\{\alpha^m, \alpha^{2m}, \ldots, \alpha^{2^s m}\}$, то $2^s \leqslant n = 2^k - 1$, т.е. степень каждого делителя не более $k = \log_2(n+1)$.
- $\deg\varphi \leqslant rk = r\log_2(n+1)$.
- Идеал, порожденный φ, имеет размерность $n - \deg\varphi$.
- $|(\varphi)| \leqslant 2^{n - r\log_2(n+1)} = \frac{2^n}{(n+1)^r}$.

Ясно, что эта оценка далека от точности.

Оценка кодового расстояния

Покажем, что расстояние между точками кода не меньше, чем $2r + 1$ (что нам и требуется!).

Оценка кодового расстояния

Покажем, что расстояние между точками кода не меньше, чем $2r+1$ (что нам и требуется!).

Все многочлены, входящие в наш код — в идеал (φ) —, кратны $\varphi \Rightarrow$ каждый кодовый многочлен имеет корни $\alpha, \alpha^2, \ldots, \alpha^{2r}$ (как и φ).

Кодовое расстояние $= \min \|\widetilde{\gamma}\|$, $\widetilde{\gamma}$ — элемент кода.

Значит, надо доказать следующее

Утверждение

Если многочлен $\psi \in (\varphi)$ имеет корни α^s, $s = 1, \ldots, 2r$, то у ψ не менее $2r+1$ ненулевого коэффициента.

Оценка кодового расстояния...

Доказательство

Рассмотрим многочлен

$$\psi(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1},$$

удовлетворяющий указанному условию.
Коэффициенты $\psi(x)$ *составляют решение следующей системы линейных уравнений:*

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \ldots & (\alpha^2)^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{2r} & (\alpha^{2r})^2 & \ldots & (\alpha^{2r})^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \ldots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}.$$

Если набор $a = (a_0, \ldots, a_{n-1})$ — решение указанной системы, то между $\|a\|$ столбцами матрицы системы есть линейная зависимость. Поэтому достаточно показать, что любые $2r$ столбцов этой матрицы линейно независимы.

Теория решения СЛАУ конечным полем ничем не отличается от привычной теории решения СЛАУ над $\mathbb{R}$ (она вовсе не зависит от поля задания).

В частности, линейная зависимость между столбцами квадратной матрицы равносильна обращению в нуль определителя этой матрицы.

Нам требуется показать, что в a не менее $2r + 1$ ненулевых элементов $\Rightarrow$ выберем из матрицы столбцы $j_1, j_2, \ldots, j_{2r}$.

Получим квадратную матрицу

$$\begin{pmatrix} \alpha^{j_1} & \alpha^{j_2} & \dots & \alpha^{j_{2r}} \\ (\alpha^2)^{j_1} & (\alpha^2)^{j_2} & \dots & (\alpha^2)^{j_{2r}} \\ \dots & \dots & \dots & \dots \\ (\alpha^{2r})^{j_1} & (\alpha^{2r})^{j_2} & \dots & (\alpha^{2r})^{j_{2r}} \end{pmatrix}$$

Вынесем из всех элементов столбца t *общий множитель* α^{j_t}. *Получим, что определитель нашей матрицы с точностью до ненулевого множителя* $\alpha^{j_1+j_2+\dots+j_{2r}}$ *равен*

$$V = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \dots & \alpha^{j_{2r}} \\ (\alpha^{j_1})^1 & (\alpha^{j_2})^2 & \dots & (\alpha^{j_{2r}})^2 \\ \dots & \dots & \dots & \dots \\ (\alpha^{j_1})^{2r-1} & (\alpha^{j_2})^{2r-1} & \dots & (\alpha^{j_{2r}})^{2r-1} \end{vmatrix}.$$

Это хорошо известный определитель Вандермонда. Вычисляется он над конечным полем точно так же, как и над $\mathbb{R}$:

$$V = \prod_{t_1 < t_2} \left(\alpha^{j_{t_2}} - \alpha^{j_{t_1}} \right).$$

В качестве α взят порождающий элемент мультипликативной группы поля $\mathbb{F}_2^{2*}$, поэтому все степени α вплоть до $(n-1)$-й различны.
Поэтому $V \neq 0$.

Это хорошо известный определитель Вандермонда. Вычисляется он над конечным полем точно так же, как и над $\mathbb{R}$:

$$V = \prod_{t_1 < t_2} \left(\alpha^{j_{t_2}} - \alpha^{j_{t_1}}\right).$$

В качестве α взят порождающий элемент мультипликативной группы поля $\mathbb{F}_2^{2*}$, поэтому все степени α вплоть до $(n-1)$-й различны.
Поэтому $V \neq 0$.

Утверждение доказано: расстояние между кодовыми словами не меньше $2r+1 \Rightarrow$ построенный код действительно исправляет r ошибок.

Что дальше?

- Для выбора минимальных многочленов при построении БЧХ-кодов составлены специальные таблицы.
- Для декодирования БЧХ-кодов используют специально разработанные эффективные алгоритмы (например, алгоритм Питерсона-Горенстейна-Цирлера).
- Широко используемым подмножеством кодов БЧХ являются *коды Рида-Соломона*, которые позволяют исправлять *пакеты ошибок*.
  Пакет ошибок представляет собой вектор ошибок (1 — символ ошибочен, 0 — нет) таких, что первый и последний из них отличны от нуля.

Раздел I

Раздел II

- Коды БЧХ

4 Теория перечисления Пойа

- Действие группы на множестве
- Применение леммы Бернсайда для решения комбинаторных задач

5 Частично упорядоченные множества

- Частично упорядоченные множества
- Операции над ч.у. множествами
- Линеаризация

6 Алгебраические решётки

- Решётки

Действие группы на множестве: два определения

- Группа $\mathbb{G} = \langle G, \circ, e \rangle$, $|G| = n$.
- Множество T, $|T| = N$.
  - $Bij(T)$ — множество всех биекций на T.
  - $Symm(T)$ — симметрическая группа множества T:

$$Symm(T) = \langle Bij(T), *, 1_T \rangle,$$

- Действие α группы $\mathbb{G}$ на множестве T — $\mathbb{G} \underset{\alpha}{:} T$.

  Два определения.

Определение (1)

$$\alpha \in \mathrm{Hom}\ (\mathbb{G}, Symm(T)).$$

Действие группы на множестве: два определения...

Определение (2)

$$\alpha = \langle \mathbb{G}, T, \circ, *, e, 1_T \rangle,$$

где

- $G \times G \xrightarrow{\circ} G$ — групповая операция;
- $G \times T \xrightarrow{*} T$ — новая операция.

Аксиомы для операций:

- $e * t = t$;
- $(g \circ h) * t = h * (g * t)$.

Запись операции $*$: $g(t) = t'$.

Аксиомы: $e(t) = t$ и $(g \circ h)(t) = h(g(t))$.

Т.е. g — *перестановки* на T, обладающие вышеуказанными свойствами.

Для данной перестановки g:

Введём отношение эквивалентности $\sim_g$ на T —

$$t \sim_g t' \stackrel{\text{def}}{=} \exists\, k \left(g^k(t) = t' \right).$$

Классы эквивалентности называют *g-циклами*. Всего $C(g)$ классов.

Количества циклов длины $1, 2, \ldots, N$ обозначают $\nu_1, \nu_2, \ldots, \nu_N$ или $\nu_1(g), \nu_2(g), \ldots, \nu_N(g)$.

Их упорядоченную совокупность, записанную как

$$Type(g) = \langle \nu_1, \nu_2, \ldots, \nu_N \rangle \quad \text{или} \quad \langle 1^{\nu_1}, 2^{\nu_2}, \ldots, N^{\nu_N} \rangle$$

называют *типом перестановки g*.

Понятно, что $C(g) = \sum\limits_{k=1}^{N} \nu_k(g)$ и $\sum\limits_{k=1}^{N} k \cdot \nu_k(g) = N$.

Пример

Пусть

$$T = \{1, \ldots, 10\},$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} =$$

$$= (1,9,3)(2,6)(4,8,10)(5)(7)$$

Тогда $Type(g) = \langle 1^2, 2^1, 3^2, 4^0, \ldots, 10^0 \rangle = \langle 2, 1, 2, 0, \ldots, 0 \rangle$
и $C(g) = 5$.

По всей группе $\mathbb{G}$:

Отношение эквивалентности $\sim_{\mathbb{G}}$ на T —

$$t \sim_{\mathbb{G}} t' \stackrel{\text{def}}{=} \exists\limits_{G} g \left(g(t) = t' \right).$$

Классы этой эквивалентности называют *орбитами*.
Число орбит (классов эквивалентности) — $C(\mathbb{G})$.
Если $C(\mathbb{G}) = 1$ (любой элемент T может быть переведён в любой), то действие $\mathbb{G} \underset{\alpha}{:} T$ называют *транзитивным*.

Класс эквивалентности, в которую попадает элемент t будем обозначать $\mathrm{Orb}\,(t)$.

Неподвижные точки группы преобразований $\mathbb{G}$: $g(t) = t$

При выполнении этого равенства можно фиксировать t или g.

1. Фиксируем g, т.е. находим все элементы множества T, которые перестановка g оставляет на месте:

$$\{\, t \in T \mid g(t) = t \,\} = \nu_1(g) \stackrel{\text{def}}{=} \operatorname{Fix}(g) \subseteq T\,.$$

2. Фиксируем t, т.е находим все перестановки g, которые оставляют данный элемент неподвижным:

$$\{\, g \in G \mid g(t) = t \,\} \stackrel{\text{def}}{=} \operatorname{Stab}(t) \subseteq G\,.$$

Справедливы равенства

$$C(\mathbb{G}) = \frac{1}{|G|} \sum_{g \in G} \Big| \operatorname{Fix}(g) \Big| = \frac{1}{|G|} \sum_{t \in T} \Big| \operatorname{Stab}(t) \Big|\,.$$

Первое равенство называется *леммой Бернсайда* (1911).

Стабилизатор есть подгруппа

1. $\mathrm{Fix}\,(g)$ — стабилизатор перестановки g;
2. $\mathrm{Stab}\,(t)$ — стабилизатор элемента t.

Лемма

$$\mathrm{Stab}\,(t) \leqslant \mathbb{G}.$$

Доказательство

Зафиксируем $t \in T$ *и рассмотрим* $g, h \in \mathrm{Stab}\,(t)$. *Тогда* $g(t) = h(t) = t$ *и* $h^{-1}(t) = 1$. *Следовательно,*

$$(g \circ h^{-1}) * t = t \Rightarrow g \circ h^{-1} \in \mathrm{Stab}\,(t)\,.$$

$|\mathrm{Stab}\,(t)| \geqslant 1$, поскольку всегда $e \in \mathrm{Stab}\,(t)$.

Стабилизатор

Лемма

Длина орбиты $\mathrm{Orb}\,(t)$ *равна индексу* $\mathrm{Stab}\,(t)$ *в группе* $\mathbb{G}$, *т.е.*

$$|\,\mathrm{Orb}\,(t)| \;=\; |G| : |\,\mathrm{Stab}\,(t)|\,.$$

Пример

O — группа вращений куба (*группа октаэдра*). Найти $\mathrm{Stab}\,(t)$.

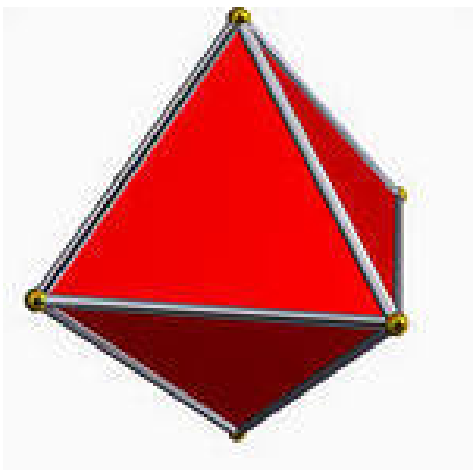
Решение: $\mathrm{Stab}\,(t) \;\cong\; \mathbb{Z}_3$ — группа вращений на 120° вокруг диагонали куба, проходящей через данную вершину.

Утверждение

Число элементов в группе вращения правильного многогранника есть $|V| \cdot |E_0|$, *где* $|V|$ — *число вершин, а* $|E_0|$ — *число рёбер, выходящих из одной вершины.*

Платоновы тела (правильные 3-х мерные многогранники)

Платоновы тела	Группа симметрии	Порядок группы
тетраэдр	T	$4 \cdot 3 = 12$
куб и октаэдр	O	$8 \cdot 3 = 24$
икосаэдр и додекаэдр	Y	$12 \cdot 5 = 60$



Октаэдр

Икосаэдр

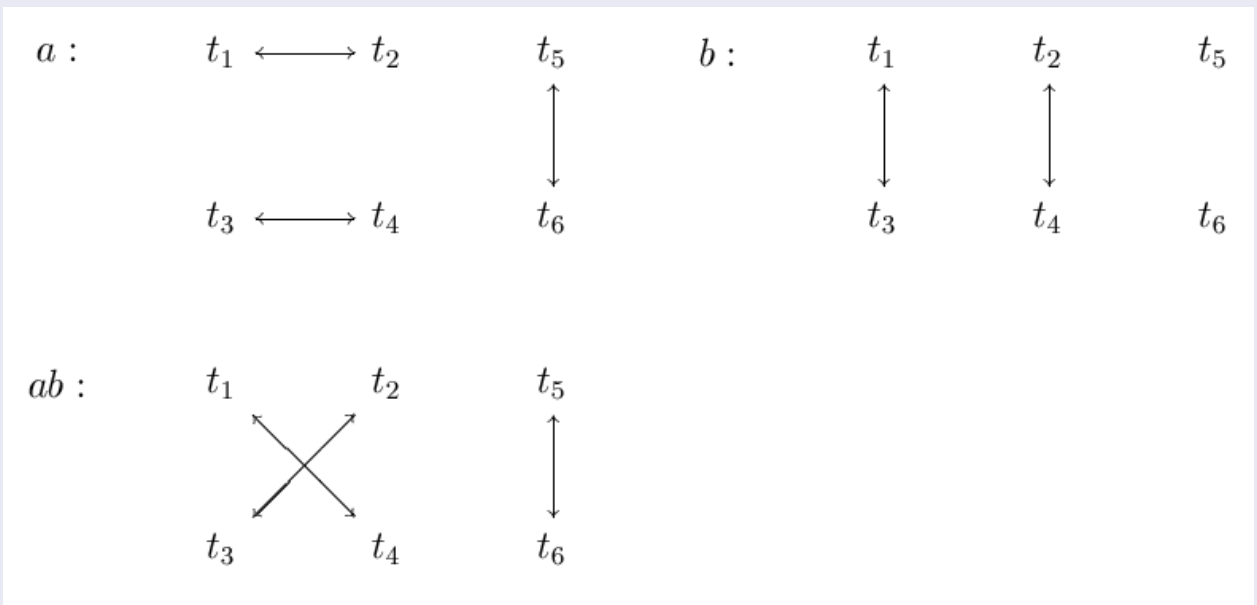
Додекаэдр

Пример

Действие группы V_4 на множестве $T = \{t_1, \dots t_6\}$

$\circ$	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

$g * t$	t_1	t_2	t_3	t_4	t_5	t_6
e	t_1	t_2	t_3	t_4	t_5	t_6
a	t_2	t_1	t_4	t_3	t_6	t_5
b	t_3	t_4	t_1	t_2	t_5	t_6
ab	t_4	t_3	t_2	t_1	t_6	t_5



$$Type(e) = \langle 6, 0, 0, 0, 0, 0 \rangle, \qquad Type(a) = \langle 0, 3, 0, 0, 0, 0 \rangle,$$
$$Type(b) = \langle 2, 2, 0, 0, 0, 0 \rangle, \qquad Type(ab) = \langle 0, 3, 0, 0, 0, 0 \rangle.$$
$$C(e) = 6\,,\ C(a) = C(ab) = 3\,,\ C(b) = 4\,.$$
$$\mathrm{Stab}\,(t_1) = \mathrm{Stab}\,(t_2) = \mathrm{Stab}\,(t_3) = \mathrm{Stab}\,(t_4) = e \leqslant V_4\,,$$
$$\mathrm{Stab}\,(t_5) = \mathrm{Stab}\,(t_6) = \langle e, b \rangle \leqslant V_4\,.$$
$$\mathrm{Fix}\,(a) = \mathrm{Fix}\,(ab) = \varnothing\,, \quad \mathrm{Fix}\,(b) = \{ t_5, t_6 \}\,, \quad \mathrm{Fix}\,(e) = T\,.$$
$$|\,\mathrm{Orb}\,(t_1)| = \frac{4}{1} = 4\,, \quad |\,\mathrm{Orb}\,(t_5)| = \frac{4}{2} = 2\,.$$
$$\frac{1}{4} \sum_{g \in G} |\,\mathrm{Fix}\,(g)| = \frac{6+2}{4} = 2\,,$$
$$\frac{1}{4} \sum_{t \in T} |\,\mathrm{Stab}\,(t)| = \frac{4 \cdot 1 + 2 \cdot 2}{4} = 2\,.$$

Раздел I

Раздел II

Задача (про слова)

Составляются слова длины $l \geqslant 2$ из алфавита $A = \{a_1, \ldots, a_m\}$. Слова считаются эквивалентными, если они получаются одно из другого транспозицией крайних букв. Определить число S неэквивалентных слов.

Решение

T — множество слов длины l в алфавите A, $N = |T| = m^l$.
Надо представить эквивалентности как орбиты некоторого действия подходящей группы G на T.
Очевидно, $g^2 = e$ и поэтому подходит $G \cong \mathbb{Z}_2 = \{e, g\}$. Легко проверить, что выше определено действие $\mathbb{Z}_2$ на T.

Число S неэквивалентных слов есть число классов эквивалентности $C(G)$ действия $\mathbb{Z}_2 \underset{\alpha}{:} T$ —

$$|\operatorname{Fix}(e)| = |T| = m^l, \qquad |\operatorname{Fix}(g)| = m^{l-2} \cdot m = m^{l-1}.$$

$$S = C(\mathbb{Z}_2) = \frac{1}{2} \sum_{g \in G} |\operatorname{Fix}(g)| = \frac{m^l + m^{l-1}}{2} = \frac{m^{l-1}(m+1)}{2}.$$

Для $l = 3$, $m = 2 \Rightarrow S = \frac{4 \cdot 3}{2} = 6$ (из 8)
Пусть $A = \{a, b\}$. Показаны слов и классы.

aaa	-1	baa	-2
aab	-2	bab	-5
aba	-3	bba	-4
abb	-4	bbb	-6

Задача

Показать, что если элементы g и h группы G сопряжены, то $\mathrm{Stab}\,(g) = \mathrm{Stab}\,(h)$.

Решение

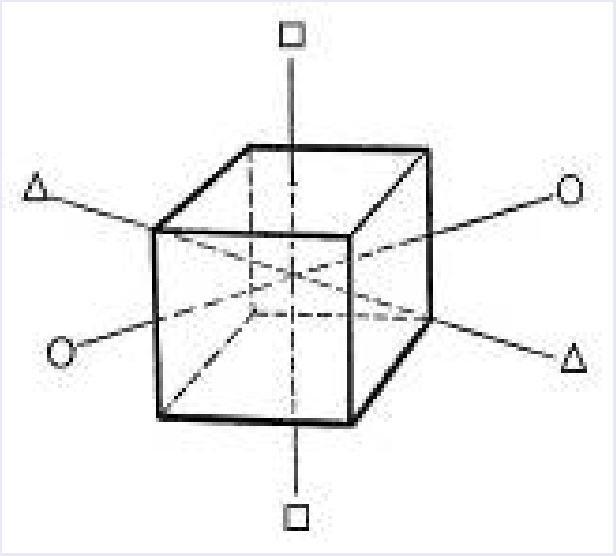
$$gf = fh \Rightarrow \mathrm{Stab}\,(gf) = \mathrm{Stab}\,(g) \cap \mathrm{Stab}\,(f) = \mathrm{Stab}\,(fh) =$$
$$= \mathrm{Stab}\,(f) \cap \mathrm{Stab}\,(h) \Rightarrow \mathrm{Stab}\,(g) = \mathrm{Stab}\,(h).$$

Задача

Группа вращений куба группу перестановок на множестве его вершин. Определить типы всех перестановок этой группы.

Решение

$O = \langle t, f, r \rangle, t^4 = f^2 = r^3 = e$, *где*

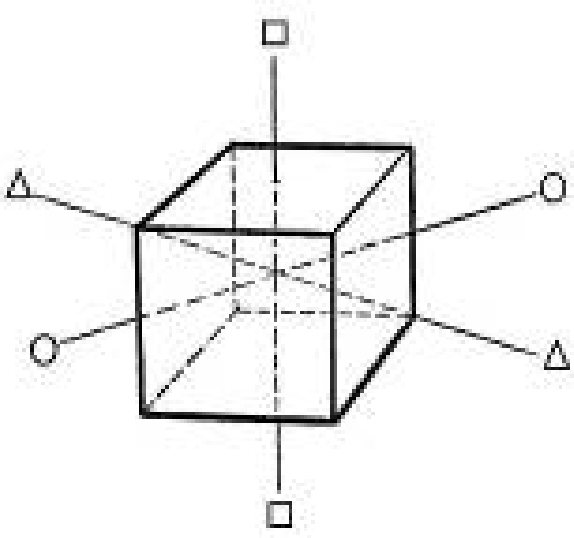


t — *вращение на* 90° *вокруг оси, проходящей через две противоположные грани* (□—□);

f — *вращение на* 180° *вокруг оси, проходящей через два противоположные ребра* (○—○);

r — *вращение на* 120° *вокруг оси, проходящей через две противоположные вершины* (△—△).

Имеем



$\square : Type(t) =$
$= Type(t^3) = \langle 0, 0, 0, 2, 0, \ldots \rangle,$
$Type(t^2) = \langle 0, 4, 0, \ldots \rangle;$

$\circ : Type(f) = \langle 0, 4, 0, \ldots \rangle;$

$\triangle$: $Type(r) = Type(r^2) = \langle 2, 0, 2, 0, \ldots \rangle.$

Цикловой индекс

Существует универсальный способ вычисления числа $\frac{1}{|G|}\sum\limits_{g\in G}\left|\operatorname{Fix}(g)\right| = C(\mathbb{G})$ классов эквивалентности(орбит).

Сопоставим каждой перестановке $g \in \mathbb{G}$ вес $w(g)$ по правилу:

$$Type(g) = \langle \nu_1, \ldots, \nu_N \rangle \;\Rightarrow\; w(g) = x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}.$$

$x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}$ — *моном*.

Определение

Средний вес подстановок в группе называется *цикловым индексом* действия $\mathbb{G} \underset{\alpha}{:} T$:

$$P(\mathbb{G} \underset{\alpha}{:} T, x_1, \ldots, x_N) = \frac{1}{|G|}\sum_{g\in G} w(g) = \frac{1}{|G|}\sum_{g\in G} x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}.$$

Для продвинутых: это (конечная) *производящая функция*.

Цикловой индекс: обозначения и свойсто

Другие обозначения: $P_{\mathbb{G}}(x_1, \ldots, x_N)$ и $P_{\mathbb{G}}$, $P(\mathbb{G})$.

- $\mathbb{G} \cong \mathbb{G}' \Rightarrow P_{\mathbb{G}} = P_{\mathbb{G}'}$ — да, если действия определены одинаково (согласовано)
- $P_{\mathbb{G}} = P_{\mathbb{G}'} \not\Rightarrow \mathbb{G} \cong \mathbb{G}'$ — нет, есть контрпример

Для применения универсального способа вычисления $C(\mathbb{G})$ надо представить эквивалентные элементы как классы эквивалентности, сохраняющие некоторые характеристики элементов при перестановках.

Число неэквивалентных раскрасок

Пусть задано действие $\mathbb{G} \underset{\alpha}{:} T$ группы $\mathbb{G}$ на множестве T.

- Припишем каждому элементу T одно из r значений — покрасим в один из r цветов. Всего возможно r^N различных раскрасок.
- Не будем различать раскраски, если при преобразовании $g : t \to t'$ элемент сохраняет цвет (t' раскрашен также как t'). Т.е. каждый g-цикл раскрашен одним способом.

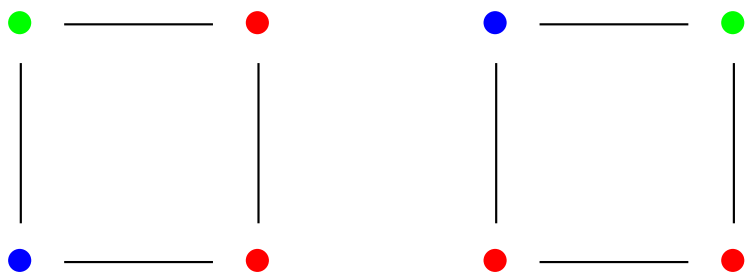


Рис. 1. Перестановка g — поворот на $+90°$

Вопрос: Сколько существует неэквивалентных раскрасок — классов эквивалентности $C(\mathbb{G})$?

Вычисление $C(\mathbb{G})$ через цикловой индекс

- Каждый класс эквивалентности это g-цикл; их $C(g) = \nu_1 + \ldots + \nu_N$ штук.
- Каждая перестановка $g \in \mathbb{G}$ с типом $\langle \nu_1, \ldots, \nu_N \rangle$ будет иметь $r^{C(g)}$ неподвижных точек.

Следовательно, по теореме Бернайса, число полученных классов эквивалентности, т.е. неэквивалентных раскрасок (приписываний) есть

Теорема

$$C(\mathbb{G} \underset{\alpha}{:} T) = P(\mathbb{G} \underset{\alpha}{:} T, r, \ldots, r).$$

Например, $P_{\mathbb{G}}(1, \ldots, 1) = 1$.

Пример

Задача (про слова)

Составляются слова длины $l \geqslant 2$ из алфавита $A = \{a_1, \ldots, a_m\}$. Слова считаются эквивалентными, если они получаются одно из другого транспозицией крайних букв. Определить число S неэквивалентных слов.

Было решение: $S = \frac{m^l + m^{l-1}}{2}$.

Другое решение: $\mathbb{G} = \{e, g\} \cong \mathbb{Z}_2$; T: $\underbrace{\bigcirc\overbrace{\bigcirc\ldots\bigcirc}^{l-2}\bigcirc}_{l}$.

Элемент группы g	$Type(g)$	$w(g)$	#мономов
e	$\langle l, 0, \ldots, 0 \rangle$	x_1^l	1
g	$\langle l-2, 1, 0, \ldots, 0 \rangle$	$x_1^{l-2}x_2^1$	1

Цикловой индекс: $P(x_1, \ldots, x_l) = \frac{x_1^l + x_1^{l-2}x_2^1}{2}$.

$P(x_1, \ldots, x_l)|_{x_1=\ldots=x_l=m} = S$.

Задача об ожерельях —

одна из классических комбинаторных задач.

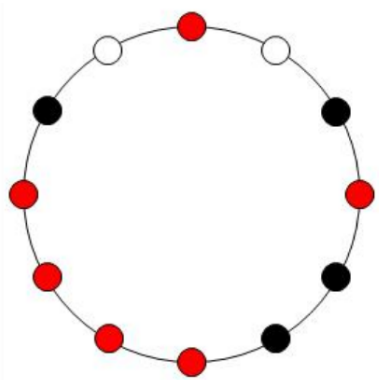
Ожерелье — окружность, на которой на равных расстояниях по дуге располагаются «бусины» (бусины располагаются в вершинах правильного многоугольника).

Задача (об ожерельях)

Сколько различных ожерелий можно составить из n бусин r цветов?

Варианты. Ожерелья равны если и только если одно получается из другого

1. *поворотом* (бусины плоские, окрашены с одной стороны);
2. *поворотом и осевой симметрией* (бусины круглые);



Задача об ожерельях: $N = 5, r = 3$

Задача

Сколько разных ожерелий можно составить из 5 бусин 3 цветов?

T — вершины правильного пятигольника. $\#Col(3) = ?$

1. Ожерелья одинаковы, если одно получается из другого поворотом

Решение

$\mathbb{G}$ — *группа вращения правильного пятигольника:* $\mathbb{G} \cong \mathbb{Z}_5 = \langle t \rangle$, $t^5 = e$, $n = 5$.

Элемент группы g	$Type(g)$	$w(g)$	*# мономов*
e	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
t, t^2, t^3, t^4	$\langle 0, 0, 0, 0, 1 \rangle$	x_5	4

Цикловой индекс: $P(x_1, x_2, x_3, x_4, x_5) = \frac{1}{5}[x_1^5 + 4x_5]$.

$$\#Col(3) = P(3, \ldots, 3) = \frac{3^5 + 4 \cdot 3}{5} = 51.$$

Задача Олимпиады «Покори Воробьёвы горы – 2009»

Для 50 детей детского сада закуплены 50 одинаковых тарелок. По краю каждой тарелки равномерно расположено 5 белых кружочков. Воспитатели хотят перекрасить какие-либо из этих кружочков в другой цвет так, чтобы все тарелки стали различными. Какое наименьшее число дополнительных цветов потребуется им для этого?

Решение (Как должны были решать дети)

Пусть требуется r цветов. Отбросим r вариантов раскраски в один цвет. Число остальных вариантов без учёта возможности поворота тарелки — $r^5 - r$; с учётом поворота — $\frac{r^5-r}{5}$ (каждый вариант повторятся 5 раз). Итого — $\#Col(r) = \frac{r^5-r}{5} + r = \frac{r^5+4r}{5}$; При 2-х дополнительных цветах $\#Col(3) = 51$.

Задача об ожерельях: $N = 5, r = 3$, 2-й вариант

2. Ожерелья одинаковы, если одно получается из другого поворотом или переворотом.

Решение

$\mathbb{G}$ — *группа диэдра*: $\mathbb{G} \cong D_5 = \langle t, f \rangle$, $t^5 = f^2 = e$, $n = |D_5| = 10$.

Элемент группы g	$Type(g)$	$w(g)$	*# мономов*
e	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
t, t^2, t^3, t^4	$\langle 0, 0, 0, 0, 1 \rangle$	x_5	4
$f, tf, \ldots, t^4 f$	$\langle 1, 2, 0, 0, 0 \rangle$	$x_1 x_2^2$	5
Итого			10

Цикловой индекс: $P = \frac{1}{10}\left[x_1^5 + 4x_5 + 5x_1x_2^2\right]$.

$$\#Col(3) = P(x_1, \ldots, x_5)|_{x_1=\ldots=x_5=3} = \frac{3^5 + 4 \cdot 3 + 5 \cdot 3^3}{10} = 39.$$

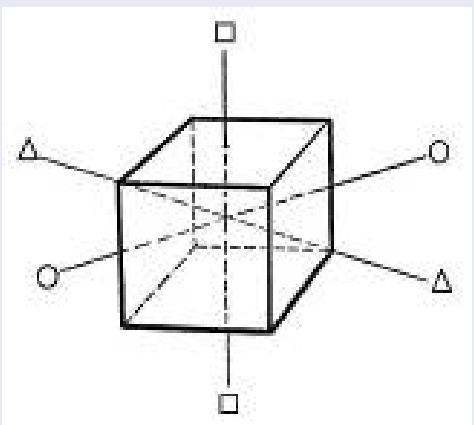
Задача о раскраске куба

Задача (раскраска куба в два цвета)

Грани куба раскрашивают в два цвета. Сколько существует различно окрашенных кубов?

Решение

$\mathbb{G} = O = \langle t, f, r \rangle$, $t^4 = f^2 = r^3 = e$, $|O| = 24$.



t — *вращение на* 90° *вокруг оси, проходящей через две противоположные грани* (□—□, *3 оси*);
f — *вращение на* 180° *вокруг оси, проходящей через два противоположные ребра* (○—○, *6 осей*);
r — *вращение на* 120° *вокруг оси, проходящей через две противоположные вершины* (△—△, *4 оси*).

Задача о раскраске куба в два цвета...

T — *множество граней куба,* $N = 6$.

Элемент группы g	$Type(g)$	$w(g)$	*# мономов*
e	$\langle 6, 0, 0, 0, 0, 0 \rangle$	x_1^6	1
t, t^3	$\langle 2, 0, 0, 1, 0, 0 \rangle$	$x_1^2 x_4$	$3 \cdot 2 = 6$
t^2	$\langle 2, 2, 0, 0, 0, 0 \rangle$	$x_1^2 x_2^2$	3
f	$\langle 0, 3, 0, 0, 0, 0 \rangle$	x_2^3	6
r, r^2	$\langle 0, 0, 2, 0, 0, 0 \rangle$	x_3^2	$4 \cdot 2 = 8$
Всего			24

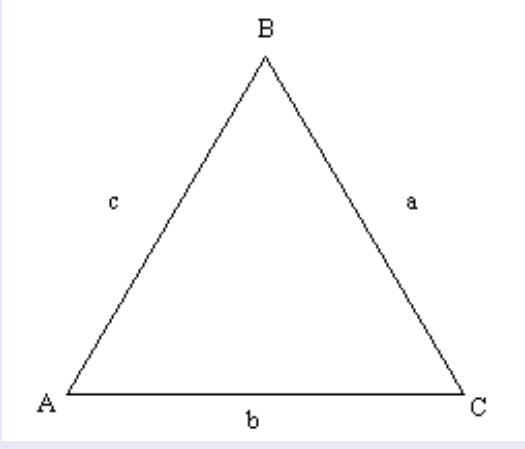
$$P = \frac{1}{24} \cdot \left[x_1^6 + 6x_1^2 x_4 + 3x_1^2 x_2^2 + 6x_2^3 + 8x_3^2 \right].$$

$$\#Col(2) = \frac{2^6 + 12 \cdot 2^3 + 3 \cdot 2^4 + 8 \cdot 2^2}{24} = 10.$$

Задача (Перечисление графов)

Сколько имеется ориентированных и неориентированных непомеченных графов (без петель и кратных рёбер) с тремя вершинами?

Решение



T — *стороны треугольника,* $N = 3$.

$\mathbb{G} \cong S_3$ — *все перестановки трёх вершин,*

$$n = 3! = 6.$$

$\mathbb{G} \underset{\alpha}{:} T$ — *действие перестановок вершин на стороны.*

Графы неориентированные — $r = 2$ — *пометки «есть ребро/нет ребра»*

ориентированные — $r = 3$ — *пометки «не ребра/ориентация ребра»*

$$S_3 = \{\, e,\ 2 * (ABC),\ 3 * ((A)(BC)) \,\}.$$

$$S_3 = \{ e,\ 2 * \underbrace{(ABC)}_{g_1},\ 3 * \underbrace{((A)(BC))}_{g_2} \}.$$

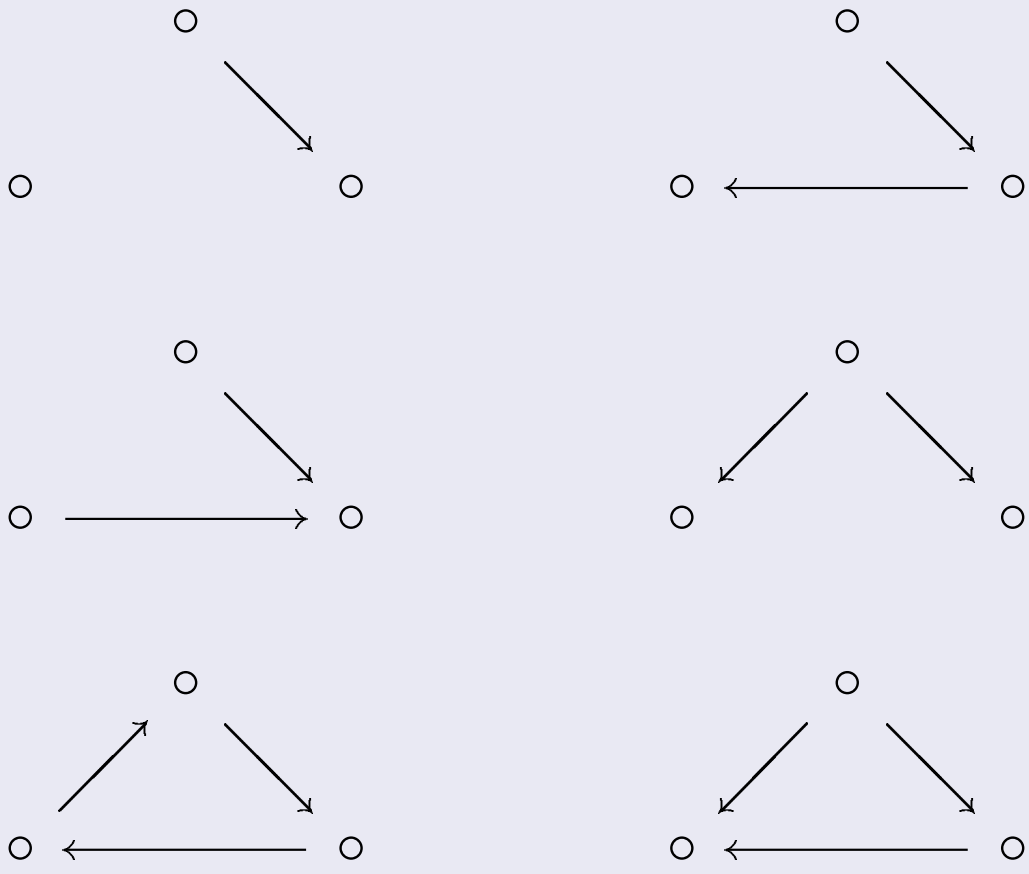
Элемент группы g	$Type(g)$	$w(g)$	*# мономов*
$e = (a)(b)(c)$	$\langle 3,\ 0,\ 0 \rangle$	x_1^3	1
$g_1 = (abc)$	$\langle 0,\ 0,\ 1 \rangle$	x_3^1	2
$g_2 = (a)(bc)$	$\langle 1,\ 1,\ 0 \rangle$	$x_1^1 x_2^1$	3
$g_2 = (\overline{a})(bc)$	$\langle 0,\ 0,\ 1 \rangle$	x_3^1	3

$\overline{a}$ — *ребро* a *сменило направление. Но* $Type((\overline{a})(bc)) = Type(\bar{a}\bar{b}\bar{c}) = Type(abc)$, *поэтому* $P = \frac{1}{6} \cdot \left[x_1^3 + 5x_3 \right]$.

Неориентированные $P(x_1, x_2, x_3) = \frac{1}{6}\left[x_1^3 + x_3^1 + x_1^1 x_2^1 \right]$,
$P(2,2,2) = 4$.

Ориентированные $P(x_1, x_2, x_3) = \frac{1}{6}\left[x_1^3 + 5x_3 \right]$,
$P(2,2,2) = 7$.

Перечислим ориентированные: пустой граф и графы



— всего 7 графов неориентированных — 4.

Цикловые индексы самодействия и действия O на элементы куба

$$P(S_n) = \sum_{\substack{(j_1,\ldots,j_n)\in\mathbb{N}_0^n \\ 1j_1+j_2+\ldots+nj_n}} \frac{x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}}{(1^{j_1}j_1!)(2^{j_2}j_2!)\ldots(n^{j_n}j_n!)},$$

$$P(\mathbb{Z}_n) = \frac{1}{n}\sum_{d|n}\varphi(d)x_d^{n/d}, \quad \varphi - \text{функция Эйлера},$$

$$P(D_n) = \frac{1}{2}P(\mathbb{Z}_n) + \begin{cases} \frac{1}{2}x_1x_2^{(n-1)/2}, & \text{если } n \text{ нечётно}, \\ \frac{1}{4}\left(x_2^{n/2} + x_1^2x_2^{(n-2)/2}\right), & \text{если } n \text{ чётно}, \end{cases}$$

$$P(O \underset{\alpha}{:} V) = \frac{1}{24}\left(x_1^8 + 9x_2^4 + 6x_4^2 + 6x_4^2 + 8x_1^2x_3^2\right),$$

$$P(O \underset{\alpha}{:} E) = \frac{1}{24}\left(x_1^{12} + 3x_2^6 + 8x_3^4 + 6x_4^2 + 8x_1^2x_2^5 + 6x_4^3\right),$$

$$P(O \underset{\alpha}{:} F) = \frac{1}{24}\left(x_1^6 + 3x_1^2x_2^2 + 6x_1^2x_4 + 6x_2^3 + 8x_3^2\right).$$

Теорема Пойа

Было: множество T, $|T| = N$, группа $\mathbb{G}$, $|G| = n$ и действие $\mathbb{G} \underset{\alpha}{:} T$.

Добавим: множество $R = \{c_1, \ldots, c_r\}$ — меток («красок»), $|R| = r$ и совокупность функций $F = R^T$ — приписывания меток (раскрашиваний).

$\mathbb{G}$, действуя на T, действует и на R^T: $\circ : R^T \times G = R^T$.

Дадим вес элементам R: $w(c_i) = y_i$, $i = \overline{1, r}$.

Теорема (Редфилда-Пойа)

Цикловой индекс действия группы $\mathbb{G}$ на R^T есть

$$W(F) = P(\mathbb{G} \underset{\alpha}{:} R^T) = P(\mathbb{G} \underset{\alpha}{:} T, x_1, \ldots, x_N)\big|_{x_k = y_1^k + \ldots + y_r^k} =$$

$$= \frac{1}{|G|} \left[\sum_{\substack{(i_1, \ldots, i_N) \in \mathbb{N}_0^N = N \\ i_1 + \ldots + i_N = N}} u_{i_1, \ldots, i_N} y_1^{i_1} \ldots y_N^{i_N} \right].$$

Следствие

Если все веса выбраны одинаковыми $(y_1 = \ldots y_r = 1)$, *то* $x_1 = \ldots x_N = r$ *и* $W(F)$ *— число классов эквивалентности*

$$C(\mathbb{G} \underset{\alpha}{:} R^T) = C(\mathbb{G} \underset{\alpha}{:} T) = P(\mathbb{G} \underset{\alpha}{:} T, r, \ldots, r)\,.$$

С помощью теоремы Бернсайда мы решали задачи об общем числе неэквивалентных разметок (раскрасок). Однако нельзя было посчитать число разметок данного типа. Теорема Пойа даёт эту возможность.

Усложним задачу об ожерельях $N = 5$, $r = 3$

Задача

Составляются ожерелья из 5 бусин 3 цветов (красный, синий, зелёный). Сколько имеется ожерелий, имеющих ровно 2 красные бусины? Ожерелья одинаковы, равны если одно получается из другого поворотом и/или переворотом.

Решение

Было: $\mathbb{G} = D_5$, *цикловой индекс* $P = \frac{1}{10}\left[x_1^5 + 4x_5 + 5x_1x_2^2\right]$.
Всего ожерелий $\#Col(3) = P(3, \ldots, 3) = 39$.

$$\left\{\begin{array}{ll} w(\text{красный}) & = y_1, \\ w(\text{синий}) & = y_2, \\ w(\text{зелёный}) & = y_3, \end{array}\right. \Rightarrow \left\{\begin{array}{l} y_1 = y, \\ y_2 = y_3 = 1, \end{array}\right. \Rightarrow \left\{\begin{array}{ll} x_1 & = y + 2, \\ x_2 & = y^2 + 2, \\ \ldots & \\ x_5 & = y^5 + 2. \end{array}\right.$$

$$C = \frac{1}{10}\left[u_0 + u_1 y + u_2 y^2 + \ldots + u_5 y^5\right] =$$
$$= \frac{1}{10}\left[(y+2)^5 + 4(y^5+2) + 5(y+2)(y^2+2)^2\right] =$$
$$= \frac{1}{10}\left[\ldots + C_5^2 y^2 2^3 + \ldots + 5(y+2)(y^2+4y+4)\right] =$$
$$= \frac{1}{10}\left[\ldots + (80+40)y^2 + \ldots\right].$$

$u_2 = 12$.

Задача

Вершины куба помечают красными и синим цветами.

Сколько существует

1. *разнопомеченных кубов;*
2. *кубов, у которых половина вершины красные;*
3. *кубов, у которых не более 2-х красных вершин?*

Решение

Цикловой индекс действия группы O *на вершины куба*

$$P(O \underset{\alpha}{:} V) = \frac{1}{24}\left[\, x_1^8 + 6x_4^2 + 9x_2^4 + 8x_1^2x_3^2 \,\right].$$

1. *Число разнопомеченных кубов —*

$$\#Col(3) = P|_{x_1=\ldots=x_8=2} = \frac{552}{24} = 23\,.$$

2. $w(\text{красный}) = y,\ w(\text{синий}) = 1,\ x_k = y^k + 1,\ k = \overline{1,8}$:

$$\#Col(4,4) = \frac{1}{24}\big[\,(y+1)^8 + 9\cdot(y^2+1)^4 + 4\cdot(y^4+1)^2 + 8\cdot(y+1)^2(y^3+1)^2\,\big] =$$

$$= \frac{1}{24}\big[\,\ldots + 28y^2 + C_8^4 y^4 + \ldots + 9(\ldots 4y^2 + 6y^4 + \ldots) + 8(\ldots + 2y + y^2 + \ldots)(\ldots + 2y^3 + \ldots)\,\big].$$

$$u_4 = \frac{1}{24}\big[\,70 + 9\cdot 6 + 6\cdot 2 + 8\cdot 2\cdot 2\,\big] = \frac{168}{24} = 7.$$

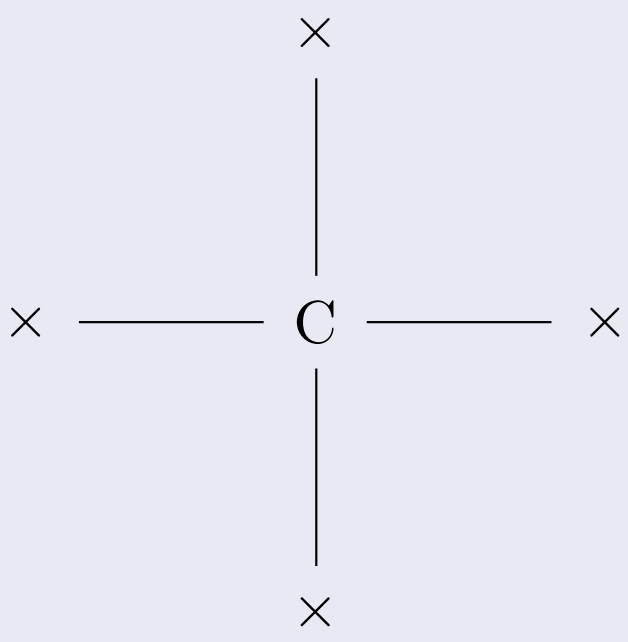
3. $\#Col(\leqslant 2, *) = u_0 + u_1 + u_2.\quad u_0 = u_1 = 1.$

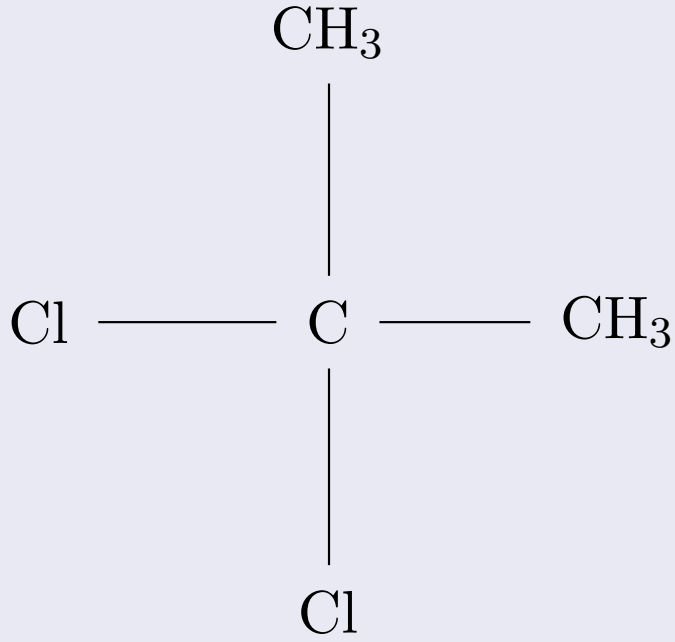
$$u_2 = \frac{1}{24}\big[\ldots + 28y^2 + \ldots + 9(\ldots + 4y^2\ldots) + 8(\ldots + y^2 + \ldots)\big] =$$

$$= \frac{72}{24} = 3.\qquad \#Col(\leqslant 2) = 1 + 1 + 3 = 5.$$

Задача

Рассматриваются молекулы 4-х валентного углерода C*:*





где на на месте $\times$ *могут находится* $\mathrm{CH_3}$ *(метил),* $\mathrm{C_2H_5}$ *(этил),* H *(водород) или* Cl *(хлор). Например — дихлорбутан.*

Задача (продолжение)

Найти

1. *общее число* M *всех молекул;*
2. *число молекул с* $H = 0, 1, 2, 3, 4$ *атомами водорода.*

Решение

1. *Имеем* $N = 4$, $\mathbb{G}$ — *группа вращения тетраэдра:*

$$P(T \underset{\alpha}{:} V) = \frac{1}{12}\left[x_1^4 + 8x_1x_3 + 3x_2^2\right].$$

Всего молекул —

$$M = P(4, \ldots, 4) = \frac{1}{12}\left[4^4 + 8\cdot 4\cdot 4 + 3\cdot 4^2\right] = \frac{16\cdot 27}{12} = 36\,.$$

2. *Веса:* $y_1 = \mathrm{H}$, $y_2 = y_3 = y_4 = 1$.
Подстановка в P: $x_k = \mathrm{H}^k + 3$, $k = \overline{1,4}$.

Имеем

$$P = \frac{1}{12}\left[(\mathrm{H}+3)^4 + 8(\mathrm{H}+3)(\mathrm{H}^3+3) + 3(\mathrm{H}^2+3)^2\right] =$$
$$= \frac{1}{12}\left[(\mathrm{H}^4 + 4\cdot\mathrm{H}^3\cdot 3 + 6\cdot\mathrm{H}^2\cdot 9 + 4\cdot\mathrm{H}\cdot 27 + 81) + \right.$$
$$\left. + 8(\mathrm{H}^4 + 3\mathrm{H}^3 + 3\mathrm{H} + 9) + 3(\mathrm{H}^4 + 6\mathrm{H}^2 + 9)\right] =$$
$$= 1\mathrm{H}^4 + 3\mathrm{H}^3 + 6\mathrm{H}^2 + 11\mathrm{H} + 15.$$

Итого имеется молекул с числом атома водорода:
с 4-мя — 1 шт., с 3-мя — 3 шт., с 2-мя — 6 шт., с 1-м — 11 шт.,
без атомов водорода — 15 шт.,
всего — $1 + 3 + 6 + 11 + 15 = 36$.

Группа вращения тетраэдра

$O = \langle t, f \rangle, t^3 = f^2 = e$, где

Раздел I

Раздел II

Частично упорядоченные множества: определение и примеры

Определение

Пару $\mathbf{P} = \langle P, \leqslant \rangle$, где P — непустое множество, а $\leqslant$ — рефлексивное, антисимметричное и транзитивное бинарное отношения на нём, называют *частично упорядоченным множеством* (сокращённо *ч.у. множеством*).

Рефлексивность: $x \leqslant x$,
Антисимметричность: $(x \leqslant y)\&(y \leqslant x) \Rightarrow x = y$,
Транзитивность: $(x \leqslant y)\&(y \leqslant z) \Rightarrow x \leqslant y$.

Примеры

- $\langle \mathcal{P}(M), \subseteq \rangle$ — классический пример ч.у. множества (упорядочивание множеств *по включению*);
- $\langle \mathbb{N}, \leqslant \rangle$ и $\langle \mathbb{N}, | \rangle$ — два упорядочивания одного множества.

Ч.у. множество $\mathbf{P} = \langle P, \leqslant \rangle$: основные понятия

- *полный (линейный) порядок*, если $\underset{P}{\forall} x, y \, ((x \leqslant y) \vee (y \leqslant x))$;
- если $(x \not\leqslant y) \vee (x \not\leqslant y)$, то x и y *сравнимы* $(x \sim y)$, иначе они *несравнимы* $(x \nsim y)$;
- если в $\mathbf{P}$ нет сравнимых элементов, то это *тривиально упорядоченное множество*.
- x *непосредственно предшествует* y (y *непосредственно следует за* x), если $x \leqslant z \leqslant y \;\Rightarrow\; (z = x) \vee (z = y)$ $(x \lessdot y)$.
- $\{\, x \in P \mid a \leqslant x \leqslant b \,\}$ — *интервал* $[\, a, b \,]$;
- $v_1 \leqslant \ldots \leqslant v_n \stackrel{\text{def}}{=} [v_1, \ldots, v_n]$ — *цепь* ($\mathbf{n}$ или $\underline{n}$), а подмножество попарно несравнимых элементов — *антицепь* в $\mathbf{P}$;
- цепь *максимальная* (или *насыщенная*), если при добавлении к ней любого элемента она перестаёт быть цепью;
- если $\underset{P}{\forall} x, y \; ((x \leqslant y) \;\Rightarrow\; (y \leq x))$, то $\leq x$ — *двойственный порядок на* P, $\geqslant \stackrel{\text{def}}{=} \leq$ или $\leqslant^d = \geqslant$.

Диаграммы Хассе

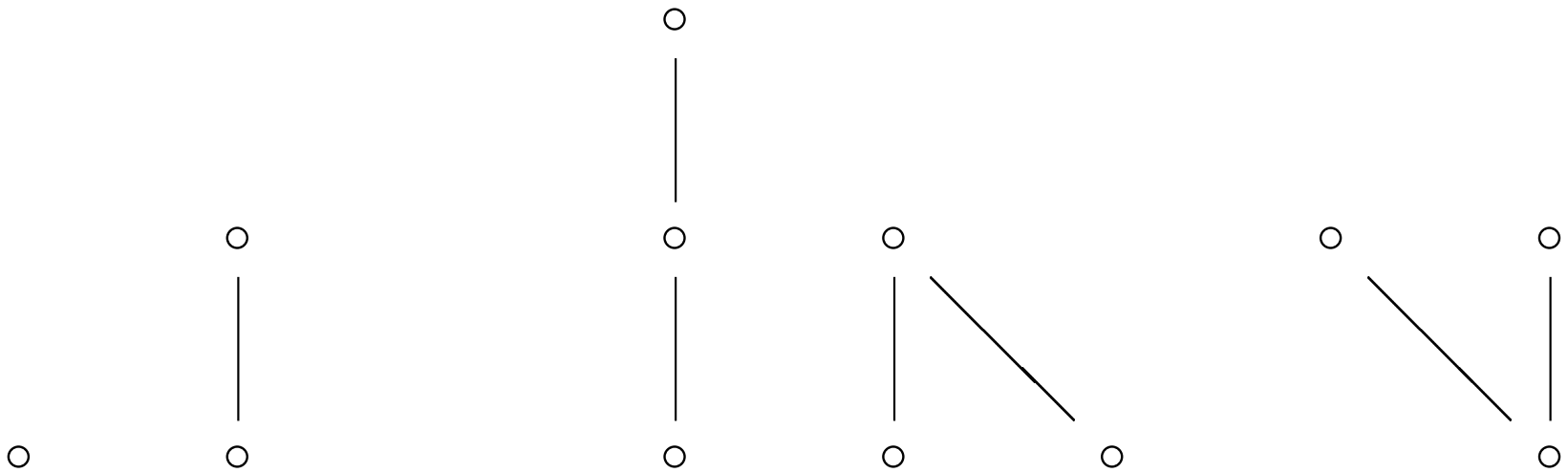


Рис. 2. Диаграммы нетривиальных непомеченных трёхэлементных ч.у. множеств

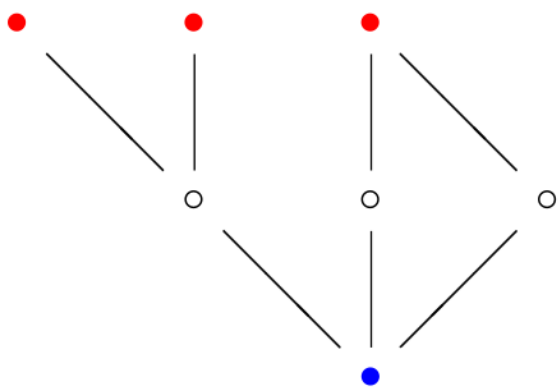
Ч.у. множества: особые элементы.

Определение

Элемент $u \in P$ ч.у. множества $\langle P, \leqslant \rangle$ называют:

- *максимальным*, если $u \leqslant x \Rightarrow u = x$,
- *минимальным*, если $u \geqslant x \Rightarrow u = x$,
- *наибольшим*, если $x \leqslant u$,
- *наименьшим*, если $x \geqslant u$

для любых $x \in P$.



● — максимальные элементы;

● — минимальный и наименьший элемент.

Наибольший (1) и наименьший (0) — *граничные элементы*.

В конечном ч.у. множестве имеется как минимум по одному максимальному и минимальному элементу.

Ранжированные ч.у. множества

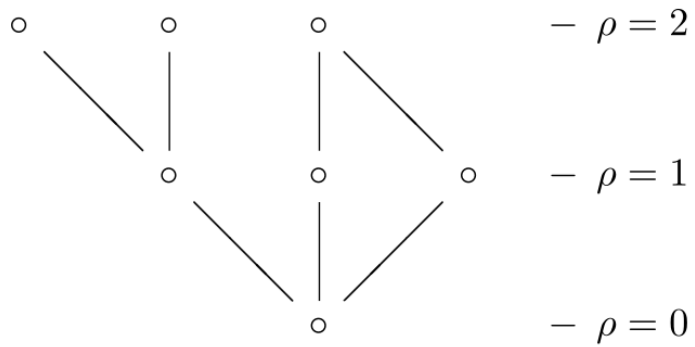
Цепное условие Жордана-Дедекинда

Все максимальные цепи между двумя данными элементами локально конечного ч.у. множества имеют одинаковую длину.

Если ч.у. множество удовлетворяет условию Жордана-Дедекинда и имеет наименьший элемент 0, то можно определить *функцию ранга* ρ:

1. $\rho(0) = 0$;
2. $a \lessdot b \Rightarrow \rho(b) = \rho(a) + 1$.

Такое множество должно иметь слои



Если множество ранжируемо, то любой его слой является антицепью.

Порядковые гомоморфизмы

Определение

Отображение $\varphi\colon P \to P'$ носителей ч.у. множеств $\mathbf{P}$ и $\mathbf{P}'$ называется соответственно

- *изотонным* (*монотонным*, *порядковым гомоморфизмо*), если $x \leqslant y \Rightarrow \varphi(x) \leqslant \varphi(y)$;
- *обратно изотонным*, если $\varphi(x) \leqslant \varphi(y) \Rightarrow x \leqslant y$;
- *антиизотонным*, если $x \leqslant y \Rightarrow \varphi(x) \geqslant \varphi(y)$.

Если φ изотонно, обратно изотонно и инъективно, то это *вложение* или *(порядковый) мономорфизм* (символически $P \overset{\varphi}{\hookrightarrow} P'$).
Сюръективный мономорфизм — *(порядковый) изоморфизм* (символически $P \cong P'$ или $P \overset{\varphi}{\cong} P'$).
Изоморфизм ч.у. множества в себя — *(порядковый) автоморфизм*.

Идеалы и фильтры ч.у. множеств

Определение

Подмножество J элементов ч.у. множества $\mathbf{P}\langle P, \leqslant \rangle$ называется его *(порядковым) идеалом*, или *(полуидеалом* если

$$(x \in J)\ \&\ (y \leqslant x)\ \Rightarrow\ y \in J.$$

Подмножество F элементов $\mathbf{P}$ называется его *(порядковым) фильтром* или *двойственным порядковым идеалом*, если

$$(x \in F)\ \&\ (x \leqslant y)\ \Rightarrow\ y \in F.$$

Согласно определению, $\varnothing$ и всё P являются порядковыми идеалами.

Ясно, что объединение и пересечение порядковых идеалов есть порядковый идеал.

$J(\mathbf{P})$ — множество всех порядковых идеалов ч.у. множества $\mathbf{P}$.

Определение

Пусть $\langle P, \leqslant \rangle$ч.у. множество и $A \subseteq P$. Множества $A^{\triangle}$ и $A^{\triangledown}$ определяемые условиями

$$A^{\triangle} = \left\{ x \in P \mid \underset{A}{\forall} a \, (a \leqslant x) \right\} \text{ и } A^{\triangledown} = \left\{ x \in P \mid \underset{A}{\forall} a \, (x \leqslant a) \right\}$$

называются *верхним* и *нижним конусами множества* A, а их элементы — *верхними* и *нижними гранями множества* A соответственно. Для одноэлементного множества $A = \{a\}$ используются обозначения $a^{\triangle}$ и $a^{\triangledown}$.

Понятно, что если $a \leqslant b$, то $a^{\triangle} \cap b^{\triangledown} = [a, b]$.

$x^{\triangledown} = J(x)$ — идеал; $x^{\triangle}$ — фильтр P; такие идеалы и фильтры называют *главными*.

Раздел I

Раздел II

- Коды БЧХ

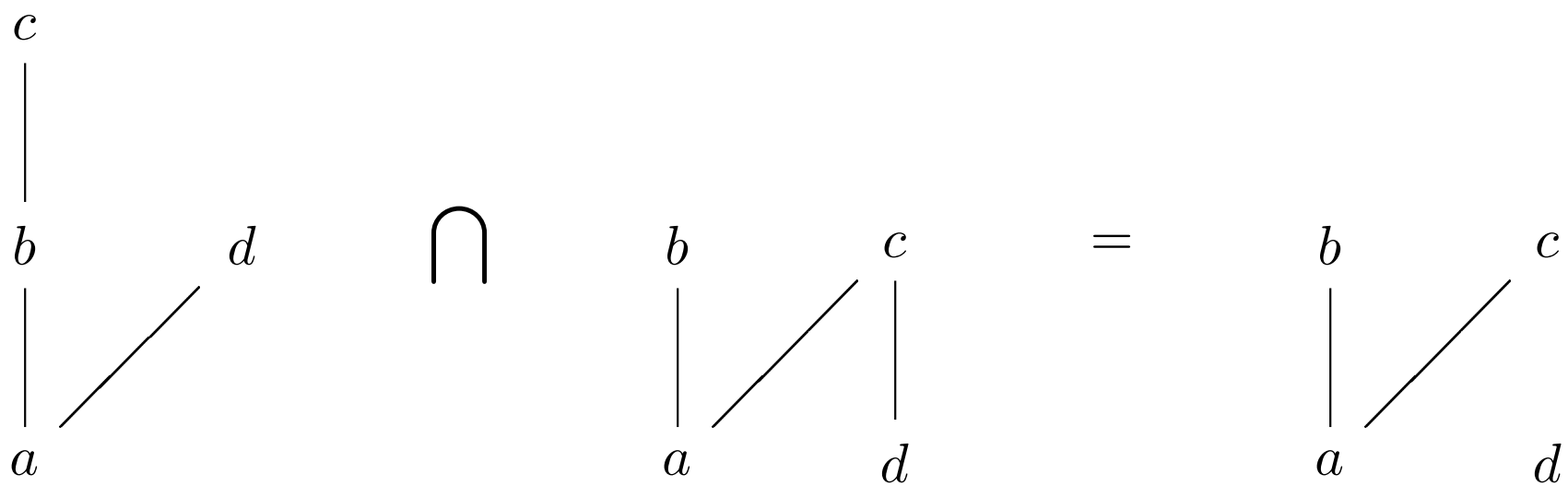
4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач

5. **Частично упорядоченные множества**
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация

6. Алгебраические решётки
   - Решётки

Пересечение

$$\underline{\langle P, \leqslant_1 \rangle \cap \langle P, \leqslant_2 \rangle = \langle P, \leqslant_1 \cap \leqslant_2 \rangle}.$$



Свойства ч.у. множеств могут не сохраняются при пересечении. Например «быть цепью»: если P — цепь, тогда P^d — также цепь, а $P \cap P^d$ — тривиально упорядоченное множество.

Прямая сумма

$\mathbf{P} = \langle P, \leqslant_P \rangle$ и $\mathbf{Q} = \langle Q, \leqslant_Q \rangle$ — два ч.у. множества, причём $P \cap Q = \varnothing$.

$$\underline{\mathbf{P} + \mathbf{Q} = \langle P \cup Q, \leqslant_P \vee \leqslant_Q \rangle.}$$

Очевидно, справедливы соотношения

$$P + Q \cong P + R \Rightarrow Q \cong R \quad \text{и} \quad (P + Q)^d \cong P^d + R^d.$$

$n\mathbf{P}$ — прямая сумма n экземпляров $\mathbf{P}$, $\mathbf{n} \cong n\mathbf{1}$.

Диаграмма прямой суммы состоит из двух диаграмм соответствующих ч.у. множеств, рассматриваемых как единая диаграмма.

Ч.у. множество, не являющееся прямой суммой некоторых двух других ч.у. множеств, называется *связным*.

Прямое произведение: определение

Прямым или *декартовым произведением* ч.у. множеств $\mathbf{P}\langle P, \leqslant_P \rangle$ и $\mathbf{Q} = \langle Q, \leqslant_Q \rangle$ называется множество

$$\mathbf{P} \times \mathbf{Q} = \langle P \times Q, \leqslant \rangle,$$
$$\text{где } (p, q) \leqslant (p', q') \Leftrightarrow (p \leqslant_P p')\&(q \leqslant_Q q').$$

$\mathbf{P}^n$ — прямое произведение n экземпляров $\mathbf{P}$: $B^n = \mathbf{2}^n$.

Если $\mathbf{P}$ и $\mathbf{Q}$ ранжированы и их ранговые функции суть ρ_P и ρ_Q, то $\mathbf{P} \times \mathbf{Q}$ также ранжировано и $\rho(x_1, x_2) = \rho_P(x_1) + \rho_Q(x_2)$;

Справедливы соотношения

$$P \times R \cong Q \times R \Rightarrow P \cong Q, \quad P^n \cong Q^n \Rightarrow P \cong Q,$$
$$(P \times Q)^d \cong P^d \times Q^d.$$

Прямое произведение: пример 1

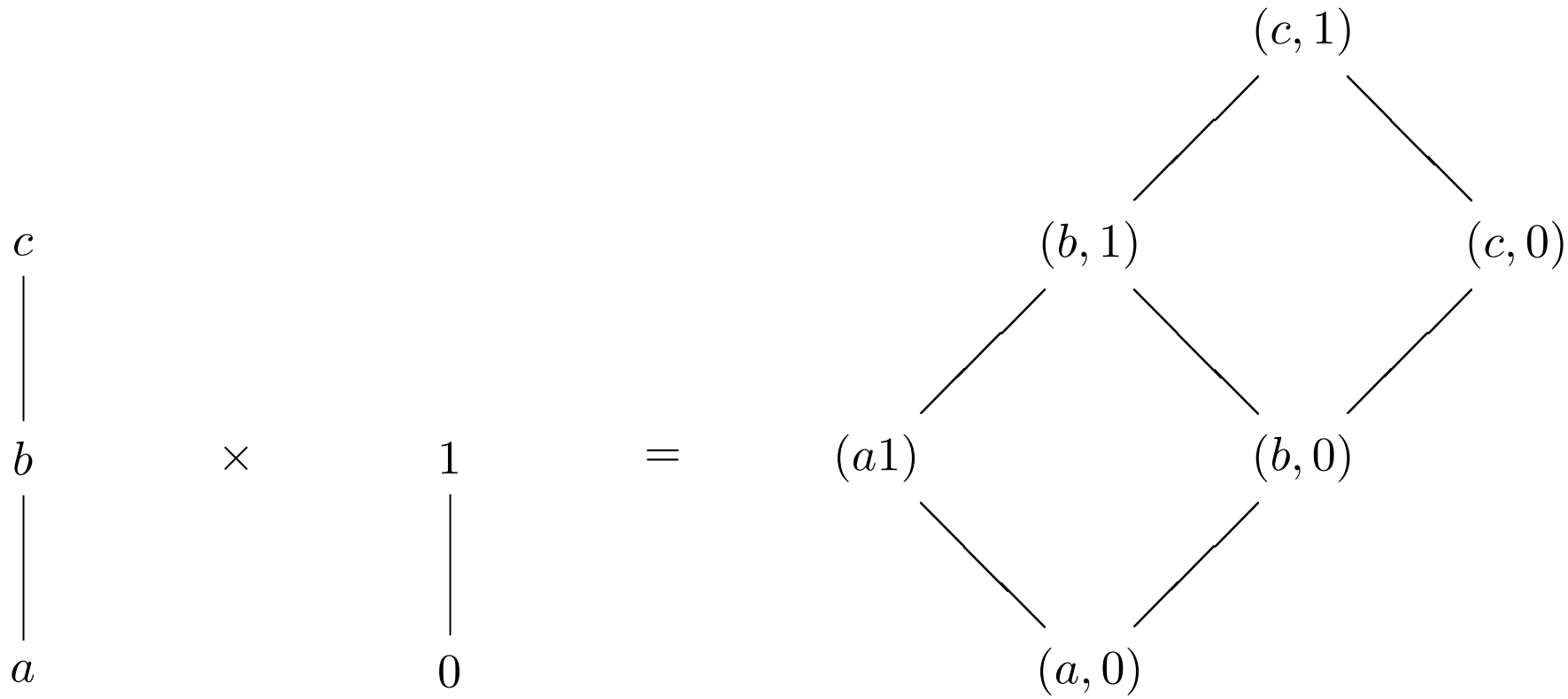


Рис. 3. Прямое произведение цепей **3** и **2**

Прямое произведение: пример 2

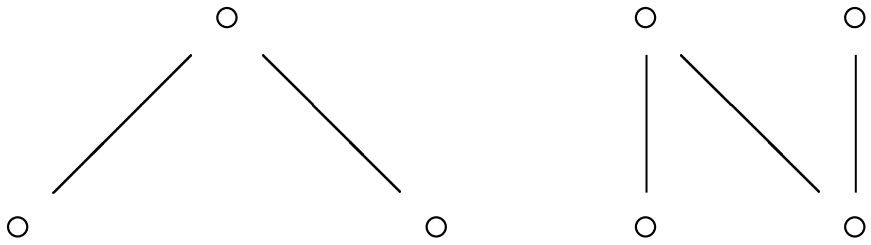


Рис. 4. Зигзаги (или заборы) $\mathbf{Z}_3$ и $\mathbf{Z}_4$

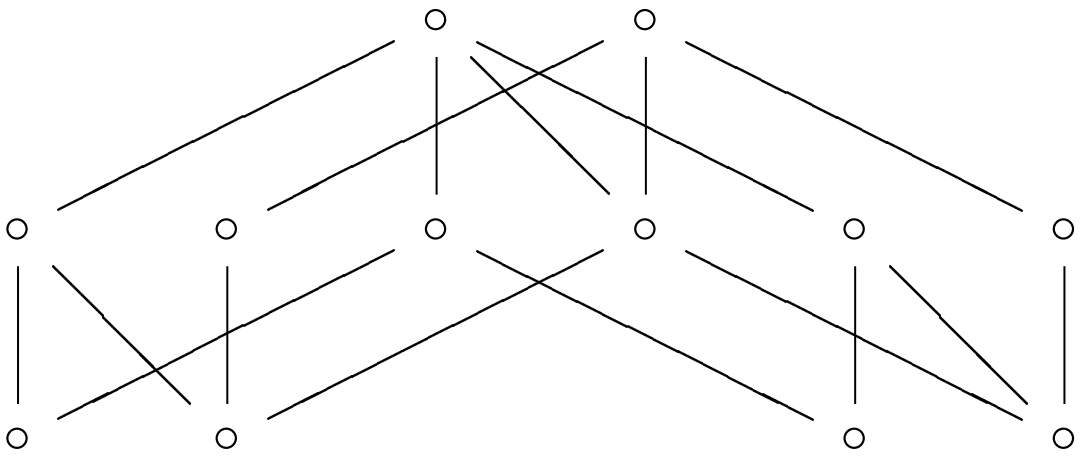


Рис. 5. Прямое произведение $\mathbf{Z}_3 \times \mathbf{Z}_4$

Теорема (Ope)

Каждый частичный порядок изоморфен некоторому подмножеству декартова произведения цепей.

Определение

Мультипликативной размерностью ч.у. множества $\mathbf{P}$ называется наименьшее число k линейных порядков $\mathbf{L}_i$ таких, существует вложение $\mathbf{P} \hookrightarrow \mathbf{L}_1 \times \ldots \times \mathbf{L}_k$.

Раздел I

Раздел II

Представление $\mathbf{P} = \langle P, \leqslant \rangle$ в виде пересечения цепей

Теорема (Шпильрайна, принцип продолжения порядка)

1. *Любой частичный порядок $\leqslant$ может быть продолжен до линейного на том же множестве.*
2. *Каждый порядок есть пересечение всех своих линейных продолжений (линеаризаций).*

$$\mathbf{P} \to \mathbf{L}, \qquad \mathbf{P} = \mathbf{L}_1 \cap \ldots \cap \mathbf{L}_{e(\mathbf{P})},$$

где $e(\mathbf{P})$ — множество всех линеаризаций ч.у. множества $\mathbf{P}$.

Доказательство (для конечного случая, $|P| = n$.)

1. *Если $\mathbf{P}$ — не цепь, то в P найдутся несравнимые элементы; произвольно определим порядок на них и продолжим его по транзитивности. Если получившиеся ч.у. множество ещё не цепь, то выберем новую пару несравнимых элементов и поступаем, как указано выше. Через конечное число шагов получаем линейный порядок.*

Доказательство (продолжение)

1. *(продолжение). Поскольку возможен различный выбор пар несравнимых элементов и при каждом выборе можно полагать как любой (из 2-х) их порядок, то действуя указанным образом можно получить различные возможные продолжения исходного частичного порядка до линейного.*
2. *Пересечение всех таких цепей даст исходное ч.у. множество. Действительно, если $x \leqslant y$, то аналогичное следование будет и во всех полученных линейных порядках, а при $x \nsim y$ всегда найдётся пара цепей с противоположным их следованием, что в пересечении цепей и даст несравнимость этих элементов.*

Для конечных множеств поиск такого продолжения для ч.у. множеств, заданных парами непосредственно следующих друг за другом вершин в теоретическом программировании называют «топологической сортировкой». Известны алгоритмы, решающие данную задачу за линейное время.

Некоторые ч.у. множества

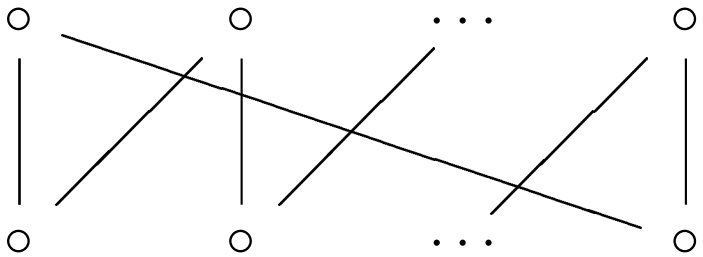


Рис. 6. Малая корона $\mathbf{s}_n$

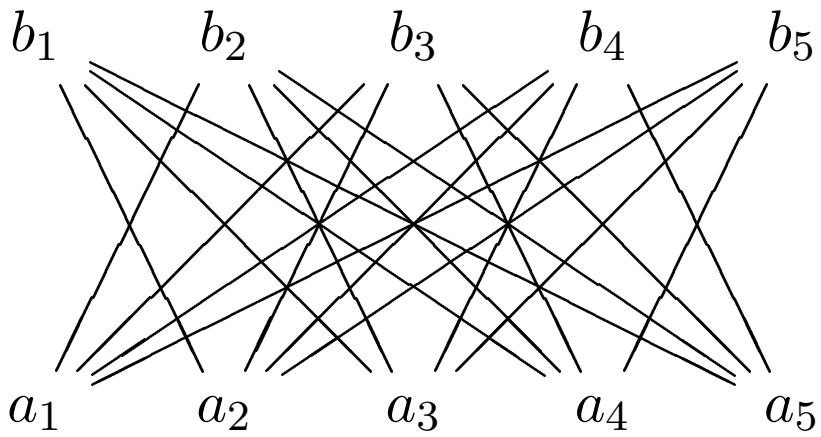


Рис. 7. Корона $\mathbf{S}_5$

«$e(\mathrm{P})=?$» — NP-полная задача, но:

- $e(\mathbf{P}+\mathbf{Q}) = \binom{|P|+|Q|}{|P|} e(\mathbf{P})e(\mathbf{Q})$;
- $e(\mathbf{2}\times\mathbf{n}) = \dfrac{1}{n+1}\binom{2n}{n}$ — *числа Каталана*;
- $$\sum_{n\geqslant 0} \frac{e(\mathbf{Z}_n)\,x^n}{n!} = \operatorname{tg} x + \sec x\,,$$

  значения $\mathbf{Z}_n$ при чётных n — *числа секанса*, а при нечётных — *числа тангенса*;
- $e(\mathbf{S}_n) = (n+1)!(n-1)!\,;$
- $$\sum_{n\geqslant 1} \frac{e(\mathbf{s}_n)}{n!}\,x^n = \frac{x}{\cos^2 x}\,;$$
- $$\frac{\log(e(B^n))}{2^n} = \log\binom{t}{\lfloor t/2\rfloor} - \frac{3}{2}\log e + o(1)\,.$$

Для практических целей (решение задач комбинаторики, дискретной оптимизации и др.) часто рассматривают связанное с ч.у. множеством $\mathbf{P}$ вероятностное пространство на множестве всех $e(\mathbf{P})$ его линеаризаций, в котором каждая линеаризация равновероятна.

В этом пространстве для элементов x, y, z, ... данного ч.у. множества рассматривают события E вида $x \leqslant y$, $(x \leqslant y)\,\&\,(x \leqslant z)$ и т.д. Вероятность $\Pr[E]$ такого события определяют как отношение числа линеаризаций, в которых имеет место E, к $e(P)$.

Теорема (XYZ-теорема)

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $x, y, z \in P$. Тогда

$$\Pr[x \leqslant y] \cdot \Pr[x \leqslant z] \leqslant \Pr[(x \leqslant y)\,\&\,(x \leqslant z)].$$

Проблема сортировки и 1/3 – 2/3 предположение

— определить линейный порядок $\mathbf{L}$ с помощью минимального количества вопросов «*верно ли, что $x < y$ в $\mathbf{L}$?*».

Обобщение: восстановить зафиксированную, но неизвестную линеаризацию $\mathbf{L}$ ч.у. множества $\mathbf{P}$ с помощью минимального количества таких вопросов.

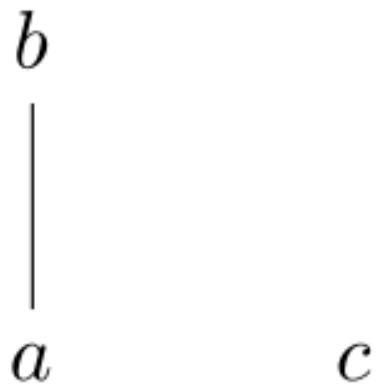
Оптимальная процедура поиска $\mathbf{L}$ включает в себя нахождение элементов x и y, для которых $\Pr[x < y] \approx \frac{1}{2}$.

С.С. Кислицын (1968) высказал «*1/3 – 2/3 предположение*»: “любое не являющееся цепью ч.у. множество содержит пару несравнимых элементов x и y, для которых

$$\frac{1}{3} \leqslant \Pr[x \leqslant y] \leqslant \frac{2}{3}\text{”}.$$

Позднее вышеприведённое утверждение независимо выдвинули американские учёные М. Фредман и Н. Линал.

1/3 – 2/3 предположение



Пример $\mathbf{2+1}$ показывает, что указанные границы несужаемы (имеется и пример десятиэлементного ч.у. множества со связанной диаграммой Хассе).

Данное предположение до сих пор успешно противостоит всем попыткам его доказать и *представляет собой одну из наиболее интригующих проблем комбинаторной теории ч.у. множеств* (С. Фелснер и У.Т. Троттер).

На сегодняшний день наиболее сильный результат:

$$0,2764 \approx \frac{5-\sqrt{5}}{10} \leqslant \Pr[x \leqslant y] \leqslant \frac{5+\sqrt{5}}{10} \approx 0,7236\,.$$

Ч.у. множества: спектр

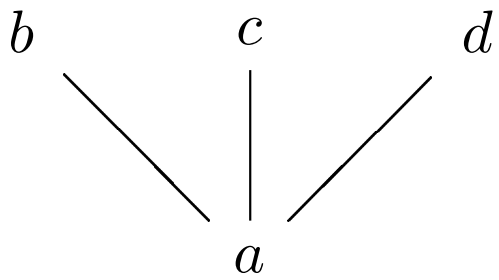
$$Spec\,(P) = \{\Pr[a \leqslant b] \mid a, b \in P,\ a \neq b\}$$

Поскольку $\Pr[a \leqslant b] = 1 - \Pr[b \leqslant a]$, спектр симметричен относительно $\frac{1}{2}$.

- для всех неодноэлементных тривиально упорядоченных множеств $Spec = \{\frac{1}{2}\}$;
- $\{0, \frac{1}{2}, 1\}$ — единственный трёхэлементный спектр;
- все четырёхэлементные спектры должны иметь вид $\{0, \alpha, 1-\alpha, 1\}$, где $0 < \alpha < \frac{1}{2}$; гипотеза (2002): $\alpha = \frac{1}{3}$.

Ч.у. множества: размерность

По теореме Шпильрайна ч.у. множество $\mathbf{P}$ совпадает с пересечением всех $e(\mathbf{P})$ своих линеаризаций. Однако тот же результат можно получить, взяв значительно меньшее число линейных продолжений. Например, ч.у. множество $\mathbf{P}$



имеет шесть линеаризаций, но $\mathbf{P} = [a, b, c, d] \cap [a, d, c, b]$.

Пусть $\mathbf{P}$ — ч.у. множество и $\mathcal{R} = \{\mathbf{L}_1, \ldots, \mathbf{L}_k\}$ — совокупность цепей такая, что $\mathbf{P} = \mathbf{L}_1 \cap \ldots \cap \mathbf{L}_k$, то говорят, что $\mathcal{R}$ *реализует* $\mathbf{P}$.

Ч.у. множества: размерность...

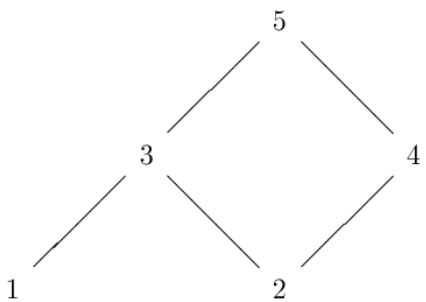
Определение

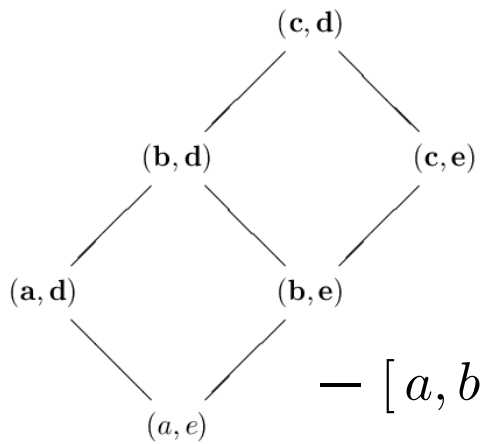
Наименьшее число линейных порядков, дающих в пересечении данное ч.у. множество $\mathbf{P}$ называется его *(порядковой) размерностью* (символически $\dim(P)$).

Теорема (Ope)

Порядковая и мультипликативная размерности ч.у. множества совпадают.

$[1,2,3,4,5] \cap [2,4,1,3,5]$:





$= [a,b,c] \times [d,e]$

$\dim(\mathbf{P})$ — более тонкая оценка ч.у. множества, чем $e(\mathbf{P})$

Размерность ... имеют:

1 — только цепи;

2 — тривиально упорядоченные множества

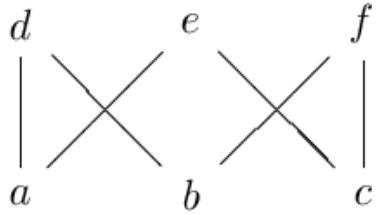
(т.е. размерность не может интерпретироваться как мера отличия данного ч.у. множества от линейного);

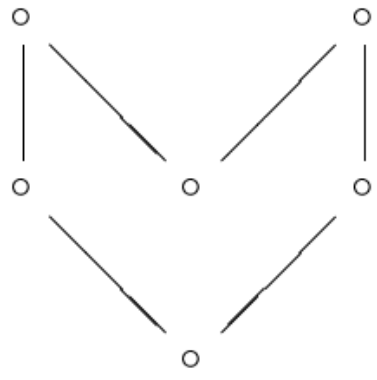
— $\mathbf{Z}_n$;

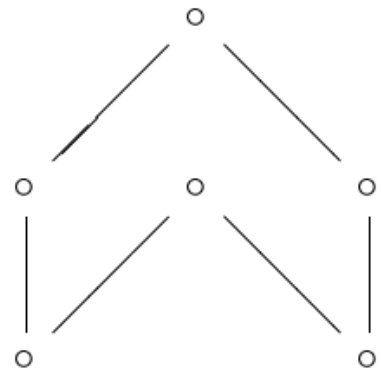
— все отличные от цепей ч.у. множеств, при $|P| \leqslant 6$, кроме

3 — $\mathbf{s}_3$, $\mathbf{sh}$ и $\mathbf{sh}^d$:

n — $\mathbf{S}_n$







О размерности ч.у. множества $\mathbf{P} = \langle P, \leqslant \rangle$

1. $\varnothing \neq Q \subseteq P \Rightarrow \dim(\mathbf{Q}) \leqslant \dim(\mathbf{P})$, при этом при удалении одного элемента его размерность уменьшается не более, чем на 1;
2. $\dim(\mathbf{P}+\mathbf{Q}) = \max\{\dim(\mathbf{P}), \dim(\mathbf{Q})\}$, если хотя бы одно из множеств не является цепью и $\dim(\mathbf{P}+\mathbf{Q}) = 2$, иначе;
3. $\dim(\mathbf{P}\times\mathbf{Q}) \leqslant \dim(\mathbf{P}) + \dim(\mathbf{Q})$;
4. $\dim(\mathbf{P}) \leqslant |P|/2$ при $|P| \geqslant 4$ (теорема Хирагучи).

Теорема («компактности»)

Пусть $\mathbf{P}$ — такое ч.у. множество, что любое его конечное ч.у. подмножество имеет размерность, не превосходящую d. Тогда $\dim(\mathbf{P}) \leqslant d$.

$$\frac{n}{4}\left(1-\frac{c_1}{\log_2 n}\right) \leqslant \dim(P) \leqslant \frac{n}{4}\left(1-\frac{c_2}{\log_2 n}\right).$$

d-несводимые ч.у. множества

Определение

Ч.у. множество $\mathbf{P}$ называется *d-несводимым* для некоторого $d \geqslant 2$, если $\dim(\mathbf{P}) = d$ и $\dim(\mathbf{P}') < d$ для любого собственного ч.у. подмножества $P' \subset P$.

... несводимые множества:

2 — двухэлементная антицепь (единственное);

3 — $\mathbf{s}_3, \mathbf{sh}, \mathbf{sh}^d + \ldots$ — описаны, регулярны и хорошо изучены;

4 — достаточно часто встречаются и весьма причудливы;

t — $\mathbf{S}_t$ (единственное $2t$-элементное) $+ \ldots$;

- каждое t-несводимое ч.у. множество является ч.у. подмножеством некоторого $(t+1)$-несводимого.

Проблема Ногина

Каково наибольшее значение $\pi(d, n)$ мощности множества максимальных элементов d-несводимого n-элементного ч.у. множества при $d \geqslant 4$?

Данная проблема до сих пор остаётся открытой.

Утверждение

$$\pi(d, n) \leqslant n - d.$$

-

Раздел I

Раздел II

- Коды БЧХ

4. Теория перечисления Пойа
   - Действие группы на множестве
   - Применение леммы Бернсайда для решения комбинаторных задач

5. Частично упорядоченные множества
   - Частично упорядоченные множества
   - Операции над ч.у. множествами
   - Линеаризация

6. **Алгебраические решётки**
   - Решётки

Ч

=