Прикладная алгебра

Лекции для III потока, 5-й семестр

Лектор — *Гуров Сергей Исаевич*

ассистент — *Кропотов Дмитрий Александрович*

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.
- *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.
- *Нефедов В.Н., Осипова В.А.* Курс дискретной математики. — М.: Изд-во МАИ, 1992.
- *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. — М.: Мир, 1976.

Раздел I

Раздел II

Раздел III

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 $\mod p$.

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

$\mathbb{F}_3$:

$+$	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

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

$\mathbb{F}_3$:

+	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 $\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 0$. 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 $\underbrace{1 + \ldots + 1}_{k \text{ раз}} = 0$. Тогда

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

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

$\{\,1,\,2,\,\ldots,\,\operatorname{char}\Bbbk - 1,\,0\,\}$ — минимальное подполе в поле $\Bbbk$.

Если все суммы вида $1 + \ldots + 1$ 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.

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 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

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

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

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

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

— *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

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

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

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

— *мультипликативная группа поля* $\mathbb{F}_p$.

Утверждение

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

Как любая конечная циклическая группа, $\mathbb{F}_p^*$ содержит *генератор* = *примитивный элемент* α:

- любой элемент $\beta \in \mathbb{F}_p^*$ является некоторой его натуральной степенью — т.е. $\beta = \alpha^i$, $i \in \{1, \ldots, p-1\}$;
- причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

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

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

Утверждение

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

Как любая конечная циклическая группа, $\mathbb{F}_p^*$ содержит *генератор* = *примитивный элемент* α:

- любой элемент $\beta \in \mathbb{F}_p^*$ является некоторой его натуральной степенью — т.е. $\beta = \alpha^i$, $i \in \{1, \ldots, p-1\}$;
- причём $1 = \alpha^{p-1}$ — т.е. $\alpha^i \neq 1$ для $1 \leqslant i \leqslant p-2$.

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:

- $\varphi(n) \leqslant n - 1$ и $\varphi(p) = p - 1$, если p — простое;
- $\varphi(n^m) = n^{m-1}\varphi(n)$, 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 $d = \text{НОД}(m, n)$.

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:

- $\varphi(n) \leqslant n - 1$ и $\varphi(p) = p - 1$, если p — простое;
- $\varphi(n^m) = n^{m-1}\varphi(n)$, 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 $d = \text{НОД}(m, n)$.

Пример

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

Первые значения функции Эйлера и степени примитивного элемента

Первые 99 значений функции Эйлера
(последовательность A000010 в OEIS)

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Первые значения функции Эйлера и степени примитивного элемента

Первые 99 значений функции Эйлера
(последовательность A000010 в OEIS)

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Для примитивного элемента α мультипликативной группы $\mathbb{F}_p^*$

$$\alpha^{p-1} = 1 \Rightarrow \alpha^p = \alpha^1 = \alpha; \quad \alpha^{-1} = \alpha^{-1} \cdot \alpha^{p-1} = \alpha^{p-2}.$$

Например, в $\mathbb{F}_5$ будет $\alpha^{-1} \neq \alpha^4$,

Первые значения функции Эйлера и степени примитивного элемента

Первые 99 значений функции Эйлера
(последовательность A000010 в OEIS)

$\varphi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Для примитивного элемента α мультипликативной группы $\mathbb{F}_p^*$

$$\alpha^{p-1} = 1 \Rightarrow \alpha^p = \alpha^1 = \alpha; \quad \alpha^{-1} = \alpha^{-1} \cdot \alpha^{p-1} = \alpha^{p-2}.$$

Например, в $\mathbb{F}_5$ будет $\alpha^{-1} \neq \alpha^4$, $\alpha^{-1} = \alpha^3$.

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 $q \mid (p-1)$.

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 $q \mid (p-1)$.

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 $q \mid (p-1)$.

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

Если α — примитивный элемент поля $\mathbb{F}_p$, то любой другой его примитивный элемент может быть получен как степень α^k, где k — целое число, взаимно простое с $p-1$.

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 $\mathbb{F}_2 = \langle \{0,1\}, +_{\bmod 2}, \cdot_{\bmod 2} \rangle$.
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 $\mathbb{F}_2 = \langle \{0, 1\}, +_{\mathrm{mod}\ 2}, \cdot_{\mathrm{mod}\ 2} \rangle$.
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 $x^2 + ax + 1$.
Если $a = 0$, то $x^2 + 1 = (x + 1)^2$.
При $a = 1$ получаем неприводимый многочлен.
$\therefore$ 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: это

$$x^3 + x^2 + 1 \ \text{ и } \ x^3 + x + 1\,.$$

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?

Найдены многочлены, у которых нет линейных 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:

$$
\begin{array}{lr}
x & 2x \\
x+1 & 2x+1 \\
x+2 & 2x+2
\end{array}
$$

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:

$$\begin{array}{lr} x & 2x \\ x+1 & 2x+1 \\ x+2 & 2x+2 \end{array}$$

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:

$$\begin{array}{lr} x & 2x \\ x+1 & 2x+1 \\ x+2 & 2x+2 \end{array}$$

Какие из них неприводимы? Все!

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

$$\begin{array}{ll} x^2+1 & 2x^2+2 \\ x^2+x+2 & 2x^2+x+1 \\ x^2+2x+2 & 2x^2+2x+1 \end{array}$$

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.

— докажем позже.

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.

— докажем позже.

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.

— докажем позже.

Вопрос

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

Ответ: нет эффективных алгоритмов 

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.

— докажем позже.

Вопрос

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

Ответ: нет эффективных алгоритмов 
(из таблиц, алгоритм из 5-й главы «Алгебры» Ван дер Вардена, алгоритм Берлекемпа...)

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.

— докажем позже.

Вопрос

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

Ответ: нет эффективных алгоритмов 
(из таблиц, алгоритм из 5-й главы «Алгебры» Ван дер Вардена, алгоритм Берлекемпа...)

Если многочлен не имеет корней, это ещё не значит, что он неприводим.

Построение конечных полей

— с использованием неприводимых многочленов.

1. Выбираем простое p и фиксируем поле
$$\mathbb{F}_p = \langle \{ \bar{0}, \bar{1}, \ldots, \overline{p-1} \}, +_{\bmod p}, \cdot_{\bmod p} \rangle.$$
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 поля $\mathbb{F}_3^2$.

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 поля $\mathbb{F}_3^2$.

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 поля $\mathbb{F}_3^2$.

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.

Число неприводимых многочленов в поле F_p^n

Неприводимый многочлен $f(x)$ — в поле F_p^n — примитивный элемент мультипликативной группы F_p^{n*}, т.е.

1. $(f(x))^{p^n-1} = 1$ и $(f(x))^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = (f(x))^i$, $i = 0, 1, \ldots, p^n - 1$.

Число неприводимых многочленов в поле F_p^n

Неприводимый многочлен $f(x)$ — в поле F_p^n — примитивный элемент мультипликативной группы F_p^{n*}, т.е.

1. $(f(x))^{p^n-1} = 1$ и $(f(x))^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = (f(x))^i$, $i = 0, 1, \ldots, p^n - 1$.

Если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое число взаимно простое с $q - 1$ $\Rightarrow$ количество различных примитивных элементов в поле F_p^n равно $\varphi(p^n - 1)$.

Число неприводимых многочленов в поле F_p^n

Неприводимый многочлен $f(x)$ — в поле F_p^n — примитивный элемент мультипликативной группы F_p^{n*}, т.е.

1. $(f(x))^{p^n-1} = 1$ и $(f(x))^i \neq 1$ для $0 < i < p^n - 1$,
2. для любого многочлена $g(x) \in \mathbb{F}_p^{n*}$ найдётся степень i такая, что $g(x) = (f(x))^i$, $i = 0, 1, \ldots, p^n - 1$.

Если α — примитивный элемент поля $GF(q)$, то любой другой примитивный элемент может быть получен как степень α^k, где k — целое число взаимно простое с $q - 1 \Rightarrow$ количество различных примитивных элементов в поле F_p^n равно $\varphi(p^n - 1)$.

Например, в поле из 64 элементов (F_2^6)

$$\varphi(63) = \varphi(3^2 \cdot 7) = 3 \cdot 2 \cdot 6 = 36$$

примитивных элементов = неприводимых многочленов.

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

- Линеаризация
- Что надо знать

5. **Алгебраические решётки**
   - Решётки: определение, основные свойства
   - Модулярные и дистрибутивные решётки
   - Применение теории решёток к задаче классификации
   - Что надо знать

Алгоритм Евклида для нахождения НОД(a, b) натуральных чисел a и b ($a \geqslant b$)

— он понадобится для вычислений в конечных полях.

Наблюдение: если d — общий делитель пары чисел (a, b) $\Leftrightarrow$ d — общий делитель чисел $(a - b, b)$.

Алгоритм Евклида для нахождения НОД(a, b) натуральных чисел a и b ($a \geqslant b$)

— он понадобится для вычислений в конечных полях.

Наблюдение: если d — общий делитель пары чисел (a, b) $\Leftrightarrow$ d — общий делитель чисел $(a - b, b)$.

Отсюда:

- пары чисел (a, b) $(a - kb, b)$, $k \in \mathbb{Z}$ имеет одинаковые общие делители;

Алгоритм Евклида для нахождения НОД(a, b) натуральных чисел a и b ($a \geqslant b$)

— он понадобится для вычислений в конечных полях.

Наблюдение: если d — общий делитель пары чисел (a, b) $\Leftrightarrow$ d — общий делитель чисел $(a - b, b)$.

Отсюда:

- пары чисел (a, b) $(a - kb, b)$, $k \in \mathbb{Z}$ имеет одинаковые общие делители;
- вместо $a - kb$ можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{Z}$, $0 \leqslant r_0 < b$;

Алгоритм Евклида для нахождения НОД(a, b) натуральных чисел a и b ($a \geqslant b$)

— он понадобится для вычислений в конечных полях.

Наблюдение: если d — общий делитель пары чисел $(a, b) \Leftrightarrow$ d — общий делитель чисел $(a - b, b)$.

Отсюда:

- пары чисел (a, b) $(a - kb, b)$, $k \in \mathbb{Z}$ имеет одинаковые общие делители;
- вместо $a - kb$ можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{Z}$, $0 \leqslant r_0 < b$;
- затем, переставив числа в паре, можно повторить процедуру; она закончится, т.к. числа в паре уменьшаются, но остаются неотрицательными.

Алгоритм Евклида для нахождения НОД(a, b) натуральных чисел a и b ($a \geqslant b$)

— он понадобится для вычислений в конечных полях.

Наблюдение: если d — общий делитель пары чисел (a, b) $\Leftrightarrow$ d — общий делитель чисел $(a-b, b)$.

Отсюда:

- пары чисел (a, b) $(a-kb, b)$, $k \in \mathbb{Z}$ имеет одинаковые общие делители;
- вместо $a-kb$ можно взять остаток r_0 от деления нацело a на b: $a = bq + r_0$, $q \in \mathbb{Z}$, $0 \leqslant r_0 < b$;
- затем, переставив числа в паре, можно повторить процедуру; она закончится, т.к. числа в паре уменьшаются, но остаются неотрицательными.

В результате за конечное число шагов образуется пара $(r_n, 0)$. Ясно, что НОД$(a, b) = r_n$.

Алгоритм Евклида: общая схема

НОД$(a, b) =?$

Шаг (-2): $r_{-2} = a$ — полагаем для удобства;

Шаг (-1): $r_{-1} = b$ — полагаем для удобства;

Шаг 0: $r_{-2} = r_{-1}q_0 + r_0$ — делим r_{-2} на r_{-1}, остаток r_0;

Шаг 1: $r_{-1} = r_0 q_1 + r_1$ — делим r_{-1} на r_0, остаток r_1;

... ...

Шаг n: $r_{n-2} = r_{n-1}q_n + r_n$ — делим r_{n-2} на r_{n-1}, остаток r_n;

Шаг $n+1$: $r_{n-1} = r_n q_{n+1} + 0$ — деление нацело $\Rightarrow$ останов.

Всегда $r_{-2} \geqslant r_{-1} > r_0 > r_1 > \ldots > r_n \geqslant 1$.

НОД$(a, b) = r_n$.

Алгоритм Евклида: пример

$\underline{\text{НОД}(252, 105) = ?}$

Алгоритм Евклида: пример

НОД$(252, 105) = ?$

Шаг (-2): $r_{-2} = 252;$

Шаг (-1): $r_{-1} = 105 \quad \Rightarrow (252, 105);$

Шаг 0: $252 = 105 \cdot 2 + 42 \quad \Rightarrow (105, 42);$

Шаг 1: $105 = 42 \cdot 2 + 21 \quad \Rightarrow (42, 21);$

Шаг 2: $42 = 21 \cdot 2 + 0 \quad \Rightarrow (21, 0).$

НОД$(252, 105) = 21.$

Алгоритм Евклида: пример

НОД$(252, 105) = ?$

Шаг (-2): $r_{-2} = 252;$

Шаг (-1): $r_{-1} = 105 \quad \Rightarrow (252, 105);$

Шаг 0: $252 = 105 \cdot 2 + 42 \quad \Rightarrow (105, 42);$

Шаг 1: $105 = 42 \cdot 2 + 21 \quad \Rightarrow (42, 21);$

Шаг 2: $42 = 21 \cdot 2 + 0 \quad \Rightarrow (21, 0).$

НОД$(252, 105) = 21.$

$$\text{НОД}(a, b, c) = \text{НОД}(a, (\text{НОД}(b, c)))$$

Теорема Безу и расширенный алгоритм Евклида

Теорема (Безу)

Если $d = \text{НОД}(a, b)$, *то найдутся* $x, y \in \mathbb{Z}$ *такие, что* $d = ax + by$.

Теорема Безу и расширенный алгоритм Евклида

Теорема (Безу)

Если $d = \text{НОД}(a, b)$, *то найдутся* $x, y \in \mathbb{Z}$ *такие, что* $d = ax + by$.

Доказательство

Рассматриваем алгоритм Евклида с конца к началу: $d = r_n = r_{n-2} - r_{n-1}q_n$, *затем, подставляя сюда значение* $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, *получаем*
$d = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$
для некоторых $\alpha, \beta \in \mathbb{Z}$ *и т.д.*

Теорема Безу и расширенный алгоритм Евклида

Теорема (Безу)

Если $d = \text{НОД}(a, b)$, *то найдутся* $x, y \in \mathbb{Z}$ *такие, что* $d = ax + by$.

Доказательство

Рассматриваем алгоритм Евклида с конца к началу: $d = r_n = r_{n-2} - r_{n-1}q_n$, *затем, подставляя сюда значение* $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$, *получаем*
$d = -q_n r_{n-3} + (1 + q_n q_{n-1})r_{n-2} = \alpha r_{n-3} + \beta r_{n-2}$
для некоторых $\alpha, \beta \in \mathbb{Z}$ *и т.д.*

Для нахождения по паре натуральных чисел (a, b) натурального d и целых x и y таких, что

$$d = \text{НОД}(a, b) = ax + ay,$$

применяют *расширенный алгоритм Евклида*.

Расширенный алгоритм Евклида

Расширенный алгоритм Евклида повторяет схему (простого) алгоритма Евклида, при в котором на каждом шаге:

- дополнительно вычисляются x_i и y_i по формулам

$$x_i = x_{i-2} - q_i x_{i-1}, \quad y_i = y_{i-2} - q_i y_{i-1}, \qquad i = 0, 1, \ldots;$$
$$x_{-2} = y_{-1} = 1\,.$$

- справедливо соотношение

$$\color{red}{r_i} = r_{i-2} - q_i r_{i-1} = (ax_{i-2} + by_{i-2}) - q_i(ax_{i-1} + by_{i-1}) =$$
$$= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = \color{red}{ax_i + by_i}.$$

Расширенный алгоритм Евклида: пример

Задача: найти натуральное d и целые x и y таких, что

$$d = \text{НОД}(a, b) = 252x + 105y.$$

Решение: имеем $x_i = x_{i-2} - q_i x_{i-1}, \quad y_i = y_{i-2} - q_i y_{i-1}$.
Сведём все вычисления в таблицу:

шаг i	r_{i-2}	r_{i-1}	q_i	r_i	x_i	y_i
-2				252	1	0
-1				105	0	1
0	252	105	2	42	1	-2
1	105	42	2	21	-2	5
2	42	21	2	0		

Ответ: $d = 21$, $x = -2$, $y = 5$.

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1. \qquad (*)$

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1. \qquad (*)$

Решение

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

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1. \qquad (*)$

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$
   Это решение перебором.
2. *Поскольку* $101y \equiv_{101} 0$, *вместо* $(*)$ *можно расширенным алгоритмом Евклида решать уравнение*
   $$4x + 101y = 1\,.$$

Задача

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

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$
   Это решение перебором.
2. *Поскольку* $101y \equiv_{101} 0$, *вместо* $(*)$ *можно расширенным алгоритмом Евклида решать уравнение*
   $$4x + 101y = 1\,.$$
   В результате работы алгоритма: $4 \cdot 76 + 101 \cdot (-3) = 1.$

Задача

В поле $\mathbb{Z}/(101)$ *решить уравнение* $4x = 1. \qquad (*)$

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots; \quad x = 304/4 = 76.$
   Это решение перебором.
2. *Поскольку* $101y \equiv_{101} 0$, *вместо* $(*)$ *можно расширенным алгоритмом Евклида решать уравнение*
   $$4x + 101y = 1\,.$$
   В результате работы алгоритма: $4 \cdot 76 + 101 \cdot (-3) = 1.$

Аналогично решаются уравнения

$$ax = c, \qquad ax + by = c$$

(перед решением коэффициенты a, b и c надо поделить на НОД).

Нахождение обратных элементов в расширениях полей $\mathbb{F}_n$

Алгоритм Евклида (а также его расширенная версия) остаётся справедливым в любом евклидовом кольце.

Нахождение обратных элементов в расширениях полей $\mathbb{F}_n$

Алгоритм Евклида (а также его расширенная версия) остаётся справедливым в любом евклидовом кольце.

Пусть $f(x)$ – неприводимый многочлен степени n над $\mathbb{F}_p$. Тогда обратный элемент h для некоторого многочлена g в поле $\mathbb{F}_p^n = \mathbb{F}_p[x]/(f(x))$ определяется условием

$$g(x) \cdot h(x) = 1 \quad \text{или} \quad f(x) \cdot a(x) + g(x) \cdot h(x) = 1\,.$$

Оно может быть решено путем применения расширенного алгоритма Евклида для пары многочленов (f, g).

Заметим, что решение данного уравнения существует всегда: f – неприводимый полином, $\deg g < \deg f \ \Rightarrow$ НОД$(f, g) = 1$.

Пример: найти $(x^2+x+3)^{-1}$ в поле $\mathbb{F}_7[x]/(x^4+x^3+x^2+3)$

Применяя расширенный алгоритм Евклида, решим уравнение

$$(x^4+x^3+x^2+3)\cdot a(x)+(x^2+x+3)\cdot b(x) \;=\; 1 \qquad (*)$$

Шаг 0.
$$\begin{aligned} r_{-2}(x) &= x^4+x^3+x^2+3,\\ r_{-1}(x) &= x^2+x+3,\\ y_{-2}(x) &= 0,\\ y_{-1}(x) &= 1. \end{aligned}$$

Шаг 1.
$$\begin{aligned} r_{-2}(x) &= r_{-1}(x)q_0(x)+r_0(x),\\ q_0(x) &= x^2+5,\\ r_0(x) &= 2x+2,\\ y_0(x) &= y_{-2}(x)-y_{-1}(x)q_0(x) = -q_0(x) = -x^2-5. \end{aligned}$$

Шаг 2.
$$\begin{aligned} r_{-1}(x) &= r_0(x)q_1(x)+r_1(x),\\ q_1(x) &= 4x,\\ r_1(x) &= 3, \quad \deg\, r_1(x) \;=\; 0\\ y_1(x) &= y_{-1}(x)-y_0(x)q_1(x) = 1+4x(x^2+5) =\\ &= 4x^3+6x+1. \end{aligned}$$

Пример...

Алгоритм заканчивает свою работу на шаге 2, т.к. $\deg r_1(x) = \deg 1$ (1 — многочлен в правой части $(*)$).

Пример...

Алгоритм заканчивает свою работу на шаге 2, т.к. $\deg r_1(x) = \deg 1$ (1 — многочлен в правой части $(*)$).

Замечание: итерациях алгоритма нет необходимости вычислять $x_i(x)$ (коэффициент при $x^4 + x^3 + x^2 + 3$), т.к. нас интересует только $y_i(x)$ — коэффициент при $x^2 + x + 3$.

Пример...

Алгоритм заканчивает свою работу на шаге 2, т.к. $\deg r_1(x) = \deg 1$ (1 — многочлен в правой части $(*)$).

Замечание: итерациях алгоритма нет необходимости вычислять $x_i(x)$ (коэффициент при $x^4 + x^3 + x^2 + 3$), т.к. нас интересует только $y_i(x)$ — коэффициент при $x^2 + x + 3$.

Остаток $r_1(x) = 3$, т.е. отличается от 1 на множитель-константу.

Чтобы получить решение уравнения $(*)$ вычисляем элемент $3^{-1} \equiv_7 5$ и домножаем на него y_1:

$$5 \cdot y_1(x) \;=\; 5 \cdot (4x^3 + 6x + 1) \;=\; 6x^3 + 2x + 5.$$

Ответ: в поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$

$$(x^2 + x + 3)^{-1} \;=\; 6x^3 + 2x + 5.$$

Раздел I

1. **Конечные поля или поля Галуа**
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. **Коды, исправляющие ошибки**
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

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: $\Bbbk \times V \xrightarrow{\cdot} V$,

Векторное пространство: определение

Определение

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

- $V = \{0, v, \dots\}$ — 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 $\Bbbk$.

Применение линейной алгебры к изучению конечных полей

Лемма

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

Применение линейной алгебры к изучению конечных полей

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 $\Bbbk$.*

Применение линейной алгебры к изучению конечных полей

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

Поле $\mathbb{F}_p^n$ есть конечная АС с элементами-многочленами

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

которую можно рассматривать как

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

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

  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 элемент* $\mathbb{F}_p^n$ *представим в виде линейной комбинации указанных векторов:*
  $\overline{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}} = a_0 \overline{1} + a_1 \overline{x} + \ldots + a_{n-1} \overline{x^{n-1}}$.
- *Обратно, пусть* $g(x) = b_0 \overline{1} + b_1 \overline{x} + \ldots + b_{n-1} \overline{x^{n-1}} = 0$. *Это означает, что многочлен* $g(x)$ *степени* $n-1$ *делится на некоторый многочлен* n*-й степени, что возможно лишь при* $b_0 = b_1 = \ldots = b_{n-1} = 0$, *т.е. 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:

1. рассмотрим поле действительных чисел $\mathbb{R}$ и кольцо многочленов $\mathbb{R}[x]$ над ним;
2. в $\mathbb{R}[x]$ возьмём неприводимый многочлен $x^2 + 1$;
3. построим поле F 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:

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

F также и векторное пространство над $\mathbb{R}$; его базис — $\{\,\overline{1}, \overline{x}\,\}$ и каждый элемент F можно представить в виде $a\overline{1} + b\overline{x}$, $a, b \in \mathbb{R}$.
Поле F изоморфно полю комплексных чисел $\mathbb{C} = \{\,a + ib \mid a, b \in \mathbb{R}, i^2 = -1\,\}$: 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* $k \mid n$.

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* $\Bbbk_1$ *некоторой размерности* d *— значит, в нём* $|\Bbbk_1|^d$ *элементов.*

Для нашего случая: $p^n = (p^k)^d$, *что и означает* $k \mid n$.

Раздел I

1. **Конечные поля или поля Галуа**
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. **Коды, исправляющие ошибки**
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

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 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 $a(x) = a_0 + a_1x + \ldots + a_nx^n$ — 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. $a_0\overline{1} + a_1\overline{x} + \ldots + a_n\overline{x}^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} \equiv_p \overline{0}$,
т.е. $\overline{x}$ — корень $a(x)$, но тогда $\overline{x}$ является корнем и $a_n^{-1}a(x)$.
2. Пусть 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 $f(x)$ *— многочлен, а* $m(x)$ *— м.м. для* β *в некотором поле Галуа и* $f(\beta) = 0$.
Тогда $f(x)$ *делится на* $m(x)$.

Свойства минимальных многочленов...

Утверждение

Пусть $f(x)$ — многочлен, а $m(x)$ — м.м. для β в некотором поле Галуа 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

$$0 = f(\beta) = u(\beta)\underbrace{m(\beta)}_{=0} + v(\beta) = v(\beta)\,,$$

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 $\beta \in \mathbb{F}_p^n$ существует м.м. и его степень не превосходит n.

Свойства минимальных многочленов...

Утверждение

Для каждого $\beta \in \mathbb{F}_p^n$ существует м.м. и его 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 равна $n \Rightarrow$ эти элементы линейно зависимы, т.е. существуют такие не все равные 0 коэффициенты $c_0, \ldots, c_n$, что

$$c_0 + c_1\beta + \ldots + c_n\beta^n = 0,$$

т.е. β — корень многочлена $f(x) = c_0 + c_1x + \ldots + c_nx^n$.
М.м. 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

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

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

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 второго сомножителя корнями будут все ненулевые элементы, а у первого — 0.

Многочлены над конечным полем: свойства...

Теорема

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

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* $y^k - 1$*.*

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 $x^m - 1$.*

Теорема даёт возможность раскладывать многочлены $x^n - 1$ при составных n. Например, разложим $x^{15} + 1$ в поле характеристики 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 из* $\mathbb{F}_p[x]$ *являются делителями* $x^{p^n} - x$.

Многочлены над конечным полем...

Теорема

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

Доказательство

$n = 1$. *Убеждаемся, что $(x-a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: при $a = 0$ это очевидно, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1 = (x^p - x)/x$.*

Многочлены над конечным полем...

Теорема

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

Доказательство

$n = 1.$ *Убеждаемся, что $(x - a) \mid (x^p - x)$, где $a \in \mathbb{F}_p$: при $a = 0$ это очевидно, а в остальных случаях доказано, что a — корень многочлена $x^{p-1} - 1 = (x^p - x)/x$.*

$n > 1.$ *Строим по неприводимому и (без ограничения общности — нормированному) многочлену $f(x)$ степени n поле $\mathbb{F}_p^n$.*
В этом поле $\overline{x}$ — корень и $f(x)$, и $x^{p^n - 1} - 1$, причём $f(x)$ — м.м. для него.
По свойствам м.м., $x^{p^n-1} - 1$ делится на $f(x)$.

Многочлены над конечным полем...

Используя эту теорему, мы можем завершить разложение:

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

— берём над $\mathbb{F}_2$ все три неприводимых многочлены 4-й степени ($x(x^{15}+1) = x^{2^4}+x$) и единственный неприводимый многочлен 2-й степени ($x(x^3+1) = x^{2^2}+x$).

Многочлены над конечным полем...

Используя эту теорему, мы можем завершить разложение:

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

— берём над $\mathbb{F}_2$ все три неприводимых многочлены 4-й степени $(x(x^{15}+1) = x^{2^4}+x)$ и единственный неприводимый многочлен 2-й степени $(x(x^3+1) = x^{2^2}+x)$.

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:

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

— берём над $\mathbb{F}_2$ все три неприводимых многочлены 4-й степени $(x(x^{15}+1) = x^{2^4}+x)$ и единственный неприводимый многочлен 2-й степени $(x(x^3+1) = x^{2^2}+x)$.

Теорема

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

Доказательство

Пусть φ — неприводимый делитель $x^{p^n}-x$ степени k.
Тогда $F \overset{\text{def}}{=} \mathbb{F}_p/(\varphi)$ — поле, которое рассмотрим как векторное пространство над $\mathbb{F}_p$ с базисом $\left\{\overline{1}, \overline{x}, \ldots, \overline{x^{k-1}}\right\}$.

Многочлены над конечным полем...

Обозначим $\overline{x} = \alpha$. *Поскольку* $(x^{p^n} - x) \vdots \varphi$, *то в* F *имеем* $\alpha^{p^n} - \alpha = 0$.

Любой элемент F *выражается через базис:* $\beta = \sum\limits_{i=0}^{k-1} a_i \alpha^i$.

Возведя обе части этого равенства в степень p^n, *получим*

$$\beta^{p^n} = \left(\sum_{i=0}^{k-1} a_i \alpha^i\right)^{p^n} = \sum_{i=0}^{k-1} a_i \alpha^i = \beta,$$

т.е. β *— корень уравнения*

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

Итак, каждый элемент поля F *является корнем* $(*)$, *но у* $(*)$ *не более* p^n *различных корней, а* $|F| = p^k$.

$\therefore\ n \geqslant k$.

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* $\beta^{p^k-1} = 1$, *но* $\deg \beta = l \;\Rightarrow\; l \mid (p^k - 1)$.

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 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* $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$:

1. *все различны;*
2. *исчерпывают список корней* $\varphi(x)$.

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 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 β, β^p, ..., $\beta^{p^{n-1}}$:

1. *все различны;*
2. *исчерпывают список корней $\varphi(x)$.*

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

Доказательство

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

Многочлены над конечным полем...

Поскольку $a^p = a$ *для всех* $a \in \mathbb{F}_p$, *то справедливо*

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

т.е. для любого многочлена $f(x) \in \mathbb{F}_p[x]$ *выполняется равенство*

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

Отсюда:

$$\varphi(\beta) = 0 \Leftrightarrow \varphi(\beta)^p = 0 \Leftrightarrow \varphi(\beta^p) = 0$$

и $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ *— корни многочлена* $\varphi(x)$.

Многочлены над конечным полем...

(2) Осталось доказать, что все $\beta, \beta^p, \ldots, \beta^{p^{n-1}}$ *различны, и тогда (поскольку многочлен степени* n *имеет не более* n *корней) можно утверждать, что найдены* ***все*** *корни многочлена* $\varphi(x)$.

Предположим, что $\beta^{p^l} = \beta^{p^k}$ *и без ограничения общности* $l < k$.

Имеем:

1. $\beta^{p^n} = \beta$;
2. *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 теоремы «Все неприводимые многочлены n*-й степени над* $\mathbb{F}_p$ *являются делителями* $x^{p^n} - x$*» получаем* $n-k+l \geqslant n \;\Rightarrow\; l \geqslant k$ *— противоречие.*

Многочлены над конечным полем: решение уравнений

Пример

Рассмотрим неприводимый над $\mathbb{F}_2$ многочлен $f(x) = x^4 + x^3 + 1$ и найдем его корни в расширении $\mathbb{F}_2^4$.

Многочлены над конечным полем: решение уравнений

Пример

Рассмотрим неприводимый над $\mathbb{F}_2$ многочлен $f(x) = x^4 + x^3 + 1$ и найдем его корни в расширении $\mathbb{F}_2^4$.
Один корень получаем немедленно: $\overline{x}$.

Многочлены над конечным полем: решение уравнений

Пример

Рассмотрим неприводимый над $\mathbb{F}_2$ многочлен $f(x) = x^4 + x^3 + 1$ и 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 неприводимый над $\mathbb{F}_2$ многочлен $f(x) = x^4 + x^3 + 1$ и 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, например, x^2 действительно корень $f(x)$:

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

Как решать уравнения, когда корней нет?

Пусть надо решить уравнение

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n = 0, \quad a_0, a_1, \ldots, a_n \in \mathbb{F}_p.$$

Как решать уравнения, когда корней нет?

Пусть надо решить уравнение

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n = 0, \quad a_0, a_1, \ldots, a_n \in \mathbb{F}_p.$$

Если $f(x)$ —

- неприводимый многочлен, то строим поле $\mathbb{F}_p[x]/(f)$, в котором корнями $f(x)$ будут
$$\overline{x},\ \overline{x^p},\ \ldots,\ \overline{x^{p^{n-1}}};$$

Как решать уравнения, когда корней нет?

Пусть надо решить уравнение

$$f(x) = a_0 + a_1x + \ldots + a_nx^n = 0, \quad a_0, a_1, \ldots, a_n \in \mathbb{F}_p.$$

Если $f(x)$ —

- неприводимый многочлен, то строим поле $\mathbb{F}_p[x]/(f)$, в котором корнями $f(x)$ будут
$$\overline{x},\ \overline{x^p},\ \ldots,\ \overline{x^{p^{n-1}}};$$
- имеет делители, то раскладываем $f(x)$ на неприводимые множители и находим их корни как в п. 1), полученные корни объединяем.
Одновременно строится минимальное поле характеристики p, в котором данный многочлен $f(x)$ раскладывается на линейные множители.

Как решать уравнения, когда корней нет?

Пусть надо решить уравнение

$$f(x) = a_0 + a_1x + \ldots + a_nx^n = 0, \quad a_0, a_1, \ldots, a_n \in \mathbb{F}_p.$$

Если $f(x)$ —

- неприводимый многочлен, то строим поле $\mathbb{F}_p[x]/(f)$, в котором корнями $f(x)$ будут
$$\overline{x},\ \overline{x^p},\ \ldots,\ \overline{x^{p^{n-1}}};$$
- имеет делители, то раскладываем $f(x)$ на неприводимые множители и находим их корни как в п. 1), полученные корни объединяем.
  Одновременно строится минимальное поле характеристики p, в котором данный многочлен $f(x)$ раскладывается на линейные множители.

В конце данного раздела будет дан алгоритм нахождения всех корней многочлена $f(x)$ над полем Галуа $\mathbb{F}_p$ для общего случая.

Раздел I

Раздел II

Раздел III

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):

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1$$

Удобнее всего это сделать, если взять многочлен $f(x) = x^4 + x + 1$ (почему?).

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):

$$x^4 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x^3 + x^2 + x + 1$$

Удобнее всего это сделать, если взять многочлен $f(x) = x^4 + x + 1$ (почему?).
Будем задавать элементы $\mathbb{F}_2^4$ наборами коэффициентов многочлена-остатка 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 $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4+x+1)$

$\mathbf{x^4 = x + 1}$ 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:

$$(x^3 + x + 1) \cdot (x^2 + x + 1) = x^2$$

— как получить это без перемножения?

$$(1, 1, 0, 1) \cdot (1, 1, 1, 0) =?$$

— то же в векторной форме...

$$\alpha = x$$

$$\alpha^7 \alpha^{10} = \alpha^{17} = \alpha^2$$

— по векторной форме взять из таблицы!.

Порядок элемента конечной группы

Лемма (о порядке элемента конечной группы)

Пусть m — *максимальный порядок элемента в конечной абелевой группе* G.
Тогда порядок любого элемента $x \in \mathbf{G} = \langle G, \circ, e \rangle$ *делит* m.

Порядок элемента конечной группы

Лемма (о порядке элемента конечной группы)

Пусть m — максимальный порядок элемента в конечной абелевой группе G.
Тогда порядок любого элемента $x \in \mathbf{G} = \langle G, \circ, e \rangle$ делит m.

Доказательство

Группа G однозначно разлагается в прямую сумму циклических групп, порядки которых являются степенями простых чисел. Для каждого простого делителя p_i порядка группы найдем циклическую группу максимального порядка p^{k_i}.
Обозначим произведение чисел p^{k_i} через M. Для любого $x \in G$ выполняется $x^M = e$, т.е. порядок x делит M.
Но произведение всех выбранных циклических групп имеет порядок M. Поэтому $m = M$.

Пути доказательства

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

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). 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 $\mathbb{F}_p$

Будем доказывать существование нормированного неприводимого многочлена. Для таких многочленов выполняется аналог основной теоремы арифметики: *каждый нормированный многочлен однозначно разлагается на произведение степеней неприводимых многочленов*.

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

Будем доказывать существование нормированного неприводимого многочлена. Для таких 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 1 однозначно определяет сомножители.*

Подсчёт неприводимых нормированных многочленов

Подсчёт неприводимых нормированных многочленов

Лемма (о числе d_n)

Если d_n — число неприводимых нормированных многочленов из $\mathbb{F}_p^n$, то

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

Подсчёт неприводимых нормированных многочленов

Лемма (о числе d_n)

Если d_n — число неприводимых нормированных многочленов из $\mathbb{F}_p^n$, то

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

Доказательство

Занумеруем $i = 1, \dots, d_n$ все неприводимые нормированные многочлены степени n и сопоставим им формальную переменную $f_{i,n}$ $\Rightarrow$ произвольному такому многочлену однозначно сопоставлен моном (многочлен степени n_j берётся в степени s_j):

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

Подсчёт неприводимых нормированных многочленов...

Доказательство

Поэтому все нормированные многочлены перечисляются формальным бесконечным произведением

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

(раскрыты скобки и бесконечное произведение записано в виде формального ряда).
Сделаем замену переменных $f_{i,n} = t^n$, которая делает все многочлены одной степени неразличимыми.

Подсчёт неприводимых нормированных многочленов...

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

Приведение подобных приведёт к тому, что:

в правой части $(*)$ *будет ряд от переменной* t.

Коэффициент при t^n *в этом ряде равен числу нормированных многочленов степени* n*, т.е.* p^n*:*

$$\sum_{n=0}^{\infty} p^n t^n.$$

Подсчёт неприводимых нормированных многочленов...

$$\prod_{i,n}\left(\sum_{k=0}^{\infty} f_{i,n}^{k}\right) = \sum_{n=0}^{\infty} p^n t^n \qquad (*)$$

в левой части *все неприводимые многочлены степени* n *дадут одинаковый множитель (сумму бесконечной геометрической прогрессии со знаменателем* t^n*) и* $(*)$ *превращается в*

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

Подсчёт неприводимых нормированных многочленов...

По формуле суммы бесконечной геометрической прогрессии:

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

Прологарифмируем («−» в обеих частях равенства сокращаются, $n \mapsto m$):

$$\sum_m d_m \ln(1-t^m) = \ln(1-pt)\,.$$

Продифференцируем по t («−» в обеих частях равенства сокращаются):

$$\sum_m d_m \frac{mt^{m-1}}{1-t^m} = \frac{p}{1-pt}\,.$$

Подсчёт неприводимых нормированных многочленов...

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

Снова воспользуемся формулой суммой геометрической прогрессии:

$$\sum_{m,k} d_m m t^{m-1} t^{mk} = \sum_n p^{n+1} t^n.$$

Умножаем на t *обе части равенства:*

$$\sum_{m,k} m d_m t^{m(k+1)} = \sum_n p^n t^n.$$

Равенство коэффициентов при одинаковых степенях t *и есть утверждение леммы* ($\sum\limits_{m|n} m \cdot d_m = p^n$).

Важные замечания

Замечание (о существовании неприводимых многочленов)

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

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

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

Важные замечания

Замечание (о существовании неприводимых многочленов)

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

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

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

Замечание (о среднем числе неприводимых многочленов)

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.

Изоморфизм полей Галуа с одинаковым числом элементов

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.

Изоморфизм полей Галуа с одинаковым числом элементов

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

Раздел III

- Линеаризация
- Что надо знать

5 Алгебраические решётки

- Решётки: определение, основные свойства
- Модулярные и дистрибутивные решётки
- Применение теории решёток к задаче классификации
- Что надо знать

Кольцо $\mathbb{F}_p/(f)$

В приложениях часто используется кольцо многочленов $GF(p) = \mathbb{F}_p[x]/(f)$ 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 многочленов $GF(p) = \mathbb{F}_p[x]/(f)$ 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 $GF(p)$ — векторное пространство над $\mathbb{F}_p$ многочленов степени $\leqslant \deg f$.

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

Нормированный делитель порождающего элемента идеала

Теорема

Пусть φ — *неприводимый нормированный многочлен, который делит* f. *Тогда*

1. *совокупность всех вычетов, кратных* φ, *образует идеал в кольце классов вычетов по модулю* f:
$$I_\varphi \stackrel{\text{def}}{=} \{t \cdot \varphi\} \lhd \mathbb{F}_p[x]/(f).$$
2. φ — *единственный нормированный многочлен минимальной степени в* I_φ.

Нормированный делитель порождающего элемента идеала

Теорема

Пусть φ — неприводимый нормированный многочлен, который делит f. Тогда

1. *совокупность всех вычетов, кратных φ, образует идеал в кольце классов вычетов по модулю f:*
$$I_\varphi \overset{\text{def}}{=} \{t \cdot \varphi\} \lhd \mathbb{F}_p[x]/(f).$$
2. *φ — единственный нормированный многочлен минимальной степени в I_φ.*

Доказательство

$$(f) = tf, \quad t, s, \varphi \in \mathbb{F}_p[x], \quad \deg f \geqslant \deg \varphi = k$$
$$\varphi = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1} + 1 \cdot x^k, \quad f = \psi\varphi.$$

Нормированный делитель...

Проверим, что I_φ — идеал.

1.

$$\begin{cases} \overline{g} \in I_\varphi \\ \overline{h} \subseteq \overline{g} \end{cases} \Leftrightarrow \begin{cases} \overline{g} = u\varphi \\ \overline{h} = vg = vu\varphi \end{cases} \Rightarrow \overline{h} \in I_\varphi.$$

2.

$$\overline{g}, \overline{h} \in I_\varphi \Leftrightarrow \begin{cases} \overline{g} = u\varphi \\ \overline{h} = v\varphi \end{cases}$$

$$\overline{g} + \overline{h} = (u+v)\varphi \in I_\varphi.$$

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

$$\omega = b_0 + b_1 x + \ldots + x^m .$$

Тогда:

$$\omega \in I_\varphi \Leftrightarrow \omega = t\varphi \Rightarrow \deg \omega = m \geqslant \deg \varphi.$$

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* $n - k$.

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 неоторым полем.
- Фиксируем некоторый базис F.
- Тогда $F \cong F^n = \{ (a_0, \ldots, a_{n-1}) \mid a_i \in F, i = 0, 1, \ldots, n - 1 \}$ — 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 $\mathbb{F}_p$ в базисе $\{\,\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\,\}$.

Циклический сдвиг координат в этом базисе равносилен умножению на x:

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

Идеал в $\mathbb{F}_p/(x^n-1)$ — циклическое пространство

Теорема

Пусть $I \subseteq \mathbb{F}_p/(x^n-1)$.
Тогда I *— циклическое пространство* $\Leftrightarrow$ $I \lhd \mathbb{F}_p/(x^n-1)$.

Идеал в $\mathbb{F}_p/(x^n-1)$ — циклическое пространство

Теорема

Пусть $I \subseteq \mathbb{F}_p/(x^n-1)$.
Тогда I *— циклическое пространство* $\Leftrightarrow$ $I \lhd \mathbb{F}_p/(x^n-1)$.

Доказательство

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

Идеал в $\mathbb{F}_p/(x^n - 1)$ — циклическое пространство

Теорема

Пусть $I \subseteq \mathbb{F}_p/(x^n - 1)$.
Тогда I *— циклическое пространство* $\Leftrightarrow$ $I \lhd \mathbb{F}_p/(x^n - 1)$.

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 $g \cdot \overline{x}$, $g \cdot \overline{x^2}, \dots$ *— циклические сдвиги, т.е. также принадлежат* I.
  Значит, $g \cdot \overline{f} \in I$ *для любого многочлена* f, *поэтому* I *— идеал.*

Примитивные корни

Показано: *любой многочлен с коэффициентами из* $\mathbb{F}_p$ *разлагается на* *линейные* *множители в некотором поле* $\mathbb{F}_q$ *характеристики* p.

Пусть $\mathbb{F}_q$ — поле характеристики p, в котором разлагается многочлен $x^n - 1$.

Примитивные корни

Показано: *любой многочлен с коэффициентами из* $\mathbb{F}_p$ *разлагается на* *линейные* *множители в некотором поле* $\mathbb{F}_q$ *характеристики* p.

Пусть $\mathbb{F}_q$ — поле характеристики p, в котором разлагается многочлен $x^n - 1$. Справедливо:

- 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 циклической группе $\mathbb{F}_q^*$ делит n.

Вывод: корни уравнения $x^n - 1 = 0$ образуют *группу корней степени* n *из единицы* — подгруппу в $\mathbb{F}_q^*$.

Эта подгруппа также циклическая; её порождающие элементы называются *примитивными корнями степени* n.

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

Подгруппа в циклической группе существует iff её порядок делит порядок циклической группы $\Rightarrow$

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

Подгруппа в циклической группе существует iff её порядок делит порядок циклической группы $\Rightarrow$ поле $\mathbb{F}_q$ содержит группу корней из единицы степени n iff $n \mid q - 1$.

Разложение $x^n - 1$ над $\mathbb{F}_p$:

1. в поле $\mathbb{F}_q$ на линейные множители (корни степени n из единицы);
2. в поле $\mathbb{F}_p$ на неприводимые множители.

Какие корни из единицы будут неприводимыми делителями $x^n - 1$ в $\mathbb{F}_p$?

Если β — корень $f(x)$, то β^p, β^{p^2} и т.д. — также его корни $\Rightarrow$ количество и степени неприводимых делителей $x^n - 1$ можно найти, разбив $\mathbb{F}_p$ на орбиты отображения $t \mapsto pt \mod n$.

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:

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

Поэтому $x^{15} - 1$ разлагается в произведение

- одного неприводимого многочлена степени 1,
- одного неприводимого многочлена степени 2,
- трех неприводимых многочленов степени 4.

Конкретно (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

Раздел III

- Линеаризация
- Что надо знать

5. Алгебраические решётки
   - Решётки: определение, основные свойства
   - Модулярные и дистрибутивные решётки
   - Применение теории решёток к задаче классификации
   - Что надо знать

Задача (ПГ-1 (Теорема Вильсона))

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

Задача (ПГ-1 (Теорема Вильсона))

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

Решение

$p = 2$: — *утверждение тривиально.*

Задача (ПГ-1 (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

- $\mathbb{F}_{17}^* = \{1, 2, \ldots, 16\} = \langle 3 \rangle$:
  $3^1 = 1,\ 3^2 = 9,\ 3^3 = 27 \equiv_{17} 10,\ 30 \equiv_{17} 13,\ 39 \equiv_{17} 5 \ldots$;
- $G = \{1^{2006}, 2^{2006}, \ldots, 16^{2006}\}$ *— 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 (ПГ-2)

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

Задача (ПГ-2)

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 (ПГ-3)

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

Задача (ПГ-3)

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 (ПГ-4)

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

Задача (ПГ-4)

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 (ПГ-5)

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

Задача (ПГ-5)

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. $$\begin{array}{rrrr|l} x^3 & +2x^2 & +4x & +1 & x+3 \\ \cline{5-5} x^3 & +3x^2 & & & x^2+4x+2 \\ \cline{1-2} & 4x^2 & +4x & & \\ & 4x^2 & +2x & & \\ \cline{2-3} & & 2x & +1 & \\ & & 2x & +1 & \\ \cline{3-4} & & & 0 & \end{array}$$
3. *многочлен* $f_1 = x^2 + 4x + 2$ *неприводим в* $\mathbb{F}_5$

<u>*Ответ*</u>: $x^3 + 2x^2 + 4x + 1 = (x+3)(x^2+4x+2)$.

Задача (ПГ-6)

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

Задача (ПГ-6)

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:*

$$\begin{aligned} &x^2 + 1, \\ &x^2 + x + 2, \\ &x^2 + 2x + 2. \end{aligned}$$

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

Ответ: $(x^2 + 1)(x^2 + x + 2)$.

Задача (ПГ-7)

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

Задача (ПГ-7)

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:
$f(x) \neq 0$ ни при одном $x = 0, 1, 2, 3, 4$.
2. Перебирая неприводимые многочлены степени 2 над $\mathbb{F}_5$, получаем

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

Задача (ПГ-8)

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

Задача (ПГ-8)

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

Решение

$$\begin{aligned}
f_1(x) &= x^2 = x \cdot x,\\
f_2(x) &= x^2 + 1 = (x+1)^2,\\
f_3(x) &= x^2 + x = x \cdot (x+1),\\
f_4(x) &= x^2 + x + 1 \text{ — } \textit{неприводим}.
\end{aligned}$$

Задача (ПГ-9)

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

Задача (ПГ-9)

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

Решение

$$\begin{aligned}
f_1(x) &= x^3,\\
f_2(x) &= x^3 + 1 = (x+1)(x^2+x+1),\\
f_3(x) &= x^3 + x = x(x+1)^2,\\
f_4(x) &= x^3 + x^2 = x^2(x+1),\\
f_5(x) &= x^3 + x + 1 \text{ — неприводим},\\
f_6(x) &= x^3 + x^2 + 1 \text{ — неприводим},\\
f_7(x) &= x^3 + x^2 + x = x(x^2+x+1),\\
f_8(x) &= x^3 + x^2 + x + 1 = (x+1)^3.
\end{aligned}$$

Задача (ПГ-10)

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

Задача (ПГ-10)

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

Решение

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

Задача (ПГ-10)

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

Решение

Должно быть: $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$. *Перебором коэффициентов в выражении* $x^2 + bx + c$, *находим подходящие многочлены:*

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

Задача (ПГ-11)

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

Задача (ПГ-11)

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

Решение

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

Задача (ПГ-11)

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

Решение

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

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

Задача (ПГ-12)

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 (ПГ-12)

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 (*$= \mathbb{F}_7^2$*).*

Задача (ПГ-12)

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 (ПГ-13)

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 (ПГ-13)

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. $\underline{x^4 = x + 1}$

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

Ответ: 3.

2. $\underline{x^4 = x^3 + 1}$

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

Задача (ПГ-14)

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 (ПГ-14)

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* $\mathbb{F}_3$.

Решение

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

1. $\underline{d_7 = ?}$

$$\sum_{m|7} m d_m = 2^7 = 1 \cdot d_1 + 7 \cdot d_7 = 128.$$

$$d_1 = 2 \quad (x,\, x+1) \Rightarrow d_7 = (128-2)/7 = 126/7 = 18.$$

Задача (ПГ-15)

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

Задача (ПГ-15)

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 (ПГ-16)

Чему равна сумма всех элементов поля $\mathbb{F}_3^7$.

Задача (ПГ-16)

Чему равна сумма всех элементов поля $\mathbb{F}_3^7$.

Решение

Все элементы поля $\mathbb{F}_3^7$ являются корнями уравнения

$$x^{3^7} - x = x^{2187} - x = 0\,. \qquad (*)$$

По теореме Виета их сумма равна коэффициенту перед x^{2186}, т.е. 0.

Задача (ПГ-17)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ *построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.*
С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Задача (ПГ-17)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ *построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.*
С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Решение

$\operatorname{char} \mathbb{F}_3^2 = 3$, *поэтому* $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = f(x)$.

Задача (ПГ-17)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ *построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.*
С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Решение

$\operatorname{char} \mathbb{F}_3^2 = 3$, *поэтому* $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = f(x)$.

$\mathbb{F}_3^{2*}$ *содержит* $3^2 - 1 = 8$ *элементов и все они могут быть представлены как степени* $\alpha^i, i = \overline{1,8}$ *примитивного элемента* α.

Задача (ПГ-17)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(-2x^2 + x + 2)$ *построить таблицу соответствий между полиномиальным и степенным представлением для ненулевых элементов.*
С помощью данной таблицы вычислить выражение

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)}.$$

Решение

$\operatorname{char} \mathbb{F}_3^2 = 3$, *поэтому* $-2x^2 + x + 2 \equiv_3 x^2 + x + 2 = f(x)$.

$\mathbb{F}_3^{2*}$ *содержит* $3^2 - 1 = 8$ *элементов и все они могут быть представлены как степени* $\alpha^i, i = \overline{1,8}$ *примитивного элемента* α.
Если элемент x *окажется примитивным, то положим* $\alpha = x$ *и, поскольку вычисления в* $\mathbb{F}_3^2$ *проводятся по* $\bmod\ f(x)$, *будем иметь* $x^2 + x + 2 = 0 \Rightarrow x^2 = -x - 2 = 2x + 1$.

Решение (продолжение; $x^2 = 2x + 1$)

$$x^2 = 2x + 1\,,$$
$$x^3 = x \cdot x^2 = x(2x+1) = 2x^2 + x = 2(2x+1) + x = 2x + 2\,,$$
$$x^4 = x \cdot x^3 = x(2x+2) = 2x^2 + 2x = 2(2x+1) + 2x = 2\,,$$
$$x^5 = x \cdot x^4 = 2x\,,$$
$$x^6 = x \cdot x^5 = 2x^2 = 2(2x+1) = x + 2\,,$$
$$x^7 = x \cdot x^6 = x(x+2) = x^2 + 2x = 2x + 1 + 2x = x + 1\,,$$
$$x^8 = (\textit{проверочка})\; x \cdot x^7 = x(x+1) = x^2 + x = 2x + 1 + x = \mathbf{1}\,.$$

— т.е. x — примитивный элемент (повезло, иначе его пришлось бы искать);

Решение (продолжение; $x^2 = 2x + 1$)

$$x^2 = 2x + 1\,,$$
$$x^3 = x \cdot x^2 = x(2x+1) = 2x^2 + x = 2(2x+1) + x = 2x + 2\,,$$
$$x^4 = x \cdot x^3 = x(2x+2) = 2x^2 + 2x = 2(2x+1) + 2x = 2\,,$$
$$x^5 = x \cdot x^4 = 2x\,,$$
$$x^6 = x \cdot x^5 = 2x^2 = 2(2x+1) = x + 2\,,$$
$$x^7 = x \cdot x^6 = x(x+2) = x^2 + 2x = 2x + 1 + 2x = x + 1\,,$$
$$x^8 = (\textit{проверочка})\; x \cdot x^7 = x(x+1) = x^2 + x = 2x + 1 + x = \mathbf{1}\,.$$

— т.е. x — примитивный элемент (повезло, иначе его пришлось бы искать); теперь вычислим значение выражения ($2^8 = 256 \equiv_3 1$):

$$\frac{1}{2x+1} - \frac{(2x)^7(2)}{(x)^9(x+2)} = \frac{1}{x^2} - \frac{x^7}{x^9x^6} = \frac{x^8}{x^2} - \frac{x^7x^8}{x^{15}} =$$
$$= x^6 - 1 = x + 2 - 1 = x + 1.$$

Задача (ПГ-18)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(x^2+1)$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

Задача (ПГ-18)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(x^2+1)$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

Решение

В данном поле $x^2+1=0 \Rightarrow x^2=-1=2$.

1. Найдём порядок элемента $x \Rightarrow$ *проверим степени, являющиеся делителями* $3^2-1=8$, *т.е.* 2 *и* 4*:*

Задача (ПГ-18)

Для поля $\mathbb{F}_3^2 = \mathbb{F}_3[x]/(x^2+1)$ построить таблицу соответствий между полиномиальным и степенным представлением для всех ненулевых элементов поля.

Решение

В данном поле $x^2+1=0 \Rightarrow x^2=-1=2$.

1. Найдём порядок элемента x $\Rightarrow$ *проверим степени, являющиеся делителями* $3^2-1=8$, *т.е.* 2 *и* 4*:*

$$x^2 = 2, \;\; x^4 = 1.$$

Следовательно, элемент $\deg x = 4$ *и* x *не является примитивным элементом. Также не являются примитивными все степени элемента* x*:* $x^2=2$, $x^3=2x$, $x^4=1$.

Решение (продолжение)

2. *Найдём порядок элемента* $x+1$*:*

$$(x+1)^2 \;=\; x^2+2x+1 = 2x, \;\; (x+1)^4 \;=\; (2x)^2 \;=\; 2,$$

т.е. $x+1$ *оказался примитивным элементом.*

Решение (продолжение)

2. *Найдём порядок элемента $x+1$:*

$$(x+1)^2 = x^2+2x+1 = 2x, \quad (x+1)^4 = (2x)^2 = 2,$$

т.е. $x+1$ *оказался примитивным элементом. Его степени:*

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

Решение (продолжение)

2. *Найдём порядок элемента $x+1$:*

$$(x+1)^2 = x^2+2x+1 = 2x, \quad (x+1)^4 = (2x)^2 = 2,$$

т.е. $x+1$ *оказался примитивным элементом. Его степени:*

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

Заметим, что вычисление очередной степени α^{i+j} часто бывает удобным провести как $\alpha^i\cdot\alpha^j$, а не как $\alpha\cdot\alpha^{i+j-1}$.

Задача (ПГ-19)

В факторкольце $\mathbb{F}_3[x]/(x^4+1)$ *найти все элементы главного идеала* $\left(x^2+x+2\right)$.

Задача (ПГ-19)

В факторкольце $\mathbb{F}_3[x]/(x^4 + 1)$ найти все элементы главного идеала $\left(x^2 + x + 2\right)$.

Решение

1. Сначала проверим, является ли многочлен $f(x) = x^2 + x + 2$ делителем $x^4 + 1$

Задача (ПГ-19)

В факторкольце $\mathbb{F}_3[x]/(x^4+1)$ *найти все элементы главного идеала* $\left(x^2+x+2\right)$.

Решение

1. Сначала проверим, является ли многочлен $f(x) = x^2+x+2$ *делителем* x^4+1*:*

$$x^4+1 \;=\; (x^2+x+2)\cdot(x^2+2x+2).$$

— да! Поэтому искомый идеал составят многочлены кольца (т.е. степени не выше 3), кратные $f(x)$*:*

$$\left(x^2+x+2\right) \;=\; \left\{(x^2+x+2)\cdot(ax+b) \mid a,b\in\mathbb{F}_3\right\}.$$

Проведём умножение:

$$(x^2+x+2)\cdot(ax+b) \;=\; ax^3+(a+b)x^2+(2a+b)x+2b.$$

Решение (продолжение)

2. *Теперь, перебирая все возможные значения* $a, b \in \mathbb{F}_3$*, найдём все элементы идеала* (x^2+x+2)*:*

a	b	$ax^3+(a+b)x^2+(2a+b)x+2b$
0	0	0
0	1	x^2+x+2
0	2	$2x^2+2x+1$
1	0	x^3+x^2+2x
1	1	x^3+2x^2+2
1	2	x^3+x+1
2	0	$2x^3+2x^2+x$
2	1	$2x^3+2x+2$
2	2	$2x^3+x^2+1$

Задача (ПГ-20)

В поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$ *найти обратный элемент для* $x^2 + x + 3$.

Задача (ПГ-20)

В поле $\mathbb{F}_7[x]/(x^4 + x^3 + x^2 + 3)$ *найти обратный элемент для* $x^2 + x + 3$.

Решение

Проще всего обратный элемент можно найти путём решения уравнения

$$\underbrace{(x^4 + x^3 + x^2 + 3) \cdot a(x)}_{=0} + (x^2 + x + 3) \cdot b(x) = 1 \qquad (*)$$

с помощью расширенного алгоритма Евклида — тогда $b(x)$ *будет искомым обратным элементом.*
Замечание: вычислять коэффициент при $x^4 + x^3 + x^2 + 3$ $(x_i(x))$ *нет необходимости (нас интересует только коэффициент при* $x^2 + x + 3$, *т.е.* $y_i(x)$*).*

Решение (продолжение -1)

Шаг 0.

$$\begin{aligned} r_{-2}(x) &= x^4 + x^3 + x^2 + 3, \quad \textit{// Инициализация} \\ r_{-1}(x) &= x^2 + x + 3, \\ y_{-2}(x) &= 0, \\ y_{-1}(x) &= 1. \end{aligned}$$

Шаг 1.

$$r_{-2}(x) = r_{-1}(x) q_0(x) + r_0(x),$$

// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком

$$\begin{aligned} q_0(x) &= x^2 + 5, \\ r_0(x) &= 2x + 2, \\ y_0(x) &= y_{-2}(x) - y_{-1}(x) q_0(x) = -q_0(x) = -x^2 - 5. \end{aligned}$$

Шаг 2.

$$r_{-1}(x) = r_0(x) q_1(x) + r_1(x),$$

// Делим $r_{-1}(x)$ на $r_0(x)$ с остатком

$$\begin{aligned} q_1(x) &= 4x, \\ r_1(x) &= 3, \\ y_1(x) &= y_{-1}(x) - y_0(x) q_1(x) = 1 + 4x(x^2 + 5) = \\ &= 4x^3 + 6x + 1. \end{aligned}$$

Решение (продолжение -2)

*Алгоритм заканчивает свою работу на **Шаге 2**, т.к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части $(*)$: 1 — многочлен 0-й степени.*

Решение (продолжение -2)

*Алгоритм заканчивает свою работу на **Шаге 2**, т.к. степень 0 очередного остатка $r_1(x) = 3$ равна степени многочлена в правой части $(*)$: 1 — многочлен 0-й степени.*

В результате работы алгоритма получено:

$$(x^2 + x + 3)(4x^3 + 6x + 1) = r_1(x) = 3.$$

Решение (продолжение -2)

*Алгоритм заканчивает свою работу на **Шаге 2**, т.к. степень 0 очередного остатка* $r_1(x) = 3$ *равна степени многочлена в правой части* $(*)$*: 1 — многочлен 0-й степени.*

В результате работы алгоритма получено:

$$(x^2 + x + 3)(4x^3 + 6x + 1) = r_1(x) = 3.$$

Чтобы найти $b(x)$*, нужно домножить* $y_1(x)$ *на* $3^{-1} = 5$*:*

$$b(x) = 5y_1(x) = 5 \cdot (4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Решение (продолжение -2)

*Алгоритм заканчивает свою работу на **Шаге 2**, т.к. степень 0 очередного остатка* $r_1(x) = 3$ *равна степени многочлена в правой части* $(*)$*: 1 — многочлен 0-й степени.*

В результате работы алгоритма получено:

$$(x^2 + x + 3)(4x^3 + 6x + 1) = r_1(x) = 3.$$

Чтобы найти $b(x)$*, нужно домножить* $y_1(x)$ *на* $3^{-1} = 5$*:*

$$b(x) = 5y_1(x) = 5 \cdot (4x^3 + 6x + 1) = 6x^3 + 2x + 5.$$

Проверка: $b(x)(x^2 + x + 3) = (6x^3 + 2x + 5)(x^2 + x + 3) =$

$$= 6x^5 + 6x^4 + 6x^3 + 4x + 1 =$$

$$= 6x(-x^3 - x^2 - 3) + 6x^4 + 6x^3 + 4x + 1 = 1.$$

Задача (ПГ-21)

В поле $\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2+3x+3)$ *найти обратную для матрицы*

$$M = \begin{pmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{pmatrix}.$$

Задача (ПГ-21)

В поле $\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2+3x+3)$ *найти обратную для матрицы*

$$M = \begin{pmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{pmatrix}.$$

Решение

Для матриц размера 2×2 *обратная матрица записывается в виде*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

1. Сначала вычислим $\det M = ad - bc$ *с учётом* $x^2 = 2x+2$*:*

$$\det M = (3x+4)(3x+2)-(x+2)(x+3) = 4x^2+3x+3-x^2-1 =$$
$$= 3x^2+3x+2 = 3(2x+2)+3x+2 = 4x+3.$$

Решение (продолжение -1)

2. *Далее найдём обратный к $4x+3$ элемент решая уравнение*

$$(x^2+3x+3)\cdot a(x) + (4x+3)\cdot b(x) = 1.$$

с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^2+3x+3$, *// Инициализация*

$r_{-1}(x) = 4x+3$,

$y_{-2}(x) = 0$,

$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,

// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком

$q_0(x) = 4x+4$,

$r_0(x) = 1$,

$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) =$

$= -4x-4 = x+1$.

Т.е. $(4x+3)^{-1} = b(x) = y_0(x) = x+1$.

Решение (продолжение -2; $x^2 \equiv_5 2x+2$)

3. Наконец, вычислим обратную матрицу

$$M^{-1} = (x+1)\begin{pmatrix} 3x+2 & 4x+3 \\ 4x+2 & 3x+4 \end{pmatrix} = \begin{pmatrix} x+3 & 1 \\ 4x & 3x \end{pmatrix}.$$

Решение (продолжение -2; $x^2 \equiv_5 2x+2$)

3. Наконец, вычислим обратную матрицу

$$M^{-1} = (x+1)\begin{pmatrix} 3x+2 & 4x+3 \\ 4x+2 & 3x+4 \end{pmatrix} = \begin{pmatrix} x+3 & 1 \\ 4x & 3x \end{pmatrix}.$$

<u>Проверка</u> (арифметические ошибки возможны):

$$\begin{pmatrix} 3x+4 & x+2 \\ x+3 & 3x+2 \end{pmatrix} \times \begin{pmatrix} x+3 & 1 \\ 4x & 3x \end{pmatrix} =$$

$$= \begin{pmatrix} (3x+4)(x+3)+4x(x+2) & 3x+4+3x(x+2) \\ (x+3)^2+4x(3x+2) & x+3+3x(3x+2) \end{pmatrix} =$$

$$= \begin{pmatrix} 2x^2+x+2 & 3x^2+4x+4 \\ 3x^2+4x+4 & 4x^2+2x+3 \end{pmatrix} =$$

$$= \begin{pmatrix} 2(2x+2)+x+2 & 3(2x+2)+4x+4 \\ 3(2x+2)+4x+4 & 4(2x+2)+2x+3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Задача (ПГ-22)

Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Задача (ПГ-22)

Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Решение

1. *Сначала пытаемся найти корни* $f(x)$ *в* $\mathbb{F}_2$*:*

$$f(0) = 1, \qquad f(1) = 1.$$

Значит, $f(x)$ *не имеет корней в* $\mathbb{F}_2$ *т.е. не имеет линейных множителей.*

Задача (ПГ-22)

Разложить на неприводимые множители многочлен

$$f(x) = x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Решение

1. Сначала пытаемся найти корни $f(x)$ в $\mathbb{F}_2$:

$$f(0) = 1, \qquad f(1) = 1.$$

Значит, $f(x)$ не имеет корней в $\mathbb{F}_2$ т.е. не имеет линейных множителей.

2. Далее ищем делители $f(x)$ среди неприводимых многочленов степени 2.
Таковых над $\mathbb{F}_2$ только один — $x^2 + x + 1$.
При делении $f(x)$ на $x^2 + x + 1$, получаем

$$f(x) = (x^2 + x + 1) \cdot (x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1).$$

Решение (продолжение -1)

Продолжаем дальше делить на $x^2 + x + 1$:

$$\begin{aligned} g(x) &= x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + 1 = \\ &= (x^2 + x + 1)(x^7 + x^4 + x^3 + x^2 + x + 1) + x, \end{aligned}$$

т.е. $x^2 + x + 1$ *— делитель* $f(x)$ *кратности 1.*

Решение (продолжение -1)

Продолжаем дальше делить на x^2+x+1:

$$g(x) = x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = \\ = (x^2+x+1)(x^7+x^4+x^3+x^2+x+1)+x,$$

т.е. x^2+x+1 *— делитель* $f(x)$ *кратности 1.*

3. *Неприводимых многочленов степени 3 над* $\mathbb{F}_2$ *два:* x^3+x+1 *и* x^3+x^2+1. *Пробуем поделить* $g(x)$ *на* x^3+x+1:

$$x^9+x^8+x^7+x^6+x^4+x^3+x^2+x+1 = \\ = (x^3+x+1)(x^6+x^5+x^3+x^2+1).$$

Решение (продолжение -2)

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ *на многочлены 3-й степени, получаем*

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

Решение (продолжение -2)

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ *на многочлены 3-й степени, получаем*

$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x + 1)(x^3 + x^2 + x + 1) + x^2,$$
$$x^6 + x^5 + x^3 + x^2 + 1 = (x^3 + x^2 + 1)x^3 + x^2 + 1.$$

Т.к. как многочлен 6-ой степени $h(x)$ *не имеет делителей 3-й и меньших степеней, то он является неприводимым: если бы он имел делитель, скажем, степени 4, то у него был бы и делитель степени* $6 - 4 = 2$*.*

Решение (продолжение -2)

Производя далее попытки деления $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ *на многочлены 3-й степени, получаем*

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

Т.к. как многочлен 6-ой степени $h(x)$ *не имеет делителей 3-й и меньших степеней, то он является неприводимым: если бы он имел делитель, скажем, степени 4, то у него был бы и делитель степени* $6 - 4 = 2$.

В итоге в $\mathbb{F}_2[x]$ *имеем разложение*

$$\begin{aligned} f(x) &= x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 = \\ &= (x^2 + x + 1)(x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1). \end{aligned}$$

Задача (ПГ-23)

Найти минимальное поле характеристики 3, в котором многочлен $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ раскладывается на линейные множители.
В данном поле найти все корни данного многочлена.

Задача (ПГ-23)

Найти минимальное поле характеристики 3, в котором многочлен $f(x) = x^3 + x + 2 \in \mathbb{F}_3[x]$ *раскладывается на линейные множители.*
В данном поле найти все корни данного многочлена.

Решение

1. Найдём разложение многочлена $f(x)$ *на неприводимые множители над* $\mathbb{F}_3$*.*

- *Проверяем корни:* $f(0) = 2$, $f(1) = 1$, $f(2) = \mathbf{0}$.
  Т.к. $x - 2 \equiv_3 x + 1$, *то* $f(x) = (x+1)(x^2+2x+2)$.
- *Найдём разложение многочлена* $g(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$.
  Он не имеет корней, его степень $= 2 \Rightarrow$ *он неприводим.*
- *Окончательно:* $f(x) = (x+1)(x^2+2x+2)$.

Решение (продолжение -1)

2. *Известно, что если* $g(x)$ *— неприводимый многочлен степени* n *над конечным полем* $\mathbb{F}_p$*, то он:*

Решение (продолжение -1)

2. *Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем $\mathbb{F}_p$, то он:*

- *в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —*
$$g(x) = (x-\alpha)\cdot(x-\alpha^p)\cdot(x-\alpha^{p^2})\cdot\ldots\cdot(x-\alpha^{p^{n-1}}),$$
где α – произвольный корень $g(x)$ в F;
- *не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.*

Решение (продолжение -1)

2. Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем $\mathbb{F}_p$, то он:

- *в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —*
  $$g(x) = (x-\alpha)\cdot(x-\alpha^p)\cdot(x-\alpha^{p^2})\cdot\ldots\cdot(x-\alpha^{p^{n-1}}),$$
  где α – произвольный корень $g(x)$ в F;
- *не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.*

3. Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$.

Решение (продолжение -1)

2. *Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем $\mathbb{F}_p$, то он:*

- *в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —*
$$g(x) = (x-\alpha)\cdot(x-\alpha^p)\cdot(x-\alpha^{p^2})\cdot\ldots\cdot(x-\alpha^{p^{n-1}}),$$
где α – произвольный корень $g(x)$ в F;
- *не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.*

3. *Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2 + 2x + 2$. В этом поле если α — корень $g(x)$, то*

- $\alpha^2 = -2\alpha - 2 = \alpha + 1;$

Решение (продолжение -1)

2. *Известно, что если $g(x)$ — неприводимый многочлен степени n над конечным полем $\mathbb{F}_p$, то он:*

- *в поле своего расширения $F = \mathbb{F}_p[x]/(g(x))$ раскладывается на n линейных множителей —*
  $$g(x) = (x-\alpha)\cdot(x-\alpha^p)\cdot(x-\alpha^{p^2})\cdot\ldots\cdot(x-\alpha^{p^{n-1}}),$$
  где α – произвольный корень $g(x)$ в F;
- *не имеет корней ни в каком конечном поле, содержащим менее, чем p^n элементов.*

3. *Рассмотрим поле $\mathbb{F}_3[x]/(g(x))$ расширения многочлена $g(x) = x^2+2x+2$. В этом поле если α — корень $g(x)$, то*

- $\alpha^2 = -2\alpha-2 = \alpha+1;$
- $\alpha^3 = \alpha(\alpha+1) = \alpha^2+\alpha = 2\alpha+1$ *— тоже корень $g(x)$*

Решение (продолжение -2; $\alpha^2 = \alpha + 1$)

Действительно (подчёркиваем слагаемые, дающие в сумме 0):

$$(x-\alpha)(x-2\alpha-1) = (x+2\alpha)\cdot(x+\alpha+2) =$$
$$= x^2 + \underline{\alpha x} + 2x + \underline{2\alpha x} + 2\alpha^2 + 4\alpha =$$
$$= x^2 + 2x + \underline{2\alpha} + 2 + \underline{4\alpha} = x^2 + 2x + 2.$$

Решение (продолжение -2; $\alpha^2 = \alpha + 1$)

Действительно (подчёркиваем слагаемые, дающие в сумме 0):

$$
\begin{aligned}
(x-\alpha)(x-2\alpha-1) &= (x+2\alpha)\cdot(x+\alpha+2) = \\
&= x^2 + \underline{\alpha x} + 2x + \underline{2\alpha x} + 2\alpha^2 + 4\alpha = \\
&= x^2 + 2x + \underline{2\alpha} + 2 + \underline{4\alpha} = x^2 + 2x + 2.
\end{aligned}
$$

Построенное расширение — поле $\mathbb{F}_3[x]/(x^2+2x+2)$ *— содержит найденный ранее корень* 2, *поэтому многочлен* $f(x)$ *в этом поле раскладывается на следующие линейные множители:*

$$
f(x) = x^3 + x + 2 = (x-2)(x-\alpha)(x-2\alpha-1) = (x+1)(x+2\alpha)(x+\alpha+2).
$$

Решение (продолжение -3)

4. *Определить корни многочлена* $g(x) = (x - \alpha)(x - 2\alpha - 1)$ *в поле* $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ *легко:*

Решение (продолжение -3)

4. Определить корни многочлена $g(x) = (x-\alpha)(x-2\alpha-1)$ *в поле* $\mathbb{F}_3[x]/(x^2+2x+2)$ *легко:*
всегда можно взять $\alpha = x$,
откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

Решение (продолжение -3)

4. *Определить корни многочлена* $g(x) = (x - \alpha)(x - 2\alpha - 1)$ *в поле* $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ *легко:*
всегда можно взять $\alpha = x$,
откуда второй корень $\alpha^3 = 2\alpha + 1 = 2x + 1$.

5. *Таким образом, в поле* $\mathbb{F}_3[x]/(x^2 + 2x + 2)$ *многочлен* $f(x) = x^3 + x + 2$ *имеет корни*

$$2, \; x \; \text{ и } \; 2x + 1.$$

Нахождение корней многочлена из $\mathbb{F}_p[x]$

Алгоритм нахождения всех корней многочлена $f(x)$ над полем Галуа $\mathbb{F}_p$

1. Разложить $f(x)$ на неприводимые множители над $\mathbb{F}_p$:
$$f(x) = g_1(x) \cdot g_2(x) \cdot \ldots \cdot g_k(x).$$
2. Для каждого многочлена $g_i(x)$, $i = \overline{1, k}$ рассмотреть расширение $\mathbb{F}_p[x]/(g_i(x))$, в котором он будет иметь корни $x = \alpha,\ \alpha^p,\ \ldots,\ \alpha^{p^{\deg g_i - 1}}$.
Записать данные корни как многочлены из $\mathbb{F}_p[x]/(g_i(x))$.
3. Объединить все корни в одном общем расширении $\mathbb{F}_p^m$, где $m = \text{НОК}\,(\deg g_1,\ \deg g_2,\ \ldots,\ \deg g_k)$.

Задача (ПГ-24)

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, *который имеет корень* α^3, *где* α — *примитивный элемент поля*

$$\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2 + x + 2).$$

Задача (ПГ-24)

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, который имеет корень α^3, где α — примитивный элемент поля

$$\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2 + x + 2).$$

Решение

1. Известно, что минимальный многочлен $m(x)$ в поле характеристики 5 вместе с корнем α^3 содержит все смежные с ним $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т.д.

Задача (ПГ-24)

Найти минимальный многочлен $m(x) \in \mathbb{F}_5[x]$, который имеет корень α^3, где α — примитивный элемент поля

$$\mathbb{F}_5^2 = \mathbb{F}_5[x]/(x^2 + x + 2).$$

Решение

1. Известно, что минимальный многочлен $m(x)$ в поле характеристики 5 вместе с корнем α^3 содержит все смежные с ним $(\alpha^3)^5 = \alpha^{15}$, $(\alpha^3)^{5^2} = \alpha^{75}$, $(\alpha^3)^{5^3} = \alpha^{375}$ и т.д.

2. В поле $\mathbb{F}_5^2$ будем иметь $\alpha^{5^2-1} = \alpha^{24} = 1$. Поэтому здесь смежный класс, образованный α^3, содержит только два элемента α^3 и α^{15} $\Rightarrow$ минимальный многочлен имеет степень 2 и может быть представлен как

$$m(x) = (x - \alpha^3)(x - \alpha^{15}) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}.$$

Решение (продолжение; $m(x) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}$)

3. Найдём коэффициенты многочлена $m(x)$ учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha + 3) = 4\alpha^2 + 3\alpha = \\
&= 4(4\alpha + 3) + 3\alpha = 4\alpha + 2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha + 2)^5 = 4\alpha^5 + 2 = \\
&= 4\alpha^2\alpha^3 + 2 = 4(4\alpha + 3)(4\alpha + 2) + 2 = \\
&= 4(\alpha^2 + 1) + 2 = 4(4\alpha + 4) + 2 = \alpha + 3, \\
\alpha^3 + \alpha^{15} &= 4\alpha + 2 + \alpha + 3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha + 2)(\alpha + 3) = \\
&= 4(4\alpha + 3) + 4\alpha + 1 = 3.
\end{aligned}$$

Решение (продолжение; $m(x) = x^2 - (\alpha^3 + \alpha^{15})x + \alpha^{18}$)

3. Найдём коэффициенты многочлена $m(x)$ учётом $\alpha^2 = -\alpha - 2 = 4\alpha + 3$:

$$\begin{aligned}
\alpha^3 &= \alpha \cdot \alpha^2 = \alpha(4\alpha+3) = 4\alpha^2 + 3\alpha = \\
&\qquad = 4(4\alpha+3) + 3\alpha = 4\alpha + 2, \\
\alpha^{15} &= (\alpha^3)^5 = (4\alpha+2)^5 = 4\alpha^5 + 2 = \\
&\qquad = 4\alpha^2\alpha^3 + 2 = 4(4\alpha+3)(4\alpha+2) + 2 = \\
&\qquad = 4(\alpha^2+1) + 2 = 4(4\alpha+4) + 2 = \alpha + 3, \\
\alpha^3 + \alpha^{15} &= 4\alpha + 2 + \alpha + 3 = 0, \\
\alpha^{18} &= \alpha^3\alpha^{15} = (4\alpha+2)(\alpha+3) = \\
&\qquad = 4(4\alpha+3) + 4\alpha + 1 = 3.
\end{aligned}$$

В итоге:

$$m(x) = x^2 + 3.$$

Раздел I

Раздел II

Раздел III

- Конечное поле и его характеристика. Мультипликативная группа, примитивный элемент поля Галуа и его нахождение. Основная теорема алгебры.
- Алгоритм Евклида и его применение.
  Теорема Безу и расширенный алгоритм Евклида.
- Неприводимые многочлены: существование и нахождение неприводимых многочленов в конечных полях. Построение конечных полей с помощью неприводимых многочленов (привести пример). Изоморфизм конечных полей.
- Векторное пространство многочленов. Базис в $\mathbb{F}_p^n$. Поля Галуа как векторные пространства. Подполя конечного поля.

- Минимальные многочлены над конечным полем: примеры и свойства. Корнями какого многочлена являются все элементы конечного поля? Делителями какого многочлена являются все неприводимые многочлены n-й степени?
- Теорема о степени любого неприводимого делителя многочлена $x^{p^n-1} - 1$.
- Теорема о корнях неприводимого многочлена. Многочлены над конечным полем: решение уравнений.
- Как решать уравнения, когда корней нет (алгоритм нахождения всех корней многочлена $f(x)$ над полем Галуа $\mathbb{F}_p$)?
- Мультипликативная группа расширения поля. Существование неприводимого многочлена степени n над полем $\mathbb{F}_p$.
- Лемма о числе неприводимых нормированных многочленов из $\mathbb{F}_p^n$. Среднее число неприводимых многочленов.

- Изоморфизм полей Галуа с одинаковым числом элементов.
- Теорема о неприводимом нормированном многочлене — делителе порождающего элемента идеала.
- Циклическое пространство: определение и примеры. Количество и степени неприводимых делителей $x^n - 1$.

Раздел I

Раздел II

Раздел III

Две задачи

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

Две задачи

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

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 (может зависеть от некоторого параметра m),
- r — максимально допустимое число ошибок;

Требуется построить код, максимизирующий число t сообщений, которое можно передать.

Решаем вспомогательную задачу —

— она проще.

Решаем вспомогательную задачу —

— она проще.

Мы увидим, что точное решение вспомогательной задачи найдено лишь для случаев $n = 2^m - 1$, $r = 1$ и $n = 23$, $r = 3$.
Для остальных пар (n, r) будет дано приближённое решение.

Решаем вспомогательную задачу —

— она проще.

Мы увидим, что точное решение вспомогательной задачи найдено лишь для случаев $n = 2^m - 1,\ r = 1$ и $n = 23,\ r = 3$.
Для остальных пар $(n,\ r)$ будет дано приближённое решение.

Основные понятия:

- Норма $\|\widetilde{\gamma}\| =$ число единичных координат в $\widetilde{\gamma} \in B^n$.
- Метрика (вспоминаем, что это такое) на множестве бинарных наборов — *хеммингово 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

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

Утверждение

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

Групповые коды

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

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: $-\widetilde{\alpha} = \widetilde{\alpha}$ *— см. выше.*

Минимальное расстояние между кодовыми словами

Теорема

Минимальное расстояние между кодовыми словами обладает свойством

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

Минимальное расстояние между кодовыми словами

Теорема

Минимальное расстояние между кодовыми словами обладает свойством

$$\min_{\widetilde{\alpha}\neq\widetilde{\beta}} \rho(\widetilde{\alpha},\widetilde{\beta}) \;=\; \min_{\widetilde{\gamma}\neq\widetilde{0}} \parallel \widetilde{\gamma} \parallel .$$

Доказательство

$\rho(\widetilde{\alpha},\widetilde{\beta}) \;= \parallel \widetilde{\alpha} \oplus \widetilde{\beta} \parallel = \parallel \widetilde{\gamma} \parallel$, *причем* $\widetilde{\gamma} \neq \widetilde{0}$ *при* $\widetilde{\alpha} \neq \widetilde{\beta}$.
Отсюда получаем оценку

$$\min_{\widetilde{\alpha}\neq\widetilde{\beta}} \rho(\widetilde{\alpha},\widetilde{\beta}) \;\geqslant\; \min_{\widetilde{\gamma}\neq\widetilde{0}} \parallel \widetilde{\gamma} \parallel .$$

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 менее 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 менее 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, то искомое кодовое слово α — ближайшее к полученному набору.

Плотная упаковка шаров в булев куб

Следствие

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

Чтобы построить код максимального размера, исправляющий r ошибок, нужно вложить в единичный куб B^n максимально возможное число непересекающихся шаров радиуса r — *задача плотной упаковки*.

Плотная упаковка шаров в булев куб

Следствие

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

Чтобы построить код максимального размера, исправляющий r ошибок, нужно вложить в единичный куб B^n максимально возможное число непересекающихся шаров радиуса r — *задача плотной упаковки*.

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

Плотная упаковка шаров в булев куб

Следствие

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

Чтобы построить код максимального размера, исправляющий r ошибок, нужно вложить в единичный куб B^n максимально возможное число непересекающихся шаров радиуса r — *задача плотной упаковки*.

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

Ответ: Такое удаётся в случаях:

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

Количество кодовых слов

Теорема (Хэмминга)

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

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

Количество кодовых слов

Теорема (Хэмминга)

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

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

Доказательство

t *есть максимальное число непересекающихся шаров радиуса* r*, помещающихся в кубе* B^n*.*

Верхняя оценка — шар радиуса r *содержит точки: сам центр + все точки с одной, двумя, ..., r измененными координатами, т.е. всего* $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{r}$ *штук и шары не пересекаются.*

Продолжение доказательства

Для оценки снизу построим негрупповой код:

1. *берем произвольную точку B^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. В результате:*

- *шары, возможно, пересекаются, но каждый шар занимает $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}$ точек $\Rightarrow$ шаров не менее*

$$\frac{2^n}{\dbinom{n}{0} + \dbinom{n}{1} + \ldots + \dbinom{n}{2r}};$$

- *шары радиуса r с центрами в выбранных точках не пересекаются.*

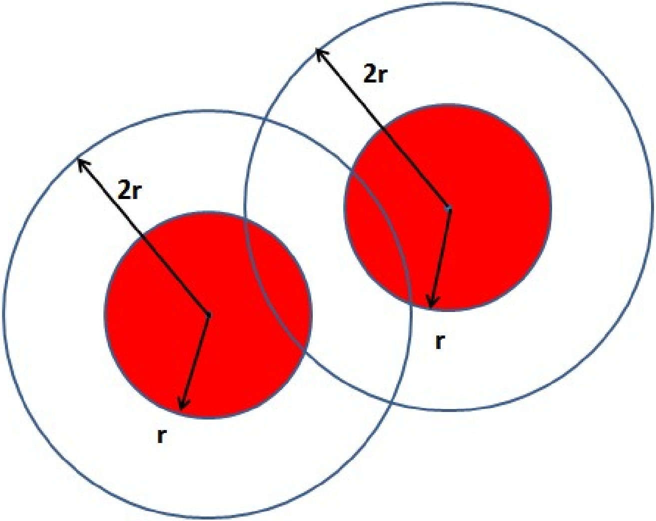


Рис. 1. К теореме Хэмминга

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

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

Построим код, а потом определим его кодовое расстояние.

Рассмотрим таблицу:

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

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

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–кодовых слов. Но

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

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

Просуммируем всевозможные совокупности строк этой таблицы, получив всего $2^{2^m-(m+1)}$ наборов–кодовых слов. Но

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

Найдём кодовое расстояние.
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 $\rho(\widetilde{\alpha}, \widetilde{\beta}) \geqslant \mathbf{3}$ $\Rightarrow$ шары радиуса 1 с центрами в полученных наборах не пересекаются.

Хэмминга длины $n = 2^3 - 1 = 7$, $r = 1$

Пример

Составим таблицу для кода Хэмминга длины 7 ($m = 3$):

$$\begin{array}{|cccc|ccc|}
\hline
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\hline
\end{array}$$

Складывая по $\mathrm{mod}\ 2$ произвольные совокупности строк, получаем 16 различных бинарных наборов, которыми 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 23-мерный единичный куб

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

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

Случай $n = 23,\ r = 3$

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

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

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

Других пар $(n,\ r)$, удовлетворяющих условию

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

неизвестно (а если таковые и есть, то у них $n \gg 1$ и такой код не представляет практического интереса).

Раздел I

Раздел II

Раздел III

Циклические коды: определение

Определение

Код C называется *циклическим*, если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leqslant s \leqslant n-1$ справедливо

$$(\alpha_0, \ldots, \alpha_{n-1}) \in C \Rightarrow (\alpha_s, \alpha_{s+1}, \ldots, \alpha_{n-1}, \alpha_0, \ldots, \alpha_{s-1}) \in C.$$

Циклические коды: определение

Определение

Код C называется *циклическим*, если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leqslant s \leqslant n-1$ справедливо

$$(\alpha_0, \ldots, \alpha_{n-1}) \in C \Rightarrow (\alpha_s, \alpha_{s+1}, \ldots, \alpha_{n-1}, \alpha_0, \ldots, \alpha_{s-1}) \in C.$$

Ранее рассматривалось и было показано:

- В кольце $\mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как линейное векторное пространство над полем $\mathbb{F}_p$ имеется базис $\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$.
  Циклический сдвиг координат в этом базисе равносилен умножению на x.

Циклические коды: определение

Определение

Код C называется *циклическим*, если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leqslant s \leqslant n-1$ справедливо

$$(\alpha_0, \ldots, \alpha_{n-1}) \in C \Rightarrow (\alpha_s, \alpha_{s+1}, \ldots, \alpha_{n-1}, \alpha_0, \ldots, \alpha_{s-1}) \in C.$$

Ранее рассматривалось и было показано:

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

Циклические коды: построение

Поэтому построить циклический код можно так:

1. выбираем некоторый делитель $\varphi(x)$ многочлена $x^n - 1$;
2. в кольце $\mathbb{F}_2[x]/(x^n - 1)$ образуем идеал $(\varphi(x))$.

$\varphi(x)$ — *образующий многочлен*.

Циклические коды: построение

Поэтому построить циклический код можно так:

1. выбираем некоторый делитель $\varphi(x)$ многочлена $x^n - 1$;
2. в кольце $\mathbb{F}_2[x]/(x^n - 1)$ образуем идеал $(\varphi(x))$.

$\varphi(x)$ — *образующий многочлен*.

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.

Для декодирования циклического кода нужно —

— принятую кодовую комбинацию поделить на φ.
Если остаток от деления $R(x) \equiv 0$, то ошибок нет (или их больше 1).
Иначе ненулевые коэффициенты остатка от деления $R(x)$ (*вектора ошибок*) определяют, в каком разряде произошла ошибка.

Для декодирования циклического кода нужно —

— принятую кодовую комбинацию поделить на φ.
Если остаток от деления $R(x) \equiv 0$, то ошибок нет (или их больше 1).
Иначе ненулевые коэффициенты остатка от деления $R(x)$ (*вектора ошибок*) определяют, в каком разряде произошла ошибка.

(исправление одной ошибки)

1) Пусть принято слово $(1111000) \leftrightarrow 1 + x + x^2 + x^3 = \psi(x)$.
Делим $\psi(x)$ на $\varphi(x)$:

$$\psi(x) = x^3 + x^2 + x + 1 = 1 \cdot \overbrace{(x^3 + x + 1)}^{\varphi(x)} + x^2,$$

т.е. $R(x) = x^2 \leftrightarrow (0010000)$.
Единственный ненулевой коэффициент показывает позицию ошибки: 2-й разряд.

Для декодирования циклического кода нужно —

— принятую кодовую комбинацию поделить на φ.
Если остаток от деления $R(x) \equiv 0$, то ошибок нет (или их больше 1).
Иначе ненулевые коэффициенты остатка от деления $R(x)$ (*вектора ошибок*) определяют, в каком разряде произошла ошибка.

(исправление одной ошибки)

1) Пусть принято слово $(1111000) \leftrightarrow 1 + x + x^2 + x^3 = \psi(x)$.
Делим $\psi(x)$ на $\varphi(x)$:

$$\psi(x) = x^3 + x^2 + x + 1 = 1 \cdot \overbrace{(x^3 + x + 1)}^{\varphi(x)} + x^2,$$

т.е. $R(x) = x^2 \leftrightarrow (0010000)$.
Единственный ненулевой коэффициент показывает позицию ошибки: 2-й разряд.

(исправление одной ошибки, продолжение)

2) Пусть принято слово $(0001100) \leftrightarrow x^4 + x^3 = \psi(x)$.
Делим $\psi(x)$ на $\varphi(x)$:

$$\psi(x) = x^4 + x^3 = (x+1)\cdot(x^3 + x + 1) + (x^2 + 1),$$

т.е. $R(x) = x^2 + 1 \leftrightarrow (1010000)$ — более одного ненулевого коэффициента.

Алгоритмы декодирования, основанные на применении *проверочной матрицы* (о них — позже) позволяют определить, что ошибка произошла во 6-м разряде.

(исправление одной ошибки, продолжение)

2) Пусть принято слово $(0001100) \leftrightarrow x^4 + x^3 = \psi(x)$.
Делим $\psi(x)$ на $\varphi(x)$:

$$\psi(x) = x^4 + x^3 = (x+1) \cdot (x^3 + x + 1) + (x^2 + 1),$$

т.е. $R(x) = x^2 + 1 \leftrightarrow (1010000)$ — более одного ненулевого коэффициента.

Алгоритмы декодирования, основанные на применении *проверочной матрицы* (о них — позже) позволяют определить, что ошибка произошла во 6-м разряде.

Операции декодирования циклических кодов (умножения и деления многочленов) просто реализуются на регистрах сдвига с обратными связями. Эта техническая простота и послужила причиной их широкого распространения.

Раздел I

Раздел II

Раздел III

Коды БЧХ — 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.

Они 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 приёмно-передающей аппаратуры).

Коды Хэмминга — частный случай БЧХ-кодов.

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

— конкретизирующей выбор идеала:

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

— конкретизирующей выбор идеала:

1. Строим поле $\mathbb{F}_2^n \cong \mathbb{F}_2[x]/(f)$, f — неприводимый многочлен степени $n = 2^m - 1$.
2. Выберем в циклической группе $\mathbb{F}_2^{n*}$ 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.
3. 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).

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

— конкретизирующей выбор идеала:

1. Строим поле $\mathbb{F}_2^n \cong \mathbb{F}_2[x]/(f)$, f — неприводимый многочлен степени $n = 2^m - 1$.
2. Выберем в циклической группе $\mathbb{F}_2^{n*}$ 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.
3. 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 ($m = 4$, 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 специально выбранных 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 $\{\alpha^t, \alpha^{2t}, \ldots, \alpha^{2^s t}\}$, то $2^s \leqslant n = 2^m - 1$, т.е. степень каждого делителя не более $m = \log_2(n+1)$.
- $\deg\varphi \leqslant rm = r\log_2(n+1)$.
- 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 специально выбранных 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 $\{\,\alpha^t, \alpha^{2t}, \ldots, \alpha^{2^s t}\,\}$, то $2^s \leqslant n = 2^m - 1$, т.е. степень каждого делителя не более $m = \log_2(n+1)$.
- $\deg\varphi \leqslant rm = r\log_2(n+1)$.
- 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 код — в идеал (φ) — кратны φ $\Rightarrow$ каждый кодовый многочлен имеет корни $\alpha, \alpha^2, \dots, \alpha^{2r}$ (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, $s = 1, \dots, 2r$, 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 $\alpha^{j_1+j_2+\ldots+j_{2r}}$ 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 характеризуется вектором ошибок (1 — символ ошибочен, 0 — нет) таких, что первый и последний из них отличны от нуля.

Раздел I

Раздел II

Раздел III

- Линеаризация
- Что надо знать

5. Алгебраические решётки
   - Решётки: определение, основные свойства
   - Модулярные и дистрибутивные решётки
   - Применение теории решёток к задаче классификации
   - Что надо знать

Задача (ТК-1)

Линейный код задан своей проверочной матрицей

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Требуется построить порождающую матрицу кода G для систематического кодирования, при котором биты исходного сообщения переходят в последние биты кодового слова.
Найти систематическое кодирование для векторов

$$\vec{u}_1 = [1\ 1\ 0]^T, \vec{u}_2 = [1\ 0\ 1]^T.$$

Задача (ТК-1)

Линейный код задан своей проверочной матрицей

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Требуется построить порождающую матрицу кода G для систематического кодирования, при котором биты исходного сообщения переходят в последние биты кодового слова.
Найти систематическое кодирование для векторов

$$\vec{u}_1 = [1\ 1\ 0]^T, \vec{u}_2 = [1\ 0\ 1]^T.$$

Решение

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_3 \end{bmatrix}$, где I_3 – единичная матрица порядка размера 3.

Решение

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_3 \end{bmatrix}$, где I_3 – единичная матрица порядка размера 3.

Такую матрицу можно получить, если привести проверочную матрицу H к виду $\begin{bmatrix} I_3 & P \end{bmatrix}$, т.е. с помощью эквивалентных преобразований строк выделить в первых трех колонках единичную матрицу:

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{1 \leftrightarrow 3} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1 \leftarrow 1+2}$$

$$\to \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1 \leftarrow 1+3} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Решение (продолжение)

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\vec{u}_1 = [1\ 1\ 0]^T$, $\vec{u}_2 = [1\ 0\ 1]^T$:

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

Решение (продолжение)

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\vec{u}_1 = [1\ 1\ 0]^T$, $\vec{u}_2 = [1\ 0\ 1]^T$:

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad [\vec{v}_1, \vec{v}_2] = G[\vec{u}_1, \vec{u}_2] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Задача (ТК-2)

Циклический $(9,3)$-код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить минимальное расстояние кода d, а также осуществить систематическое кодирование полинома

$$u(x) = x^2 + x.$$

Задача (ТК-2)

Циклический $(9,3)$-код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить минимальное расстояние кода d, а также осуществить систематическое кодирование полинома

$$u(x) = x^2 + x.$$

Решение

Для определения минимального кодового расстояния d найдём все кодовые полиномы:

$$v(x) = g(x)(ax^2 + bx + c) = (x^6 + x^3 + 1)(ax^2 + bx + c) =$$
$$= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c, \ a, b, c \in \mathbb{F}_2.$$

Решение (продолжение...)

В векторном виде все кодовые слова представляются как $[a, b, c, a, b, c, a, b, c]$.

Следовательно, минимальный хэммингов вес ненулевого кодового слова равен 3, *т.е.* $d = 3$.

Решение (продолжение...)

В векторном виде все кодовые слова представляются как $[a, b, c, a, b, c, a, b, c]$.
Следовательно, минимальный хэммингов вес ненулевого кодового слова равен 3, *т.е.* $d = 3$.
Систематическое кодирование полинома $u(x)$ *вычисляем непосредственно*

$$v(x) = x^6 u(x) + \mathrm{mod}(x^6 u(x),\ g(x)) =$$
$$= x^8 + x^7 + \mathrm{mod}(x^8 + x^7, x^6 + x^3 + 1) = x^8 + x^7 + x^5 + x^4 + x^2 + x.$$

Задача (ТК-3)

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/(x^3 + x + 1)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Задача (ТК-3)

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/(x^3 + x + 1)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Решение

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$*:*

$$s = w(\alpha) = \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 =$$

$$= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 =$$

$$= \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

Задача (TK-3)

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/(x^3+x+1)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Решение

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$*:*

$$s = w(\alpha) = \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 =$$
$$= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 =$$
$$= \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

Далее необходимо найти полином ошибок вида $e(x) = x^k$ *такой, что* $e(\alpha) = s$, *т.е. найти такое* k, *что* $\alpha^k = 1$.

Задача (TK-3)

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/(x^3+x+1)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Решение

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$*:*

$$s = w(\alpha) = \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 =$$
$$= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 =$$
$$= \alpha^3 + \alpha = \alpha + 1 + \alpha = 1.$$

Далее необходимо найти полином ошибок вида $e(x) = x^k$ *такой, что* $e(\alpha) = s$*, т.е. найти такое* k*, что* $\alpha^k = 1$*.*
Очевидно, что $k = 0 \Rightarrow \hat{v}(x) = w(x) + e(x) = x^7 + x^6 + x^2$.

Задача (ТК-4)

Рассмотрим код БЧХ с нулями α^i, $i = 1, \ldots, 4$, *где* α *— примитивный элемент поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$.
Требуется найти полином локаторов ошибок $\sigma(x)$ *для принятого полинома*

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

Задача (ТК-4)

Рассмотрим код БЧХ с нулями α^i, $i = 1, \ldots, 4$, *где* α *— примитивный элемент поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$.
Требуется найти полином локаторов ошибок $\sigma(x)$ *для принятого полинома*

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

Решение

Для удобства вычислений в поле $\mathbb{F}_2^4$ *построим таблицу соответствий между степенным и полиномиальным представлением элементов поля.*

Решение (продолжение -1; $\alpha^4 = \alpha + 1$)

α	α
α^2	α^2
α^3	α^3
α^4	$\alpha + 1$
α^5	$\alpha^2 + \alpha$
α^6	$\alpha^3 + \alpha^2$
α^7	$\alpha^3 + \alpha + 1$
α^8	$\alpha^2 + 1$
α^9	$\alpha^3 + \alpha$
α^{10}	$\alpha^2 + \alpha + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$
α^{14}	$\alpha^3 + 1$
α^{15}	1

Решение (продолжение -2)

С помощью этой таблицы вычислим синдромы:

$$
\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.
\end{aligned}
$$

Решение (продолжение -2)

С помощью этой таблицы вычислим синдромы:

$$\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7,\\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14},\\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0,\\
s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.
\end{aligned}$$

Синдромный полином — $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$*.*
Синдромов всего четыре, следовательно, $t = 2$*.*

Решение (продолжение -2)

С помощью этой таблицы вычислим синдромы:

$$
\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.
\end{aligned}
$$

Синдромный полином — $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$. *Синдромов всего четыре, следовательно,* $t = 2$. *Полином локаторов ошибок* $\sigma(x)$ *является решением уравнения*

$$x^{2t+1}a(x) + s(x)\sigma(x) = \lambda(x), \ \deg \lambda(x) \leqslant t.$$

Решение (продолжение -3; $x^{2t+1}a(x) + s(x)\sigma(x) = \lambda(x),\ \deg\lambda(x) \leqslant t$)

Решаем с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^5$, *// Инициализация*

$r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$,

$y_{-2}(x) = 0$,

$y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,

// Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком

$q_0(x) = \alpha^2 x$,

$r_0(x) = \alpha x^3 + \alpha^9 x^2 + \alpha^2 x$,

$y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = \alpha^2 x$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,

// Делим $r_{-1}(x)$ на $r_0(x)$ с остатком

$q_1(x) = \alpha^{12}x + \alpha^5$,

$r_1(x) = \alpha^{14}x^2 + 1$,

$y_1(x) = y_{-1}(x) - y_0(x)q_1(x) =$

$= 1 + \alpha^2 x(\alpha^{12}x + \alpha^5) = \alpha^{14}x^2 + \alpha^7 x + 1$.

Решение (продолжение -4)

Таким образом, искомый полином локаторов ошибок

$$\sigma(x) = \alpha^{14}x^2 + \alpha^7 x + 1.$$

Задача (ТК-5)

Рассмотрим код БЧХ, нули которого определяются степенями α,
где α *– примитивный элемент поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$.
Пусть для некоторого принятого слова $w(x)$ *полином локаторов ошибок* $\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$.
Требуется определить позиции ошибок в $w(x)$.

Задача (ТК-5)

Рассмотрим код БЧХ, нули которого определяются степенями α,
где α *– примитивный элемент поля* $\mathbb{F}_2[x]/(x^4 + x + 1)$.
Пусть для некоторого принятого слова $w(x)$ *полином локаторов ошибок* $\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$.
Требуется определить позиции ошибок в $w(x)$.

Решение

Найдём корни полинома локаторов ошибок полным перебором. Для вычислений будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной выше.

Решение (продолжение; $\alpha^4 = \alpha + 1$)

$$
\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3 + 1, \\
\sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3, \\
\sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha, \\
\sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1, \\
\sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = 0, \\
\sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1, \\
\sigma(\alpha^7) &= \alpha + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1, \\
\sigma(\alpha^8) &= \alpha^3 + \alpha^{14} + 1 = 0, \\
\sigma(\alpha^9) &= \alpha^5 + 1 + 1 = \alpha^2 + \alpha, \\
\sigma(\alpha^{10}) &= \alpha^7 + \alpha + 1 = \alpha^3,
\end{aligned}
$$

Решение (продолжение -1)

$$\sigma(\alpha^{11}) = \alpha^9+\alpha^2+1 = \alpha^3+\alpha^2+\alpha+1,$$
$$\sigma(\alpha^{12}) = \alpha^{11}+\alpha^3+1 = \alpha^2+\alpha+1,$$
$$\sigma(\alpha^{13}) = \alpha^{13}+\alpha^4+1 = \alpha^3+\alpha^2+\alpha+1,$$
$$\sigma(\alpha^{14}) = 1+\alpha^5+1 = \alpha^2+\alpha,$$
$$\sigma(\alpha^{15}) = \alpha^2+\alpha^6+1 = \alpha^3+1.$$

Решение (продолжение -1)

$$\sigma(\alpha^{11}) = \alpha^9 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{12}) = \alpha^{11} + \alpha^3 + 1 = \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{13}) = \alpha^{13} + \alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{14}) = 1 + \alpha^5 + 1 = \alpha^2 + \alpha,$$
$$\sigma(\alpha^{15}) = \alpha^2 + \alpha^6 + 1 = \alpha^3 + 1.$$

Заметим, что полином локаторов ошибок $\sigma(x)$ является полиномом над полем $\mathbb{F}_2^4$. Поэтому здесь не выполняется свойство $\sigma(\alpha^2) = (\sigma(\alpha))^2$.

Решение (продолжение -1)

$$\sigma(\alpha^{11}) = \alpha^9 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{12}) = \alpha^{11} + \alpha^3 + 1 = \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{13}) = \alpha^{13} + \alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{14}) = 1 + \alpha^5 + 1 = \alpha^2 + \alpha,$$
$$\sigma(\alpha^{15}) = \alpha^2 + \alpha^6 + 1 = \alpha^3 + 1.$$

Заметим, что полином локаторов ошибок $\sigma(x)$ является полиномом над полем $\mathbb{F}_2^4$. Поэтому здесь не выполняется свойство $\sigma(\alpha^2) = (\sigma(\alpha))^2$.
Обратные элементы для обнаруженных корней α^5 и α^8 равны, соответственно, α^{10} и α^7. Отсюда получаем, что полином ошибок

$$e(x) = x^{10} + x^7.$$

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать

2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

- Задачи построения кодов, исправляющих ошибки. Основные понятия метрики на единичном кубе.
  Групповые коды: определения, свойства. Кодовое расстояние.
  Построение кода как задача плотной упаковки.
- Теорема Хэмминга. Пример построения кода Хэмминга.
- Циклические коды: определение, построение и декодирование.
- Коды БЧХ как частный случай циклических кодов. Идея построения кода БЧХ и оценка его кодового расстояния.
- Коды БЧХ: алгоритмы кодирования и декодирования.

Раздел I

1 Конечные поля или поля Галуа

- Поля вычетов по модулю простого числа
- Вычисление элементов в конечных полях
- Линейная алгебра над конечным полем
- Корни многочленов над конечным полем
- Существование и единственность поля Галуа из p^n элементов
- Циклические подпространства
- Задачи
- Что надо знать

2 Коды, исправляющие ошибки

- Основная задача теории кодирования
- Циклические коды

Раздел II

Раздел III

- Линеаризация
- Что надо знать

5. Алгебраические решётки
   - Решётки: определение, основные свойства
   - Модулярные и дистрибутивные решётки
   - Применение теории решёток к задаче классификации
   - Что надо знать

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 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:

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

Определение (1)

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

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

Действие группы на множестве: два определения...

Определение (2)

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

где

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

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.

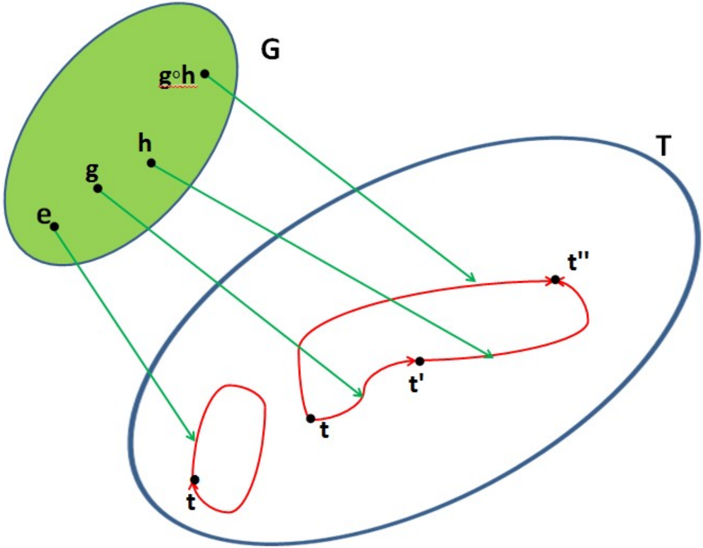


Рис. 2. К определению действия группы на множестве

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 $C(g)$ циклов (классов эквивалентности).

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

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 $C(g)$ циклов (классов эквивалентности).

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

$$\begin{aligned} T &= \{\,1,\,\ldots,\,10\,\},\\ g &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 9 & 6 & 1 & 8 & 5 & 2 & 7 & 10 & 3 & 4 \end{pmatrix} =\\ &= (1,9,3)(2,6)(4,8,10)(5)(7) \end{aligned}$$

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 —

$$t \sim_{\mathbb{G}} t' \overset{\text{def}}{=} \underset{G}{\exists}\, g \left(g(t) = t' \right).$$

Классы этой эквивалентности называют *орбитами*.

По всей группе $\mathbb{G}$:

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

$$t \sim_{\mathbb{G}} t' \overset{\text{def}}{=} \underset{G}{\exists}\, g \left(g(t) = t' \right).$$

Классы этой эквивалентности называют *орбитами*.

Число орбит (классов эквивалентности) — $C(\mathbb{G})$.

По всей группе $\mathbb{G}$:

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

$$t \sim_{\mathbb{G}} t' \stackrel{\text{def}}{=} \underset{G}{\exists}\, g\, \big(\, g(t) = t' \,\big)\,.$$

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 (*фиксатор*):

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

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 (*фиксатор*):

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

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

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

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 (*фиксатор*):

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

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

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

Справедливы равенства

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

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 (*фиксатор*):

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

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

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

Справедливы равенства

$$C(\mathbb{G}) = \frac{1}{|G|}\sum_{g\in G}\Bigl|\mathrm{Fix}\,(g)\Bigr| = \frac{1}{|G|}\sum_{t\in T}\Bigl|\mathrm{Stab}\,(t)\Bigr|\,;$$

первое называется *леммой Бёрнсайда* (W.Burnside, 1911).

Стабилизатор есть подгруппа

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

Лемма

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

Стабилизатор есть подгруппа

1. $\mathrm{Fix}\,(g)$ — *фиксатор* 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* $h^{-1}(t) = t$. *Следовательно,*

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

Стабилизатор есть подгруппа

1. $\mathrm{Fix}\,(g)$ — *фиксатор* 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* $h^{-1}(t) = t$. *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 $\mathrm{Stab}\,(t)$.

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.

Стабилизатор

Лемма

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

$$|\operatorname{Orb}(t)| = |G| : |\operatorname{Stab}(t)|.$$

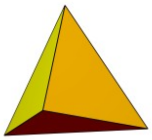
Пример

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

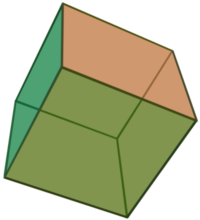
Решение: $\operatorname{Stab}(t) \cong \mathbb{Z}_3$ — группа вращений на 120° вокруг диагонали куба, проходящей через данную вершину.

Утверждение

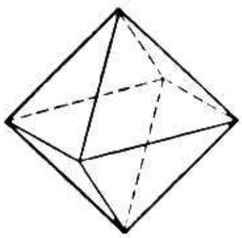
Число элементов в группе вращения правильного многогранника есть $|V| \cdot |E_0|$, *где* $|V|$ *— число вершин, а* $|E_0|$ *— число рёбер, выходящих из одной вершины.*



Это тетраэдр



А это — кубик



Октаэдр двойственен кубу

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

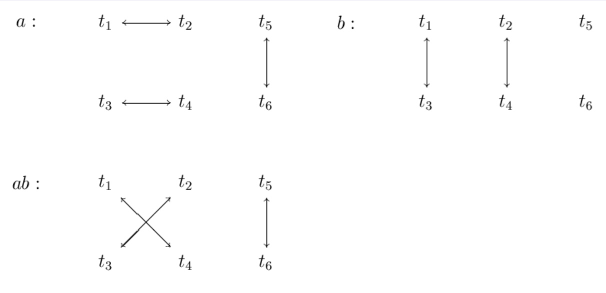
Додекаэдр

Пример

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

$\circ$	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

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

Простая задача

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 перестановкой крайних букв. Определить число S неэквивалентных слов.

Простая задача

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 перестановкой 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 $G \cong \mathbb{Z}_2 = \{e, g\}$.

Действие: g переставляет в слове крайние буквы.

Продолжение решения

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 всего 8)*

Продолжение решения

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 всего 8)*
Пусть $A = \{a, b\}$. *Показаны слова и классы.*

aaa	*baa*
aab	*bab*
aba	*bba*
abb	*bbb*

Стабилизаторы сопряжённых элементов группы совпадают

Задача

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

Стабилизаторы сопряжённых элементов группы совпадают

Задача

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

Решение

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

Действие группы O на вершины куба

Задача

Группа вращений куба действует на множество его вершин. Определить типы всех перестановок этой группы.

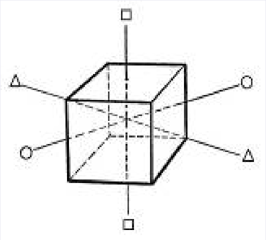
Действие группы O на вершины куба

Задача

Группа вращений куба действует на множество его вершин. Определить типы всех перестановок этой группы.

Решение

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

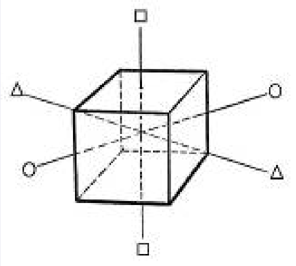


t — *вращение на* 90° *вокруг оси, проходящей через середины двух противоположных граней* ($\square$—$\square$);

f — *вращение на* 180° *вокруг оси, проходящей через середины двух противоположных рёбер* ($\circ$—$\circ$);

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

Действие группы O на вершины куба: продолжение решения



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

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

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

Цикловой индекс

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

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

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

Цикловой индекс

Существует универсальный способ вычисления числа $\frac{1}{|G|}\sum_{g\in G}\Big|\mathrm{Fix}\,(g)\Big| = C(\mathbb{G})$ классов эквивалентности (орбит).

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

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

Определение

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

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

Цикловой индекс

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

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

$$Type(g) = \langle \nu_1, \dots, \nu_N \rangle \Rightarrow w(g) = \underbrace{x_1^{\nu_1} \cdot \ldots \cdot x_N^{\nu_N}}_{\text{моном}}.$$

Определение

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

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

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

Цикловой индекс: обозначения и свойста

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

Цикловой индекс: обозначения и свойста

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

Как применять лемму не Бёрнсайда?

Для применения универсального способа вычисления $C(\mathbb{G})$ надо представить эквивалентные элементы множества как классы эквивалентности действия некоторой группы на этом множестве.

Число неэквивалентных раскрасок

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

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 (неформально: покрасим в один из r цветов). Всего имеется r^N раскрасок.

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 (неформально: покрасим в один из r цветов). Всего имеется r^N раскрасок.
- Не будем различать раскраски, если при преобразовании $g : t \to t'$ элемент сохраняет цвет (t раскрашен также как t', и каждый g-цикл раскрашен одним своим цветом).

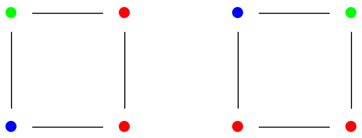


Рис. 3. Перестановка g (поворот на 90°) не даёт нового раскрашивания

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 (неформально: покрасим в один из r цветов). Всего имеется r^N раскрасок.
- Не будем различать раскраски, если при преобразовании $g : t \to t'$ элемент сохраняет цвет (t раскрашен также как t', и каждый g-цикл раскрашен одним своим цветом).

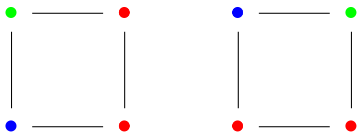


Рис. 3. Перестановка g (поворот на 90°) не даёт нового раскрашивания

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.

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 лемме Бёрсайда, число полученных классов эквивалентности, т.е. неэквивалентных раскрасок (приписываний) есть

Теорема

$$C(\mathbb{G} \underset{\alpha}{:} T) = P(\mathbb{G} \underset{\alpha}{:} T, x_1, \ldots, x_N)\Big|_{x_1 = \ldots x_N = r} = P_{\mathbb{G}}(r, \ldots, r).$$

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 лемме Бёрсайда, число полученных классов эквивалентности, т.е. неэквивалентных раскрасок (приписываний) есть

Теорема

$$C(\mathbb{G} \underset{\alpha}{:} T) = P(\mathbb{G} \underset{\alpha}{:} T, x_1, \ldots, x_N)\Big|_{x_1 = \ldots x_N = r} = P_{\mathbb{G}}(r, \ldots, r).$$

Например, $P_{\mathbb{G}}(1, \ldots, 1) = 1$: если все элементы покрасить в один цвет, то таких раскрасок одна.

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 перестановкой крайних букв. Определить число* S *неэквивалентных слов.*

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 перестановкой крайних букв. Определить число S неэквивалентных слов.

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

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 перестановкой 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: $\underbrace{\bigcirc \overbrace{\bigcirc \ldots \bigcirc}^{l-2} \bigcirc}_{l}$.

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

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

Классическая комбинаторная задача об ожерельях

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

Классическая комбинаторная задача об ожерельях

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?

Классическая комбинаторная задача об ожерельях

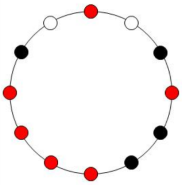
Ожерелье — окружность, на которой на равных расстояниях по дуге располагаются «бусины» (бусины располагаются в вершинах правильного многоугольника).

Задача (об ожерельях)

Сколько различных ожерелий можно составить из n бусин r цветов?

Варианты. Ожерелья равны iff 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?

Задача об ожерельях: $N = 5, r = 3$

Задача

Сколько разных ожерелий можно составить из 5 бусин 3 цветов?

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

1. Ожерелья одинаковы, если одно получается из другого поворотом

Задача об ожерельях: $N = 5, r = 3$

Задача

Сколько разных ожерелий можно составить из 5 бусин 3 цветов?

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

1. Ожерелья одинаковы, если одно получается из другого поворотом

Решение

$\mathbb{G} \cong \mathbb{Z}_5 = \langle t \rangle$, $t^5 = e$, $n = 5$.

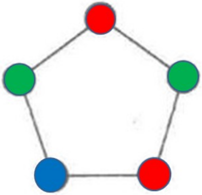
Элемент группы g	$Type(g)$	$w(g)$	# мономов
e	$\langle 5, 0, 0, 0, 0 \rangle$	x_1^5	1
$t,\ t^2,\ t^3,\ t^4$	$\langle 0, 0, 0, 0, 1 \rangle$	x_5	4

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

$$\#Col(3) = P(3, \ldots, 3) = \frac{3^5 + 4 \cdot 3}{5} = \frac{3 \cdot 85}{5} = 3 \cdot 17 = 51.$$

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?



Как должны были решать дети

Решение

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: $\#Col(r) = \dfrac{r^5 - r}{5} + r = \dfrac{r^5 + 4r}{5}$;

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.

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

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

Запомним этот ответ.

Задача о раскраске куба

Задача (раскраска куба в два цвета)

Грани куба раскрашивают в 2 цвета.
Сколько существует различно окрашенных кубов?

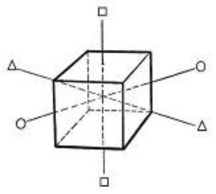
Задача о раскраске куба

Задача (раскраска куба в два цвета)

Грани куба раскрашивают в 2 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 середины двух противоположных граней (□—□, 3 оси);
f — вращение на 180° вокруг оси, проходящей через середины двух противоположных рёбер (○—○, 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 неориентированных непомеченных графов (без петель и кратных рёбер) с тремя вершинами?

Задача (Перечисление графов)

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

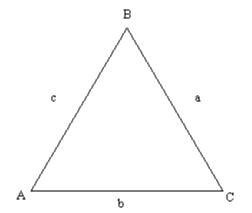
Решение

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»*

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

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

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

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

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

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

$P_1(x_1, x_2, x_3) \;=\; \frac{1}{6}\left[\, x_1^3 + 2x_3^1 + 3x_1^1 x_2^1 \,\right],$
$P_1(2, 2, 2) \;=\; \mathbf{4}.$

Цикловые индексы самодействия и действия O на элементы куба

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

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

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

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

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

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

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать

2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

Теорема Пойа

К множеству T, $|T| = N$, группе $\mathbb{G}$, $|G| = n$ и действию $\mathbb{G} \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T.

Теорема Пойа

К множеству T, $|T| = N$, группе $\mathbb{G}$, $|G| = n$ и действию $\mathbb{G} \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T. $\mathbb{G}$, действуя на T, действует и на R^T — $\circ : R^T \times G \stackrel{\circ}{=} R^T$.

Теорема Пойа

К множеству T, $|T| = N$, группе $\mathbb{G}$, $|G| = n$ и действию $\mathbb{G} \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T. $\mathbb{G}$, действуя на T, действует и на R^T — $\circ : R^T \times G \overset{\circ}{=} R^T$. Дадим вес элементам R: $w(c_i) = y_i$, $i = \overline{1, r}$.

Теорема Пойа

К множеству T, $|T| = N$, группе $\mathbb{G}$, $|G| = n$ и действию $\mathbb{G} \underset{\alpha}{:} T$ добавим множество $R = \{c_1, \ldots, c_r\}$, меток («красок»), и совокупность функций $F = R^T$ — приписывания меток (*раскрашиваний*) элементам T. $\mathbb{G}$, действуя на T, действует и на R^T — $\circ : R^T \times G \overset{\circ}{=} R^T$. 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

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

Следствие

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

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

— лемма Бёрнсайда.

Следствие

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

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

— лемма Бёрнсайда.

Что можно определить (подсчитать) с помощью:

леммы Бёрнсайда — общее число неэквивалентных разметок (раскрасок);

теорема Редфилда-Пойа — число разметок данного типа, (содержащих данное количество элементов конкретного цвета).

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, если одно получается из другого поворотом и/или переворотом.

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, 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* $\#Col(3) = P(3, \ldots, 3) = 39$.

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, 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* $\#Col(3) = P(3, \ldots, 3) = 39$.

$$x_1 = y_1 + y_2 + y_3,\ x_2 = y_1^2 + y_2^2 + y_3^2,\ \ldots,\ x_k = y_1^k + y_k^2 + y_k^2.$$

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, 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* $\#Col(3) = P(3,\ldots,3) = 39$.

$$x_1 = y_1 + y_2 + y_3,\ x_2 = y_1^2 + y_2^2 + y_3^2,\ \ldots,\ x_k = y_1^k + y_k^2 + y_k^2.$$

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

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

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

$$C = \frac{1}{10}\left[u_0 + u_1 y + u_2 y^2 + \ldots + u_5 y^5\right] =$$

$$= \frac{1}{10}\left[(y+2)^5 + 4(y^5+2) + 5(y+2)(y^2+2)^2\right] =$$

$$= \frac{1}{10}\left[\ldots + C_5^2 y^2 2^3 + \ldots + 5(y+2)(y^4+4y^2+4)\right] =$$

$$= \frac{1}{10}\left[\ldots + (10\cdot 8 + 5\cdot 2\cdot 4)y^2 + \ldots\right].$$

$$u_2 = \frac{80+40}{10} = 12.$$

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?*

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

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

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

$$\#Col(4,4) = \frac{1}{24}\Big[\,(y+1)^8 + 9\cdot(y^2+1)^4 + 6\cdot(y^4+1)^2 + 8\cdot(y+1)^2(y^3+1)^2\,\Big] =$$

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

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

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

$$\#Col(4,4) = \frac{1}{24}\Big[(y+1)^8 + 9\cdot(y^2+1)^4 + 6\cdot(y^4+1)^2 + 8\cdot(y+1)^2(y^3+1)^2\Big] =$$

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

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

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

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

$$= \frac{28+36+8}{24} = \frac{72}{24} = 3. \quad \#Col(\leqslant 2, *) = 1+1+3 = 5.$$

Задача

Рассматриваются молекулы 4-х валентного углерода C*:*

$$
\begin{array}{ccccc}
 & & \times & & \\
 & & | & & \\
\times & — & \mathrm{C} & — & \times \\
 & & | & & \\
 & & \times & &
\end{array}
\qquad\qquad
\begin{array}{ccccc}
 & & \mathrm{CH_3} & & \\
 & & | & & \\
\mathrm{Cl} & — & \mathrm{C} & — & \mathrm{CH_3} \\
 & & | & & \\
 & & \mathrm{Cl} & &
\end{array}
$$

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.*

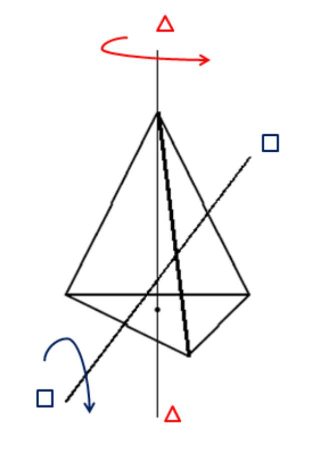
Решение

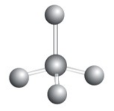
Какая группа действует на каком множестве?

Решение

Какая группа действует на каком множестве?

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





t — *вращение на* 120° *вокруг оси, проходящей через вершину и центр тетраэдра* ($\triangle$—$\triangle$);

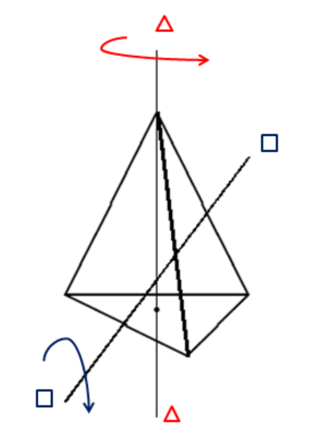
f — *вращение на* 180° *вокруг оси, проходящей через центры двух противоположных рёбер* ($\square$—$\square$).

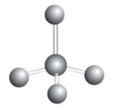
$$P(T \underset{\alpha}{:} V) = \frac{1}{12}\left[x_1^4 + 8x_1x_3 + 3x_2^2\right].$$

Решение

Какая группа действует на каком множестве?

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





t — вращение на 120° вокруг оси, проходящей через вершину и центр тетраэдра ($\triangle$—$\triangle$);

f — вращение на 180° вокруг оси, проходящей через центры двух противоположных рёбер ($\square$—$\square$).

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

Почему перед x_1x_3 коэффициент 8, ведь осей $\triangle$—$\triangle$ всего 4?

(продолжение)

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 (4 радикала) —

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

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

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

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 — $1 + 3 + 6 + 11 + 15 = 36$.

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

- Действие группы на множестве: два определения. g-циклы, тип перестановки. Орбиты.
  Неподвижные точки группы преобразований: фиксатор и стабилизатор. Лемма Бёрнсайда.
- Группы вращений платоновых тел. Примеры.
- Применение леммы Бёрнсайда для решения комбинаторных задач. Примеры.
- Действие группы вращений куба на его элементы.
- Цикловой индекс: определение и свойства. Вычисление числа орбит через цикловой индекс. Примеры.
- Решения комбинаторной задачи об ожерельях.
- Теорема Редфилда-Пойа и её применение для решения комбинаторных задач. Примеры.

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать

2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

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: $(x \leqslant y) \,\&\, (y \leqslant z) \Rightarrow x \leqslant z$.

Примеры

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

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

- если $(x \leqslant y) \vee (y \leqslant x)$, то x и y *сравнимы* $(x \sim y)$, иначе они *несравнимы* $(x \nsim y)$;
- *полный (линейный) порядок*, если $\forall x, y\, (x \sim y)$;
- если в $\mathbf{P}$ нет ни одной пары различных 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* $[\, a, b \,]$;
- $v_1 \leqslant \ldots \leqslant v_n \overset{\text{def}}{=} [v_1, \ldots, v_n]$ — *цепь* ($\mathbf{n}$ или $\underline{n}$), а совокупность попарно несравнимых элементов — *антицепь* в $\mathbf{P}$;
- цепь *максимальная* (или *насыщенная*), если при добавлении к ней любого элемента она перестаёт быть цепью;
- если $\forall x, y \; \big((x \leqslant y) \;\Rightarrow\; (y \leq x) \big)$, то $\leq$ — *двойственный порядок на* P, $\geqslant \overset{\text{def}}{=} \leq$ или $\leqslant^d = \geqslant$.

Диаграммы Хассе

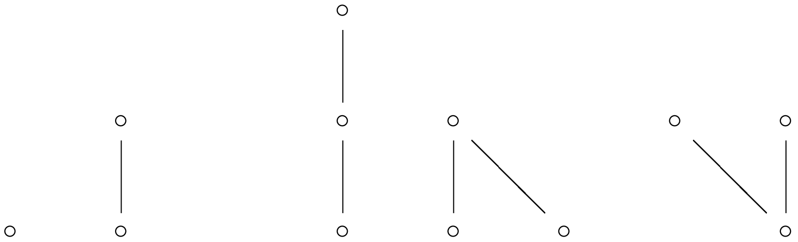


Рис. 4. Диаграммы 4-х нетривиальных непомеченных 3-элементных ч.у. множеств

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 $x \in P$.

Ч.у. множества: особые элементы

Определение

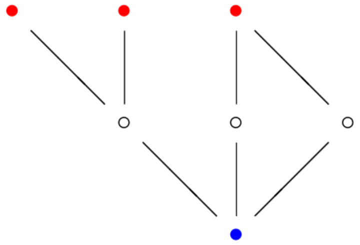
Элемент $u \in P$ ч.у. множества $\langle P, \leqslant \rangle$ называют:

- *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 $x \in P$.

Элемент наибольший, если все другие элементы содержатся в нём, и он максимальный, если нет элементов, содержащих его (аналогично для наименьшего и минимального элементов).

Особые элементы ч.у. множества: пример

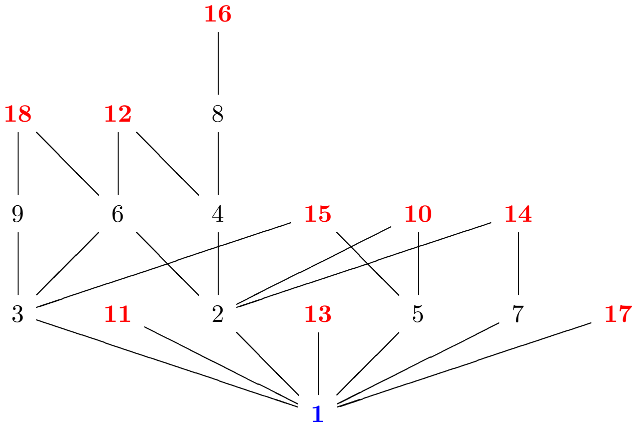


- — максимальные элементы;
- — минимальный и наименьший элемент;

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

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

Ч.у. множество $\langle \{1, \ldots, 18\}, | \rangle$



1 — наименьший элемент, ● — максимальные.

Ранжированные ч.у. множества

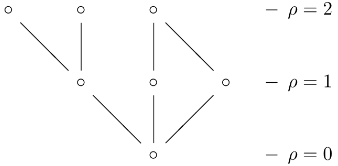
Цепное условие Жордана-Дедекинда

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 гомоморфизмом*), 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

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

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

$$(x \in F)\,\&\,(x \leqslant y) \;\Rightarrow\; y \in F.$$

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

$$(x \in F) \,\&\, (x \leqslant y) \;\Rightarrow\; y \in F.$$

По определению, $\varnothing$ и всё P — порядковые идеалы.

Объединение и пересечение порядковых идеалов есть порядковый идеал.

$J(\mathbf{P})$ — множество всех порядковых идеалов ч.у. множества $\mathbf{P}$.

Конусы

Определение

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$. Множества $A^{\vartriangle}$ и $A^{\triangledown}$ определяемые условиями

$$A^{\vartriangle} = \{x \in P \mid \underset{A}{\forall a} \, (a \leqslant x)\} \text{ и } A^{\triangledown} = \{x \in P \mid \underset{A}{\forall a} \, (x \leqslant a)\}$$

называются *верхним* и *нижним конусами множества* A, а их элементы — *верхними* и *нижними гранями множества* A соответственно. Для одноэлементного множества $A = \{a\}$ используются обозначения $a^{\vartriangle}$ и $a^{\triangledown}$.

Конусы

Определение

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$. Множества $A^{\vartriangle}$ и $A^{\triangledown}$ определяемые условиями

$$A^{\vartriangle} = \{x \in P \mid \underset{A}{\forall a}\ (a \leqslant x)\} \text{ и } A^{\triangledown} = \{x \in P \mid \underset{A}{\forall a}\ (x \leqslant a)\}$$

называются *верхним* и *нижним конусами множества* A, а их элементы — *верхними* и *нижними гранями множества* A соответственно. Для одноэлементного множества $A = \{a\}$ используются обозначения $a^{\vartriangle}$ и $a^{\triangledown}$.

Понятно, что если $a \leqslant b$, то $a^{\vartriangle} \cap b^{\triangledown} = [a, b]$.

$x^{\triangledown} = J(x)$ — идеал; $x^{\vartriangle}$ — фильтр P; такие идеалы и фильтры называют *главными*.

Точные грани

Определение

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$.

- Наименьший элемент в $A^{\vartriangle}$ называется *точной верхней гранью множества* A (символически $\sup A$).
- Наибольший элемент в $A^{\triangledown}$ называется *точной нижней гранью множества* A (символически $\inf A$).

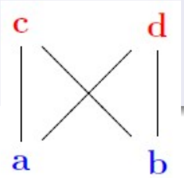
Точные грани

Определение

Пусть $\langle P, \leqslant \rangle$ — ч.у. множество и $A \subseteq P$.

- Наименьший элемент в $A^{\triangle}$ называется *точной верхней гранью множества* A (символически $\sup A$).
- Наибольший элемент в A^{∇} называется *точной нижней гранью множества* A (символически $\inf A$).

Пример ($\sup A$ и/или $\inf A$ могут и не существовать)



$\{a,b\}^{\triangle} = \{c,d\}$, но множество $\{c,d\}$ не имеет инфимума $\Rightarrow$ $\sup\{a,b\}$ отсутствует. Аналогично, отсутствует $\inf\{c,d\}$.

Раздел I

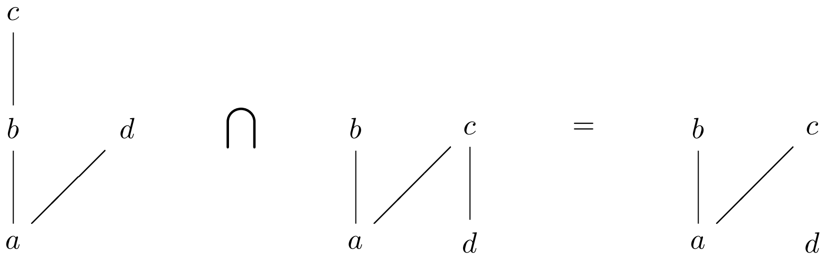
1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

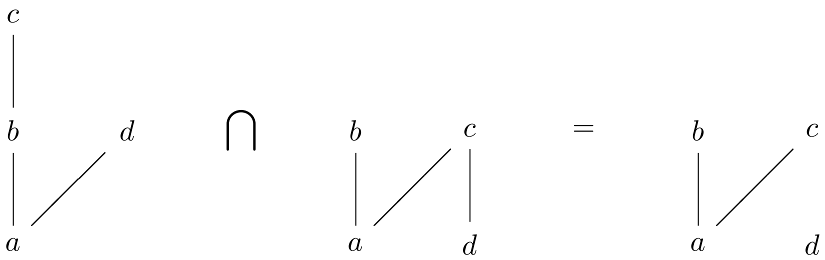
Пересечение

$$\langle P, \leqslant_1 \rangle \cap \langle P, \leqslant_2 \rangle = \langle P, \leqslant_1 \cap \leqslant_2 \rangle.$$



Пересечение

$$\langle\, P,\, \leqslant_1 \rangle \cap \langle\, P,\, \leqslant_2 \rangle \;=\; \langle\, P,\, \leqslant_1 \cap \leqslant_2 \rangle.$$



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 $P \cap Q = \varnothing$.

$$\mathbf{P} + \mathbf{Q} \;=\; \langle\, P \cup Q,\ \leqslant_P \vee \leqslant_Q \,\rangle.$$

Прямая сумма

$\mathbf{P} = \langle\, P, \leqslant_P \,\rangle$ и $\mathbf{Q} = \langle\, Q, \leqslant_Q \,\rangle$ — два ч.у. множества, причём $P \cap Q = \varnothing$.

$$\underline{\mathbf{P} + \mathbf{Q} \;=\; \langle\, P \cup Q,\ \leqslant_P \vee \leqslant_Q \,\rangle.}$$

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 $\mathbf{P}$, $n\mathbf{1}$ — n-элементная антицепь.

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

$$\mathbf{P} \times \mathbf{Q} \;= \langle\, P \times Q,\, \leqslant \rangle,$$

где $(p,\, q) \leqslant (p',\, q') \;\Leftrightarrow\; (p \leqslant_P p')\&(q \leqslant_Q q')$.

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

$$\mathbf{P} \times \mathbf{Q} = \langle\, P \times Q,\, \leqslant \,\rangle,$$

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

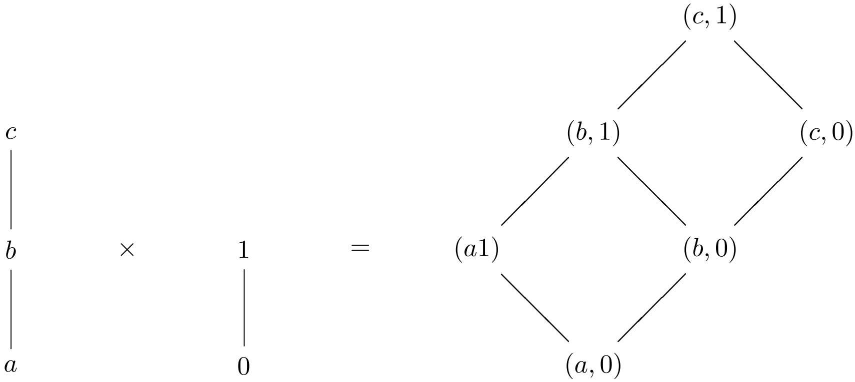


Рис. 5. Прямое произведение цепей $\mathbf{3}$ и $\mathbf{2}$

Прямое произведение: пример 2

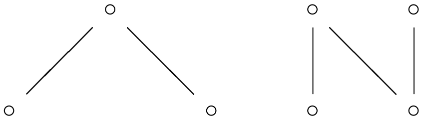


Рис. 6. Зигзаги (или заборы) $\mathbf{Z}_3$ и $\mathbf{Z}_4$

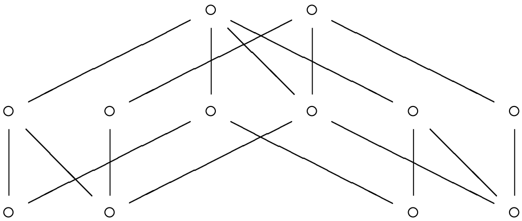


Рис. 7. Прямое произведение $\mathbf{Z}_3 \times \mathbf{Z}_4$

Теорема (Оре)

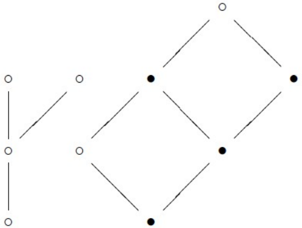
Каждый частичный порядок изоморфен некоторому подмножеству декартова произведения цепей.

Теорема (Оре)

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

Раздел III

- Линеаризация
- Что надо знать

5 Алгебраические решётки

- Решётки: определение, основные свойства
- Модулярные и дистрибутивные решётки
- Применение теории решёток к задаче классификации
- Что надо знать

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 $\mathbf{P}$.

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, $|P| = n$)

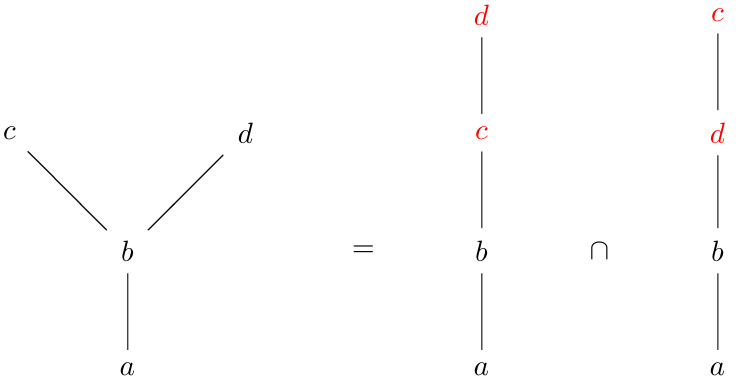
1. *Если $\mathbf{P}$ — не цепь, то в P найдутся несравнимые элементы; произвольно определим порядок на них и продолжим его по транзитивности. Если получившиеся ч.у. множество ещё не цепь, то выберем новую пару несравнимых элементов и поступаем, как указано выше. Через конечное число шагов получаем линейный порядок.*

Топологическая сортировка

1. *(продолжение). Т.к. возможен различный выбор пар несравнимых элементов и при каждом выборе можно полагать любой их порядок, то можно получить все возможные линейные продолжения исходного частичного порядка.*
2. *Пересечение всех таких цепей даст исходное ч.у. множество: 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 ч.у. множеств заданных парами вида $a \lessdot b$, поиск такого линейного продолжения в теоретическом программировании называют *топологической сортировкой*. Задача решается за линейное время.

Представление ч.у. множества пересечением цепей



Некоторые ч.у. множества

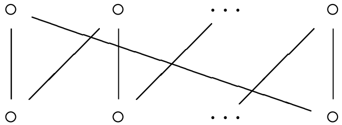


Рис. 8. Малая корона $\mathbf{s}_n$

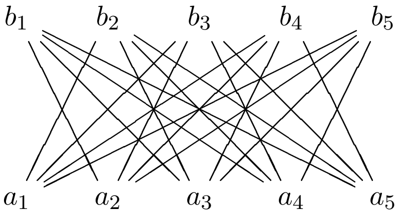


Рис. 9. Корона $\mathbf{S}_5$

«$e(\mathrm{P}) = ?$» — NP-полная задача, но:

- $e(\mathbf{P}+\mathbf{Q}) = \binom{n+m}{n} e(\mathbf{P})e(\mathbf{Q}), \quad n = |\mathbf{P}|,\ m = |\mathbf{Q}|;$
- $e(\mathbf{2}\times\mathbf{n}) = \frac{1}{n+1}\binom{2n}{n}$ — *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*;
- $e(\mathbf{S}_n) = (n+1)!(n-1)!\,;$
- $$\sum_{n\geqslant 1} \frac{e(\mathbf{s}_n)}{n!}\,x^n = \frac{x}{\cos^2 x}\,;$$
- $$\frac{\log(e(B^n))}{2^n} = \log\binom{n}{\lfloor n/2\rfloor} - \frac{3}{2}\log e + o(1)\,.$$

Вероятностное пространство на линеарезациях

При решении 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*.

Вероятностное пространство на линеарезациях

При решении 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, $\ldots$ данного ч.у. множества рассматривают события E вида $x \leqslant y$, $(x \leqslant y) \,\&\, (x \leqslant z)$ и т.д.

Вероятностное пространство на линеарезациях

При решении 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, $\ldots$ 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:

$$\Pr[E] = \frac{\text{число линеаризаций, в которых имеет место } E}{e(\mathbf{P})}.$$

Вероятностное пространство на линеарезациях

При решении 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, $\ldots$ 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:

$$\Pr[E] = \frac{\text{число линеаризаций, в которых имеет место } E}{e(\mathbf{P})}.$$

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 порядк $\mathbf{L}$ с помощью минимального количества вопросов «*верно ли, что $x < y$ в $\mathbf{L}$?*».

Обобщение: $\mathbf{L}$ — зафиксированная, но неизвестная линеаризация ч.у. множества $\mathbf{P}$.

Оптимальная процедура поиска $\mathbf{L}$ включает в себя нахождение элементов x и y, для которых $\Pr[\,x < y\,] \approx \frac{1}{2}$.

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: $\mathbf{L}$ — зафиксированная, но неизвестная линеаризация ч.у. множества $\mathbf{P}$.

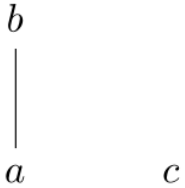
Оптимальная процедура поиска $\mathbf{L}$ включает в себя нахождение элементов x и y, для которых $\Pr[x < y] \approx \frac{1}{2}$.

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*

$$\frac{1}{3} \leqslant \Pr[x \leqslant y] \leqslant \frac{2}{3}\text{''}.$$

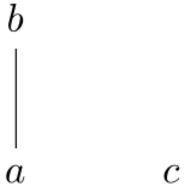
Позднее это утверждение независимо выдвинули американские исследователи М. Фредман и Н. Линал.

1/3 – 2/3 предположение



Пример $\mathbf{2}+\mathbf{1}$ показывает, что указанные границы несужаемы (имеется и пример десятиэлементного ч.у. множества со связанной диаграммой Хассе).

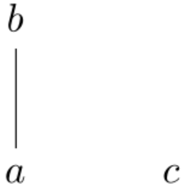
1/3 – 2/3 предположение



Пример $\mathbf{2}+\mathbf{1}$ 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).

1/3 – 2/3 предположение



Пример $\mathbf{2} + \mathbf{1}$ 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

Определение:

$$\underline{Spec\,(\mathbf{P}) \;=\; \{\; \mathrm{Pr}\,[\,a \leqslant b\,] \mid a, b \in P,\; a \neq b\,\}}$$

Ч.у. множества: спектр

Определение:

$$\underline{Spec\,(\mathbf{P}) \;=\; \{\; \Pr\,[\,a \leqslant b\,] \mid a, b \in P,\; a \neq b\,\}}$$

Ясно, что

- 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 $0 < \alpha < \frac{1}{2}$;

Ч.у. множества: спектр

Определение:

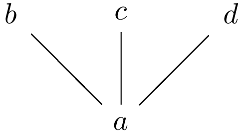
$$\underline{Spec\,(\mathbf{P}) \;=\; \{\ \Pr\,[\,a \leqslant b\,] \mid a, b \in P,\ a \neq b\,\}}$$

Ясно, что

- 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 $0 < \alpha < \frac{1}{2}$;
  <u>Гипотеза (2002)</u>: $\alpha \;=\; \frac{1}{3}$.

Ч.у. множества: размерность

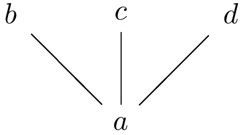
По теореме Шпильрайна ч.у. множество $\mathbf{P}$ совпадает с пересечением всех $e(\mathbf{P})$ своих линеаризаций.
Однако тот же результат можно получить, взяв значительно меньшее число линейных продолжений. Например, ч.у. множество $\mathbf{P}$



имеет 6 линеаризаций, но $\mathbf{P} = [a, b, c, d] \cap [a, d, c, b]$.

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 6 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 $\dim(P)$).

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 (Оре)

Порядковая и мультипликативная размерности ч.у. множества совпадают.

Ч.у. множества: размерность...

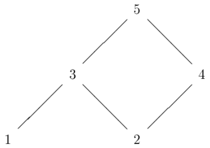
Определение

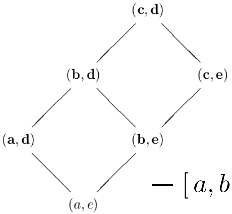
Наименьшее число линейных порядков, дающих в пересечении данное ч.у. множество $\mathbf{P}$ называется его *(порядковой) размерностью* (символически $\dim(P)$).

Теорема (Оре)

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 $e(\mathbf{P})$

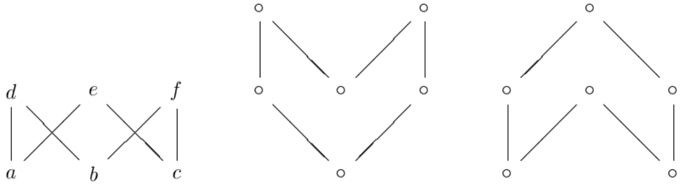
Размерность ... имеют:

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 — s_3, $\mathbf{sh}$ и $\mathbf{sh}^d$ (см. диаграммы) :

n — $\mathbf{S}_n$



О размерности ч.у. множества $\mathbf{P} = \langle P, \leqslant \rangle$

- $\varnothing \neq Q \subseteq P \Rightarrow \dim(\mathbf{Q}) \leqslant \dim(\mathbf{P})$, при удалении 1-го элемента его размерность уменьшается не более, чем на 1;
- $\dim(\mathbf{P}+\mathbf{Q}) = \max\{\dim(\mathbf{P}), \dim(\mathbf{Q})\}$, если хотя бы одно из множеств не является цепью и $\dim(\mathbf{P}+\mathbf{Q}) = 2$;
- $\dim(\mathbf{P} \times \mathbf{Q}) \leqslant \dim(\mathbf{P}) + \dim(\mathbf{Q})$;
- $\dim(\mathbf{P}) \leqslant |\mathbf{P}|/2$ при $|\mathbf{P}| \geqslant 4$ (теорема Хирагучи).

О размерности ч.у. множества $\mathbf{P} = \langle P, \leqslant \rangle$

- $\varnothing \neq Q \subseteq P \Rightarrow \dim(\mathbf{Q}) \leqslant \dim(\mathbf{P})$, при удалении 1-го элемента его размерность уменьшается не более, чем на 1;
- $\dim(\mathbf{P}+\mathbf{Q}) = \max \{ \dim(\mathbf{P}), \dim(\mathbf{Q}) \}$, если хотя бы одно из множеств не является цепью и $\dim(\mathbf{P}+\mathbf{Q}) = 2$;
- $\dim(\mathbf{P} \times \mathbf{Q}) \leqslant \dim(\mathbf{P}) + \dim(\mathbf{Q})$;
- $\dim(\mathbf{P}) \leqslant |\mathbf{P}|/2$ при $|\mathbf{P}| \geqslant 4$ (теорема Хирагучи).

Теорема («компактности»)

Пусть $\mathbf{P}$ — такое ч.у. множество, что любое его конечное ч.у. подмножество имеет размерность, не превосходящую d. Тогда $\dim(\mathbf{P}) \leqslant d$.

О размерности ч.у. множества $\mathbf{P} = \langle P, \leqslant \rangle$

- $\varnothing \neq Q \subseteq P \Rightarrow \dim(\mathbf{Q}) \leqslant \dim(\mathbf{P})$, при удалении 1-го элемента его размерность уменьшается не более, чем на 1;
- $\dim(\mathbf{P}+\mathbf{Q}) = \max\left\{ \dim(\mathbf{P}), \dim(\mathbf{Q}) \right\}$, если хотя бы одно из множеств не является цепью и $\dim(\mathbf{P}+\mathbf{Q}) = 2$;
- $\dim(\mathbf{P} \times \mathbf{Q}) \leqslant \dim(\mathbf{P}) + \dim(\mathbf{Q})$;
- $\dim(\mathbf{P}) \leqslant |\mathbf{P}|/2$ при $|\mathbf{P}| \geqslant 4$ (теорема Хирагучи).

Теорема («компактности»)

Пусть $\mathbf{P}$ *— такое ч.у. множество, что любое его конечное ч.у. подмножество имеет размерность, не превосходящую* d. *Тогда* $\dim(\mathbf{P}) \leqslant d$.

$$wp1: \quad \frac{n}{4}\left(1 - \frac{c_1}{\log n}\right) \leqslant \dim(\mathbf{P}) \leqslant \frac{n}{4}\left(1 - \frac{c_2}{\log n}\right), \quad n = |\mathbf{P}|.$$

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);

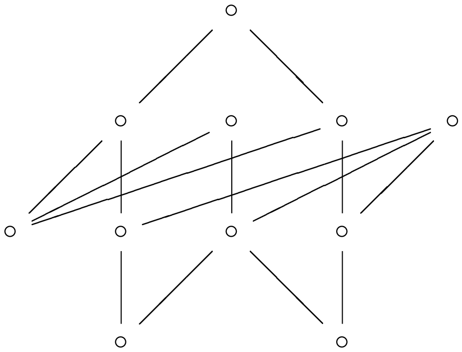
3 — $\mathbf{s}_3, \mathbf{sh}, \mathbf{sh}^d + \ldots$ — описаны, регулярны и хорошо изучены;

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.

4-несводимое ч.у. множество



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.

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

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

- Коды БЧХ
- Задачи
- Что надо знать

3. **Теория перечисления Пойа**
   - Действие группы на множестве
   - Применение леммы Бёрнсайда для решения комбинаторных задач
   - Применение теоремы Пойа для решения комбинаторных задач
   - Что надо знать

4. **Некоторые вопросы теории частично упорядоченных множеств**
   - Основные понятия теории ч.у. множеств
   - Операции над ч.у. множествами

Раздел III

- Линеаризация
- Что надо знать

5 Алгебраические решётки

- Решётки: определение, основные свойства
- Модулярные и дистрибутивные решётки
- Применение теории решёток к задаче классификации
- Что надо знать

- Частично упорядоченные (ч.у.) множества: определение, примеры, основные понятия. Диаграммы Хассе и особые элементы ч.у. множеств.
- Ранжированные ч.у. множества. Цепное условие Жордана-Дедекинда. Порядковые гомоморфизмы
- Идеалы и фильтры ч.у. множеств. Конусы. Точные грани.
- Операции над ч.у. множествами.
- Теорема Шпильрайна. Линейное продолжение ч.у. множества и топологическая сортировка.
- Линеаризации и вероятностное пространство над ними. XYZ-теорема. Проблема сортировки и «$1/3 - 2/3$ предположение».
- Спектр и размерность ч.у. множеств. Свойства размерности, d-несводимые множества и проблема Ногина.

Раздел I

Раздел II

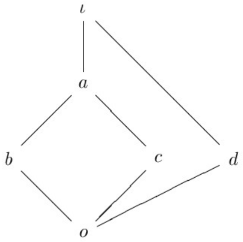
Раздел III

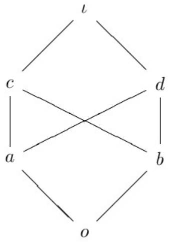
Решёточно упорядоченное множество

Определение

Ч.у. множество, в котором для любых элементов a и b существуют $\inf\{a, b\}$ и $\sup\{a, b\}$ называют *решёточно упорядоченным*.

Решётка называется *полной*, если *любое подмножество* её элементов имеет точные верхнюю и нижнюю грани.





Алгебраические решётки: определение

Определение

Алгебраическая решётка — это тройка $\mathbf{L} = \langle L, \sqcup, \sqcap \rangle$, где L — непустое множество, а $\sqcup$ (*объединение*), $\sqcap$ (*пересечение*) — бинарные операции на нём, подчиняющимися парам законов коммутативности, ассоциативности, идемпотентности и поглощения:

$$x \sqcup y = y \sqcup x; \qquad x \sqcap y = y \sqcap x;$$
$$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z; \qquad x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z;$$
$$x \sqcup x = x; \qquad x \sqcap x = x,$$
$$x \sqcap (x \sqcup y) = x; \qquad x \sqcup (x \sqcap y) = x.$$

Алгебраические решётки: определение

Определение

Алгебраическая решётка — это тройка $\mathbf{L} = \langle L, \sqcup, \sqcap \rangle$, где L — непустое множество, а $\sqcup$ (*объединение*), $\sqcap$ (*пересечение*) — бинарные операции на нём, подчиняющимися парам законов коммутативности, ассоциативности, идемпотентности и поглощения:

$$x \sqcup y = y \sqcup x; \qquad x \sqcap y = y \sqcap x;$$
$$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z; \qquad x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z;$$
$$x \sqcup x = x; \qquad x \sqcap x = x,$$
$$x \sqcap (x \sqcup y) = x; \qquad x \sqcup (x \sqcap y) = x.$$

Принцип двойственности для решёток

Любое утверждение, истинное для любых произвольных элементов решётки, остаётся таковым при замене $\sqcap \leftrightarrow \sqcup$.

Решётка всех разбиений множества — беллиан

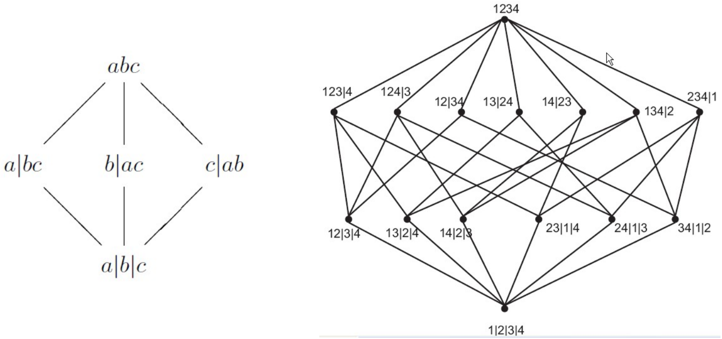


Рис. 10. Беллианы множеств $\{a, b, c\}$ и $\{1, 2, 3, 4\}$

$|\Pi_n| = B(n)$ — количество всевозможных эквивалентностей n-элементном множестве, *число Белла*.

$$B(3) = 5,\ B(4) = 15,\ \ldots,\ B(20) =$$

Решётка всех разбиений множества — беллиан

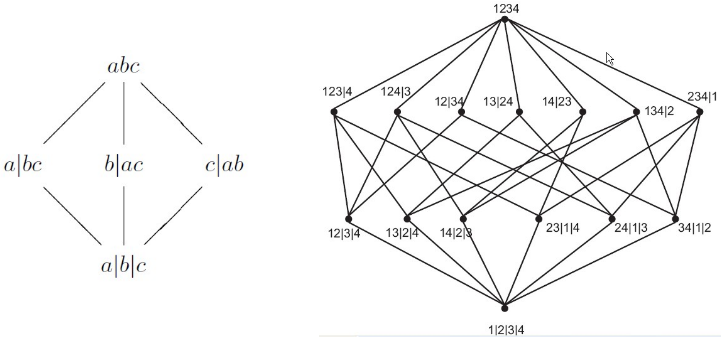


Рис. 10. Беллианы множеств $\{a, b, c\}$ и $\{1, 2, 3, 4\}$

$|\Pi_n| = B(n)$ — количество всевозможных эквивалентностей n-элементном множестве, *число Белла*.

$$B(3) = 5,\ B(4) = 15,\ \ldots,\ B(20) = 51724158235372,\ \ldots.$$

Эквивалентность решёточно упорядоченных множеств и решёток

Теорема

1. *Пусть* $\langle\, P, \leqslant \,\rangle$ *— решёточно упорядоченное множество. Если для любых элементов* x *и* y *из* P *положить*

$$x \sqcup y \stackrel{\text{def}}{=} \sup\{x, y\}, \qquad x \sqcap y \stackrel{\text{def}}{=} \inf\{x, y\},$$

то структура $\langle\, P, \sqcup, \sqcap \,\rangle$ *будет решёткой.*

2. *Пусть* $\langle\, L, \sqcup, \sqcap \,\rangle$ *— решётка. Если для любых элементов* x *и* y *из* L *положить*

$$x \leqslant y \stackrel{\text{def}}{=} x \sqcap y = x \quad (\text{или } x \leqslant y \stackrel{\text{def}}{=} x \sqcup y = y),$$

то структура $\langle\, L, \leqslant \,\rangle$ *будет решёточно упорядоченным множеством.*

Эквивалентность решёточно упорядоченных множеств и решёток...

Теорема устанавливает взаимно-однозначное соответствие между решёточно упорядоченными множествами и решётками: из одной АС всегда можно получить другую.

Поэтому термин «решётка» применяют для обоих понятий: любую решётку можно представить либо как упорядоченное множество, либо как алгебру.

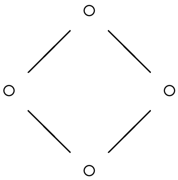
решёточно упорядоченные множества	решётки
$\langle \mathbb{R}, \leqslant \rangle$	$\langle \mathbb{R}, \max, \min \rangle$
$\langle \mathbb{N}, \mid \rangle$	$\langle \mathbb{N}, \vee, \wedge \rangle$
$\langle \mathcal{P}(A), \subseteq \rangle$	$\langle \mathcal{P}(A), \cup, \cap \rangle$

Возможность такого рассмотрения решёток позволяет вводить в них как порядковые, так и алгебраические операции, что приводит к богатой и многообразной в приложениях теории.

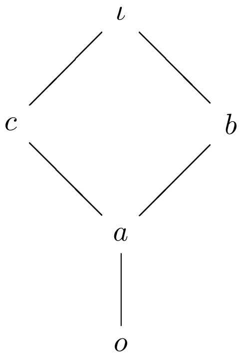
Решётки: примеры

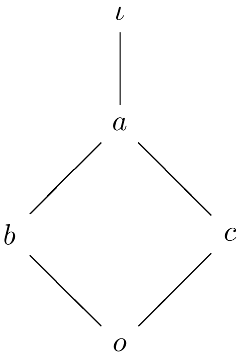
Решётки ($A \neq \varnothing$) —

- все булевы алгебры;
- все цепи;
- единственные 1-, 2-, 3-элементные решётки — цепи $\mathbf{1}$, $\mathbf{2}$, $\mathbf{3}$
- 4-элементные решётки — $\mathbf{4}$ и B^2:

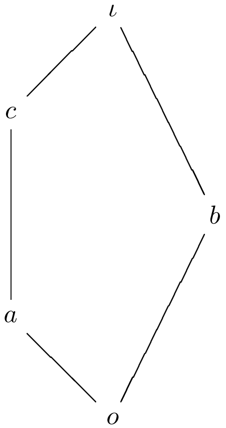


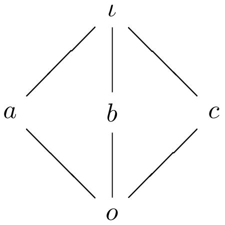
5-элементные решётки —





5-элементные решётки — пятиугольник N_5 и бриллиант M_3





$+$ цепь $\mathbf{5}$

Решётки: универсальные грани и атомы

Наименьший элемент решётки (как р.у.м.) — её *ноль* (o), наибольший — *единица* (ι).
o и ι решётки — её *универсальные грани*.

Решётки: универсальные грани и атомы

Наименьший элемент решётки (как р.у.м.) — её *ноль* (o), наибольший — *единица* (ι).
o и ι решётки — её *универсальные грани*.

Решётка может и не иметь универсальных граней: $\mathbb{Z}$, $\langle \mathbb{N}, | \rangle$ — только $o = 1$.

Решётки: универсальные грани и атомы

Наименьший элемент решётки (как р.у.м.) — её *ноль* (o), наибольший — *единица* (ι).
o и ι решётки — её *универсальные грани*.

Решётка может и не иметь универсальных граней: $\mathbb{Z}$, $\langle \mathbb{N}, | \rangle$ — только $o = 1$.

Все конечные решётки содержат o и ι.

Решётки: универсальные грани и атомы

Наименьший элемент решётки (как р.у.м.) — её *ноль* (o),
наибольший — *единица* (ι).
o и ι решётки — её *универсальные грани*.

Решётка может и не иметь универсальных граней: $\mathbb{Z}$, $\langle \mathbb{N}, | \rangle$ — только $o = 1$.

Все конечные решётки содержат o и ι.

Определение

Элемент $a \neq o$ решётки $\mathbf{L}$ с нулём o называется *атомом* если для любого элемента x этой решётки пересечение $a \sqcap x$ равно либо o, либо a.
В последнем случае говорят, что *элемент x содержит атом a*.

Гомоморфизмы решёток

Определение

Отображение φ решётки $\mathbf{L}$ в решётку $\mathbf{L}'$ называется *алгебраическим* или *решёточным гомоморфизмом*, если для любых $x, y \in \mathbf{L}$ справедливы равенства

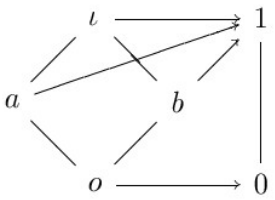
$$\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y) \quad \text{и} \quad \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y).$$

Биективный решёточный гомоморфизм есть *решёточный изоморфизм*. Изоморфизм решётки в себя называется *автоморфизмом*.

Инъективные и сюръективные решёточные гомоморфизмы называют *решёточными* (или *алгебраическими*) *мономорфизмами* (*вложениями*) и *эпиморфизмами* соответственно.

Связь порядкового и решёточного гомоморфизмов решёток

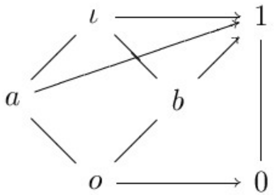
Связь порядкового и решёточного гомоморфизмов решёток



1) Порядковые гомоморфизмы решёток как ч.у. множеств, вообще говоря, не являются алгебраическими.

2) Любое отображение одной решётки на другую, сохраняющее хотя бы одну из решёточных операций, является порядковым гомоморфизмом.

Связь порядкового и решёточного гомоморфизмов решёток



1) Порядковые гомоморфизмы решёток как ч.у. множеств, вообще говоря, не являются алгебраическими.

2) Любое отображение одной решётки на другую, сохраняющее хотя бы одну из решёточных операций, является порядковым гомоморфизмом.

В случае изоморфизма проблемы снимаются.

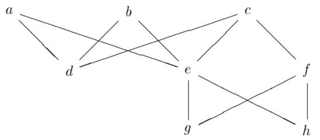
Теорема (об эквивалентности двух видов изоморфизма решёток)

Две решётки алгебраически изоморфны, iff они изоморфны как ч.у. множества.

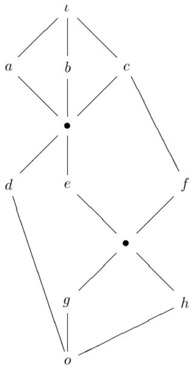
Пополнение произвольного ч.у. множество до (полной) решётки

Теорема (замыкание Макнила)

Всякое ч.у. множество можно вложить в подходящую полную решётку с сохранением всех точных граней.



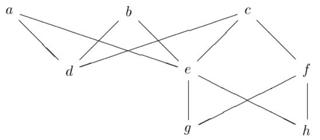
Универсальные грани и элементы, отмеченные знаком • суть сечения Макнила.

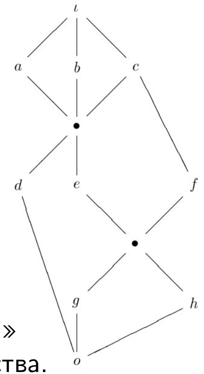


Пополнение произвольного ч.у. множество до (полной) решётки

Теорема (замыкание Макнила)

Всякое ч.у. множество можно вложить в подходящую полную решётку с сохранением всех точных граней.





Универсальные грани и элементы, отмеченные знаком • суть сечения Макнила.

Теорема показывает, что знаменитое построение Р. Дедекиндом действительных чисел «сечениями» на самом деле применимо для любого ч.у. множества.

Идеалы решёток

Определение

Пусть $\langle L, \sqcup, \sqcap \rangle$ — решётка. Непустое подмножество I элементов L называется её *(решёточным) идеалом*, если

$$1)\ (x \in I)\,\&\,(y \leqslant x) \ \Rightarrow\ y \in I \quad \text{и} \quad 2)\ x, y \in I \ \Rightarrow\ x \sqcup y \in I\,.$$

Двойственно, непустое подмножество F элементов L называется её *решёточным фильтром*, если

$$1)\ (x \in F)\,\&\,(x \leqslant y) \ \Rightarrow\ y \in F \quad \text{и} \quad 2)\ x, y \in F \ \Rightarrow\ x \sqcap y \in F\,.$$

Непустое подмножество I оказывается решёточным идеалом, iff для любых её элементов x и y справедлива эквивалентность $x, y \in I \ \Leftrightarrow\ x \sqcup y \in I$ и аналогично для фильтров.

Решётки: теоремы о вложениях

Теорема (о представлении решёток)

Всякая решётка может быть вложена в булеан подходящего множества с сохранением всех точных нижних граней.

Решётки: теоремы о вложениях

Теорема (о представлении решёток)

Всякая решётка может быть вложена в булеан подходящего множества с сохранением всех точных нижних граней.

Теорема (Макнил)

Всякую решётку можно вложить в подходящую полную решётку с сохранением всех точных граней.

Решётки: теоремы о вложениях

Теорема (о представлении решёток)

Всякая решётка может быть вложена в булеан подходящего множества с сохранением всех точных нижних граней.

Теорема (Макнил)

Всякую решётку можно вложить в подходящую полную решётку с сохранением всех точных граней.

Теорема

Всякую конечную решётку можно вложить в конечную решётку разбиений.

Подрешётки

Определение

Непустое подмножество L' решётки $\mathbf{L} = \langle L, \sqcup, \sqcap \rangle$ называется её *подрешёткой* (символически $\mathbf{L}' \leqslant \mathbf{L}$), если $\mathbf{L}'$ устойчиво относительно сужений $\sqcup$ и $\sqcap$.

Подрешётки

Определение

Непустое подмножество L' решётки $\mathbf{L} = \langle L, \sqcup, \sqcap \rangle$ называется её *подрешёткой* (символически $\mathbf{L}' \leqslant \mathbf{L}$), если $\mathbf{L}'$ устойчиво относительно сужений $\sqcup$ и $\sqcap$.

Каждое подмножество решётки L является подрешёткой, iff L — цепь.

Из определения следует, что подмножество элементов решётки $\mathbf{L}$ может быть решёткой относительно наследуемого частичного порядка, но не подрешёткой L.

Подрешётка и не-подрешётка решётки $\mathbf{L} = \mathbf{4} \times \mathbf{4}$

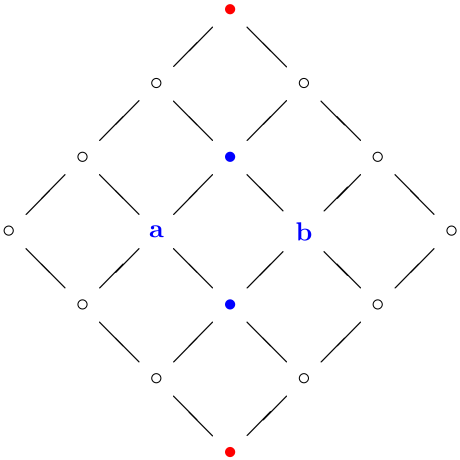


Рис. 11. $\{\mathbf{a}, \mathbf{b}, \bullet, \bullet\} \leqslant \mathbf{4}^2$, но $\{\mathbf{a}, \mathbf{b}, \bullet, \bullet\} \not\leqslant \mathbf{4}^2$

Раздел I

Раздел II

Раздел III

- Линеаризация
- Что надо знать

5 Алгебраические решётки

- Решётки: определение, основные свойства
- Модулярные и дистрибутивные решётки
- Применение теории решёток к задаче классификации
- Что надо знать

Модулярные решётки

Определение

Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *модулярной*, если для любых $x,\ y,\ z \in L$ в ней выполняется следующий *модулярный закон*

$$Mod: x \leqslant y \ \Rightarrow \ x \sqcup (y \sqcap z) \ = \ y \sqcap (x \sqcup z).$$

Модулярные решётки

Определение

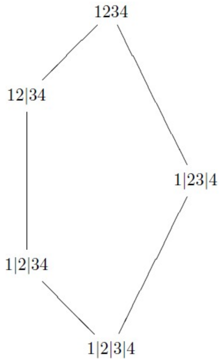
Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *модулярной*, если для любых $x, y, z \in L$ в ней выполняется следующий *модулярный закон*

$$Mod : x \leqslant y \;\Rightarrow\; x \sqcup (y \sqcap z) \;=\; y \sqcap (x \sqcup z).$$

Пример

1. Модулярными являются все цепи, решётка $\langle \mathbb{N}, | \rangle$, булевы алгебры и их подрешётки.
2. Решётка $NSub\,G$ всех нормальных подгрупп группы G образует модулярна (пересечение групп — всегда группа, а объединение нормальных подгрупп совпадает с их произведением).
3. Решётка всех эквивалентностей на данном множестве в общем случае не модулярна.

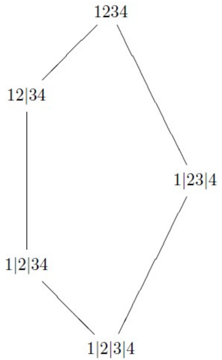
Пятиугольник N_5 — немодулярная решётка



Решётка всех эквивалентностей на данном множестве в общем случае не модулярна.

$$\alpha = (1|23|4),\ \beta = (12|34),\ \gamma = (12|34),\ \alpha \leqslant \gamma$$
$$\alpha \sqcup (\gamma \sqcap \beta) = \alpha \sqcup o = \alpha \neq \gamma \sqcap (\alpha \sqcup \beta) = \gamma \sqcap \iota = \gamma.$$

Пятиугольник N_5 — немодулярная решётка



Решётка всех эквивалентностей на данном множестве в общем случае не модулярна.

$$\alpha = (1|23|4),\ \beta = (12|34),\ \gamma = (12|34),\ \alpha \leqslant \gamma$$
$$\alpha \sqcup (\gamma \sqcap \beta) = \alpha \sqcup o = \alpha \neq \gamma \sqcap (\alpha \sqcup \beta) = \gamma \sqcap \iota = \gamma.$$

Немодулярность N_5 оказывается ключевой:

Теорема (критерий модулярности решётки)

Решётка модулярна, iff никакая её подрешётка не изоморфна пятиугольнику N_5.

Дистрибутивные решётки

Определение

Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *дистрибутивной*, если в ней выполняются дистрибутивные законы

$$\begin{aligned} (x \sqcup y) \sqcap z &= (x \sqcap z) \sqcup (y \sqcap z); \\ (x \sqcap y) \sqcup z &= (x \sqcup z) \sqcap (y \sqcup z). \end{aligned}$$

Дистрибутивные решётки

Определение

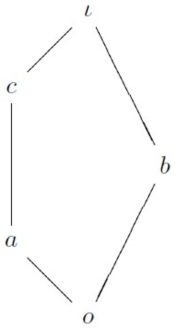
Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *дистрибутивной*, если в ней выполняются дистрибутивные законы

$$(x \sqcup y) \sqcap z \;=\; (x \sqcap z) \sqcup (y \sqcap z);$$
$$(x \sqcap y) \sqcup z \;=\; (x \sqcup z) \sqcap (y \sqcup z).$$

Пример

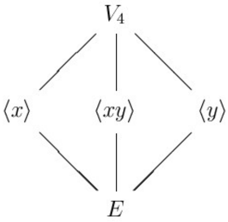
1. Все цепи, булевы алгебры и их подрешётки дистрибутивны.
2. Решётка всех подпространств векторного пространства, упомянутая выше в качестве примера модулярной решётки, не является дистрибутивной.
3. Решётка $\mathrm{Sub}\, C$ всех подгрупп циклической группы C дистрибутивна.

Всякая дистрибутивная решётка модулярна



$$(a \sqcup b) \sqcap c = \iota \sqcap c = c \neq (a \sqcap c) \sqcup (b \sqcap c) = a \sqcup o = a$$

Модулярный закон — ослабленная форма второго дистрибутивного закона



$V_4 = \langle\, e, x, y, xy \,\rangle$ — четверная Клейна, решётка $Sub\, V_4 \cong M_3$ (ромб) подгрупп V_4 (все они нормальны) модулярна, но не дистрибутивна: $a = \langle x \rangle$, $b = \langle y \rangle$, $c = \langle xy \rangle$,

$$(a \sqcup b) \sqcap c = \iota \sqcap c = c \neq (a \sqcap c) \sqcup (b \sqcap c) = o \sqcup o = o.$$

Критерий дистрибутивности решётки

Недистрибутивность M_3, оказывается ключевой: справедлива

Теорема

Модулярная решётка является дистрибутивной, iff никакая её подрешётка не изоморфна ромбу M_3.

Критерий дистрибутивности решётки

Недистрибутивность M_3, оказывается ключевой: справедлива

Теорема

Модулярная решётка является дистрибутивной, iff никакая её подрешётка не изоморфна ромбу M_3.

Следствие (критерий дистрибутивности решётки)

Решётка дистрибутивна, iff никакая её подрешётка не изоморфна ни пятиугольнику N_5, ни ромбу M_3.

Дистрибутивность решётки $J(\mathbf{P})$

Лемма

$J(\mathbf{P}) \leqslant \langle \mathcal{P}(\mathbf{P}), \cup, \cap \rangle \ \Rightarrow$ *решётка $J(\mathbf{P})$ дистрибутивна.*

Дистрибутивность решётки $J(\mathbf{P})$

Лемма

$J(\mathbf{P}) \leqslant \langle \mathcal{P}(\mathbf{P}), \cup, \cap \rangle \Rightarrow$ *решётка $J(\mathbf{P})$ дистрибутивна*.

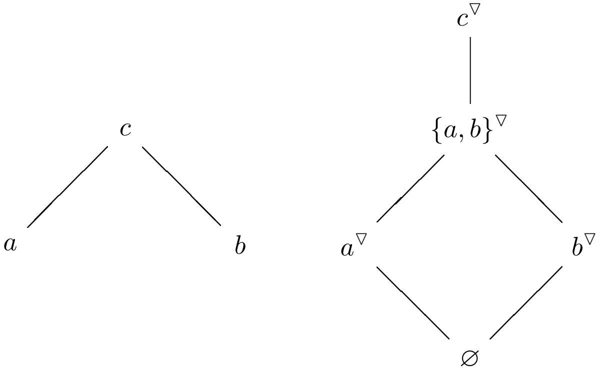


Рис. 12. Z_3, $J(Z_3)$

Неразложимые элементы решёток

В конечных дистрибутивных решётках важную роль играют не атомы (например, в конечной цепи всего один атом), а неразложимые в объединение элементы.

Неразложимые элементы решёток

В конечных дистрибутивных решётках важную роль играют не атомы (например, в конечной цепи всего один атом), а неразложимые в объединение элементы.

Определение

Элемент $z \neq o$ решётки назовём *неразложимым*, если из $z = x \sqcup y$ следует либо $z = x$, либо $z = y$.

Неразложимые элементы решёток

В конечных дистрибутивных решётках важную роль играют не атомы (например, в конечной цепи всего один атом), а неразложимые в объединение элементы.

Определение

Элемент $z \neq o$ решётки назовём *неразложимым*, если из $z = x \sqcup y$ следует либо $z = x$, либо $z = y$.

Пример

1. Атомы любой решётки неразложимы, и в атомной булевой алгебре нет других неразложимых элементов.
2. В решётке $\langle \mathbb{N}, | \rangle$ неразложимы в точности степени простых чисел.
3. В цепи ни один элемент не является разложимым.

Неразложимые элементы решёток...

Лемма

В конечной решётке каждый ненулевой элемент может быть представлен в виде объединения неразложимых элементов.

Неразложимые элементы решёток...

Лемма

В конечной решётке каждый ненулевой элемент может быть представлен в виде объединения неразложимых элементов.

Доказательство

Если элемент b *неразложим, то* $b = b \sqcup b$. *Пусть* $b = b_1 \sqcup b_2$ *и* $b_1 \neq b \neq b_2$.

- *Если и* b_1, *и* b_2 *неразложимы, то лемма доказана.*
- *В противном случае представляем* b_1 *и/или* b_2 *в виде объединения строго содержащихся в них элементов, и т.д. В силу конечности решётки указанный процесс закончится, и исходный элемент* b *будет представлен в виде объединения неразложимых элементов.*

Представление произвольных элементов решётки через неразложимые

Обозначения для подмножеств элементов (дистрибутивной) решётки L

- $\operatorname{Irr} \mathbf{L}$ — множество неразложимых в объединение элементов $\mathbf{L}$;
- $\operatorname{Irr}(x) = \{\, y \in \operatorname{Irr} \mathbf{L} \mid y \leqslant x \,\}$ — множество неразложимых элементов $\mathbf{L}$, содержащихся в x.

Представление произвольных элементов решётки через неразложимые

Обозначения для подмножеств элементов (дистрибутивной) решётки $\mathbf{L}$

- $\operatorname{Irr} \mathbf{L}$ — множество неразложимых в объединение элементов $\mathbf{L}$;
- $\operatorname{Irr}(x) = \{ y \in \operatorname{Irr} \mathbf{L} \mid y \leqslant x \}$ — множество неразложимых элементов $\mathbf{L}$, содержащихся в x.

Доказанная лемма утверждает, что в конечной решётке каждый ненулевой элемент x допускает представление:

$$x = \bigsqcup_{a \in \operatorname{Irr}(x)} a.$$

Изоморфизм ч.у. множества и неразложимых элементов решётки его порядковых идеалов

Лемма

Если $\mathbf{P}$ — *ч.у. множество, то* $\mathrm{Irr}\, J(\mathbf{P}) \cong \mathbf{P}$.

Изоморфизм ч.у. множества и неразложимых элементов решётки его порядковых идеалов

Лемма

Если $\mathbf{P}$ *— ч.у. множество, то* $\mathrm{Irr}\ J(\mathbf{P}) \cong \mathbf{P}$.

Доказательство

Пусть $\mathbf{P}$ *— ч.у. множество и тогда* $J(\mathbf{P})$ *— дистрибутивная решётка его порядковых идеалов. Порядковый идеал решётки неразложим, iff он является главным:* $x^{\nabla} \Rightarrow \mathrm{Irr}\ J(\mathbf{P}) \cong J_0(\mathbf{P}) = \{\, x^{\nabla} \mid x \in P \,\}$.

Ранее был установлен изоморфизм между ч.у. множеством и совокупностью его главных идеалов:

$$\varphi : P \to J(P), \quad \varphi(x) = x^{\nabla},$$

поэтому $P \cong J_0(P) = \mathrm{Irr}\ J(P)$.

$\mathrm{Irr}\ J(\mathbf{P}) \cong \mathbf{P}$: пример

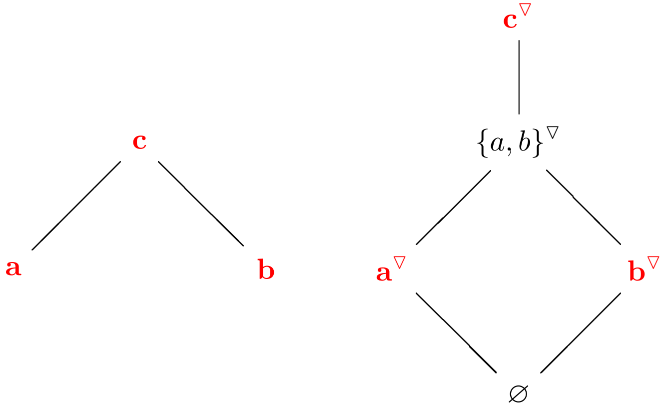


Рис. 13. Z_3, множество $Irr\,J(Z_3)$ выделено

Фундаментальная теорема о конечных дистрибутивных решётках

Теорема (ФТКДР, *Г. Биркгоф*)

Всякая конечная дистрибутивная решётка $\mathbf{L}$ *изоморфна решётке порядковых идеалов ч.у. множества её неразложимых элементов:* $\mathbf{L} = J(Irr\,\mathbf{L})$

Фундаментальная теорема о конечных дистрибутивных решётках

Теорема (ФТКДР, *Г. Биркгоф*)

Всякая конечная дистрибутивная решётка $\mathbf{L}$ *изоморфна решётке порядковых идеалов ч.у. множества её неразложимых элементов:* $\mathbf{L} = J(Irr\,\mathbf{L})$

Доказательство (набросок)

Пусть $\mathbf{L} = \langle L, \sqcup, \sqcap \rangle$ *— конечная дистрибутивная решётка и* $J(\mathrm{Irr}\ \mathbf{L})$ *— решётка порядковых идеалов ч.у. множества* $\mathrm{Irr}\ \mathbf{L}$*.*
Рассмотрим отображение $\psi : L \to J(\mathrm{Irr}\ \mathbf{L})\,, \quad \psi(x) = \mathrm{Irr}(x)$.

- *Отображение* ψ *есть биекция.*
- $x \leqslant y \ \Leftrightarrow\ \mathrm{Irr}(x) \subseteq \mathrm{Irr}(y) \ \Leftrightarrow\ \psi(x) \subseteq \psi(y)$.

$\therefore\ \psi$ *— (порядковый) изоморфизм между* $\mathbf{L}$ *и* $J(\mathrm{Irr}\ \mathbf{L})$.

ФТКДР $\mathbf{L} = J(Irr\,\mathbf{L})$: иллюстрация

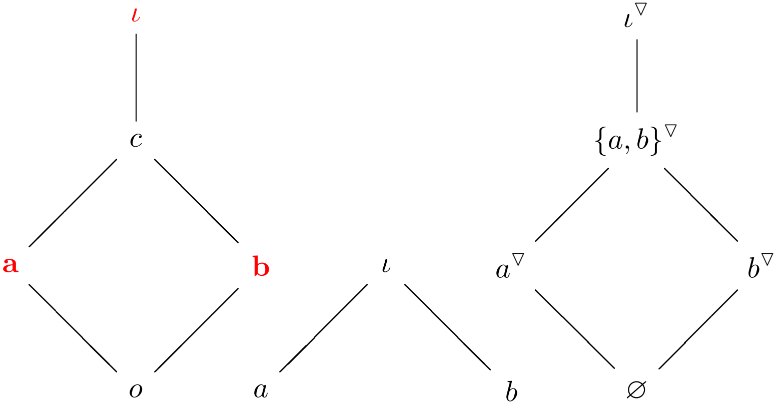


Рис. 14. $\mathbf{L}$ $\quad$ $Irr\,\mathbf{L}$ $\quad$ $J(Irr\,\mathbf{L})$

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

- Коды БЧХ
- Задачи
- Что надо знать

3 Теория перечисления Пойа

- Действие группы на множестве
- Применение леммы Бёрнсайда для решения комбинаторных задач
- Применение теоремы Пойа для решения комбинаторных задач
- Что надо знать

4 Некоторые вопросы теории частично упорядоченных множеств

- Основные понятия теории ч.у. множеств
- Операции над ч.у. множествами

Раздел III

- Линеаризация
- Что надо знать

5. **Алгебраические решётки**
   - Решётки: определение, основные свойства
   - Модулярные и дистрибутивные решётки
   - Применение теории решёток к задаче классификации
   - Что надо знать

Классификация по прецедентам: постановка задачи

Классификация по прецедентам: постановка задачи

1. Множество объектов $\mathcal{X}$ разделено на несколько подмножеств (*классов*).

Классификация по прецедентам: постановка задачи

1. Множество объектов $\mathcal{X}$ разделено на несколько подмножеств (*классов*).
2. Информация о таком разбиении содержится только в указании о принадлежности к данным классам элементов конечной *обучающей последовательности* (*выборки*) из $\mathcal{X}$, элементы которой называют *прецедентами*.

Классификация по прецедентам: постановка задачи

1. Множество объектов $\mathcal{X}$ разделено на несколько подмножеств (*классов*).
2. Информация о таком разбиении содержится только в указании о принадлежности к данным классам элементов конечной *обучающей последовательности* (*выборки*) из $\mathcal{X}$, элементы которой называют *прецедентами*.
3. Объекты имеют описание на некотором формальном языке, указывающем степень обладания объектами конечным числом признаков из множества $M = \{x_1, \ldots, x_n\}$.

Классификация: пространство объектов

прецедент	класс
Объект 1	A
Объект 2	B
...	...
Объект L	A
Объект X	?

- Поиск полезных ископаемых
- Медицинская диагностика
- Прогнозирование
- ...

Рис. 15. Информационная модель классификации

Классификация: признаковая матрица

Часто используется описание в виде *объектно-признаковой* $(0,1)$-*матрицы* $\mathcal{M}$, в которой объектам соответствуют строки, признакам — столбцы, а элементы матрицы кодируют наличие/отсутствие признаков у объектов.

Класс K_i	x_1	x_2	$\dots$	x_n
Объект 1	1	0	$\dots$	1
Объект 2	0	1	$\dots$	1
Объект 3	1	1	$\dots$	0
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
Объект m_i	0	1	$\dots$	0

— для каждого из классов $K_1, \dots, K_s$, $s \geqslant 2$. Далее $s = 2$.

Классификация: язык описания и решающее правило

Задача обучения

По матрице $\mathcal{M}$ сформулировать *решающее правило*, которое по описанию нового объекта из $\mathcal{X}$ указывало бы имя класса, его содержащего.

Классификация: язык описания и решающее правило

Задача обучения

По матрице $\mathcal{M}$ сформулировать *решающее правило*, которое по описанию нового объекта из $\mathcal{X}$ указывало бы имя класса, его содержащего.

Решающее правило должно максимизировать некоторой функционал, определяющей *качество классификации*.

Классификация: язык описания и решающее правило

Задача обучения

По матрице $\mathcal{M}$ сформулировать *решающее правило*, которое по описанию нового объекта из $\mathcal{X}$ указывало бы имя класса, его содержащего.

Решающее правило должно максимизировать некоторой функционал, определяющей *качество классификации*.

Таким функционалом в подавляющем числе случаев является минимум (не абсолютный!) числа ошибок классификации, однако может также учитываться, например, и доля отказов.

Классификация: подходы к решению задачи

- метрические методы (*NN*, ...);
- разделяющие поверхности (*SVM*, ...);
- потенциальные функции;
- логические методы;
- коллективные решающие правила (*области компетенции, голосование, алгебраический подход*);
- структурные методы;
- ...
- реляционный подход (***АФП (FCA)***, ...)

Классификация: подходы к решению задачи

- метрические методы (*NN*, ...);
- разделяющие поверхности (*SVM*, ...);
- потенциальные функции;
- логические методы;
- коллективные решающие правила (*области компетенции, голосование, алгебраический подход*);
- структурные методы;
- ...
- реляционный подход (***АФП (FCA)***, ...)

Wille R., Ganter B. Formal concept analysis. Berlin; Heidelberg; New York: Springer-Verl., 1999.

Соответствия Галуа: определение

Далее запись отображений:

$\boxed{f(a)}$ записывается как $\boxed{af}$,

$\boxed{f(A)}$ записывается как $\boxed{fA}$.

Соответствия Галуа: определение

Далее запись отображений:
$\boxed{f(a)}$ записывается как $\boxed{af}$,
$\boxed{f(A)}$ записывается как $\boxed{fA}$.

Определение

Пусть $\mathbf{P}$ и $\mathbf{Q}$ — ч.у. множества. Пара отображений (φ, ψ), $\varphi : \mathbf{P} \to \mathbf{Q}$, $\psi : \mathbf{Q} \to \mathbf{P}$, удовлетворяющая свойствам

1. φ и ψ антиизотонны;
2. $x\varphi\psi \geqslant p$ и $y\psi\varphi \geqslant q$ ($\varphi\psi$ и $\psi\varphi$ — *операторы замыкания* (на $\mathbf{P}$ и $\mathbf{Q}$ соответственно).

называется *соответствием Галуа* между $\mathbf{P}$ и $\mathbf{Q}$.

Справедливы и более сильные соотношения

$$p \leqslant q\psi \Leftrightarrow q \leqslant p\varphi \quad \text{и} \quad \varphi = \varphi\psi\varphi,\ \psi = \psi\varphi\psi\,.$$

Понятие: философское отступление...

Понятие — это ...

... целостная совокупность суждений, утверждающих об отличительных признаках вещи

Понятие: философское отступление...

Понятие — это ...

... целостная совокупность суждений, утверждающих об отличительных признаках вещи

Примеры:

искусство, наука, ...

Понятие: философское отступление...

Понятие — это ...

... целостная совокупность суждений, утверждающих об отличительных признаках вещи

Примеры:

искусство, наука, ...

Объём понятия — это ...

... *совокупность всех вещей*, обладающих зафиксированными в данном понятии признаками

Понятие: философское отступление...

Понятие — это ...

... целостная совокупность суждений, утверждающих об отличительных признаках вещи

Примеры:

искусство, *наука*, ...

Объём понятия — это ...

... *совокупность всех вещей*, обладающих зафиксированными в данном понятии признаками

Примеры:

искусство: *литература*, *живопись*, *архитектура*,...

наука: *биология*, *физика*, *химия*...

Понятие: философское отступление...

Понятие — это ...

... целостная совокупность суждений, утверждающих об отличительных признаках вещи

Примеры:

искусство, *наука*, ...

Объём понятия — это ...

... *совокупность всех вещей*, обладающих зафиксированными в данном понятии признаками

Примеры:

искусство: *литература*, *живопись*, *архитектура*,...
наука: *биология*, *физика*, *химия*...

Понятие: философское отступление...

Содержание понятия — это ...

... *совокупность свойств*, присущих всем объектам данного понятия

Понятие: философское отступление...

Содержание понятия — это ...

... *совокупность свойств*, присущих всем объектам данного понятия

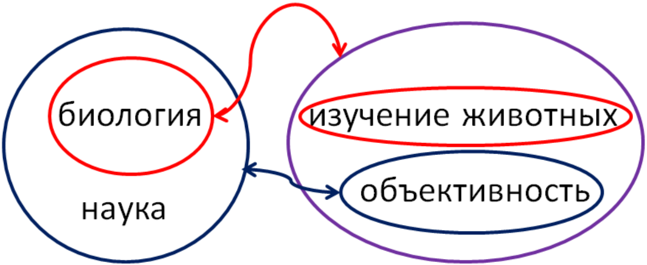
Примеры:

искусство: *результат отражения действительности в форме чувственных образов, создание выразительных форм, ...*

наука: *познавательная деятельность, объективность, систематичность, ...*

Закон обратного отношения между содержанием и объёмом понятия:

Большее по объёму понятие имеет меньшее содержание



Антимонотонность соответствий Галуа отражает этот закон

Классификация: положительные и отрицательные примеры

Рассматриваются задачи, в которых множество $\mathcal{X}$ разбито на два непересекающихся класса:
$\mathcal{X}^+$ (*положительный*) и
$\mathcal{X}^-$ (*отрицательный*)
относительно обладания/необладания их объектами некоторым целевым признаком $z \notin M$.

Прецеденты из данных классов называются, соответственно, *положительными* и *отрицательными примерами*.

Имеем 2 класса и $z = "x \in \mathcal{X}^+"$

АФП: формальный контекст

Пусть G и M — множества, называемые соответственно *множествами объектов* и *признаков*, а I — соответствие между G и M *отношением инцидентности*.

gIm означает, что объект $g \in G$ обладает признаком $m \in M$.

Определение

Тройка $K = (G, M, I)$ называется *формальным контекстом*.

В конечном случае контекст может быть задан в виде объектно-признаковой $(0, 1)$-матрицы.

Соответствия Галуа в АФП и нотация

Утверждение

Если для произвольных $A \subseteq G$ и $B \subseteq M$ ввести отображения $\varphi : 2^G \to 2^M$ и $\psi : 2^M \to 2^G$ такие, что

$$A\varphi = \{ m \subseteq M \mid \forall g \in A\,(gIm) \} = A',$$
$$B\psi = \{ g \subseteq G \mid \forall m \in B\,(gIm) \} = B',$$

то пара отображений (φ, ψ) является соответствием Галуа между ч.у. множествами 2^G и 2^M, упорядоченными по включению.

Формальные объём и содержание

Определение

Пусть дан контекст $K = (G, M, I)$. Пара подмножеств (A, B), где $A \subseteq G$, а $B \subseteq M$, и таких, что $A' = B$ и $B' = A$, называется *формальным понятием* данного контекста с *формальным объёмом* A и *формальным содержанием* B.

Если контекст K представлен в виде объектно-признаковой $(0, 1)$-матрицы, то формальному понятию соответствует максимальная её подматрица, заполненная единицами.

Формальные объём и содержание — замкнутые, соответственно, относительно $\varphi\psi$ и $\psi\varphi$ множества.

Решётка формальных понятий

Теорема (основная АФП)

Множество всех формальных понятий данного контекста K образует полную решётку, обозначаемую $\mathfrak{B}(K)$, относительно операций $\vee$ (объединение) и $\wedge$ (пересечение):

$$(A_1, B_1) \vee (A_2, B_2) = \left((B_1 \cap B_2)', B_1 \cap B_2 \right),$$
$$(A_1, B_1) \wedge (A_2, B_2) = \left(A_1 \cap A_2, (A_1 \cap A_2)' \right)$$

и называемую решёткой формальных понятий.

Решётка формальных понятий

Теорема (основная АФП)

Множество всех формальных понятий данного контекста K образует полную решётку, обозначаемую $\mathfrak{B}(K)$, относительно операций $\vee$ (объединение) и $\wedge$ (пересечение):

$$(A_1, B_1) \vee (A_2, B_2) = \left((B_1 \cap B_2)', B_1 \cap B_2 \right),$$
$$(A_1, B_1) \wedge (A_2, B_2) = \left(A_1 \cap A_2, (A_1 \cap A_2)' \right)$$

и называемую решёткой формальных понятий.

$$(A_1,\, B_1) \leqslant (A_2,\, B_2) \Leftrightarrow A_1 \leqslant A_2 \Leftrightarrow B_1 \geqslant B_2$$

Решётка формальных понятий

Теорема (основная АФП)

Множество всех формальных понятий данного контекста K образует полную решётку, обозначаемую $\mathfrak{B}(K)$, относительно операций $\vee$ (объединение) и $\wedge$ (пересечение):

$$(A_1, B_1) \vee (A_2, B_2) = \big((B_1 \cap B_2)', B_1 \cap B_2 \big),$$
$$(A_1, B_1) \wedge (A_2, B_2) = \big(A_1 \cap A_2, (A_1 \cap A_2)' \big)$$

и называемую решёткой формальных понятий.

$$(A_1,\, B_1) \leqslant (A_2,\, B_2) \Leftrightarrow A_1 \leqslant A_2 \Leftrightarrow B_1 \geqslant B_2$$

У решётки $\mathfrak{B}(K)$ формального контекста $K = (G, M, I)$:

единица ι — формальное понятие $(G,\, G')$;
атомы — формальные понятия вида $(g,\, g')$;
нуль o — формальное понятие $(\varnothing,\, M)$ с пустым объёмом.

Два контекста: объём и содержание

Данные для обучения классификации описываются положительным $K_+ = (G_+, M, I_+)$ и отрицательным $K_- = (G_-, M, I_-)$ контекстами.

Операторы Галуа в этих контекстах обозначаются соответствующими верхними индексами: A^+, A^-, B^+ и т.д.

Определение

Формальное понятие $(A_+, B_+) \in K_+$ называется *положительным*.
A_+ — *положительный формальный объём*,
B_+ — *положительное формальное содержание*.

Аналогично определяются отрицательные формальные объём и содержание для контекста K_-.

Гипотезы

Определение

Положительное формальное содержание B_+ положительного понятия (A_+, B_+) называется:

Гипотезы

Определение

Положительное формальное содержание B_+ положительного понятия (A_+, B_+) называется:

- *положительной (+) предгипотезой*, если $\forall (A_-, B_-) \in K_- \ (B_+ \neq B_-)$, т. е. оно не является формальным содержанием ни одного отрицательного понятия;

Гипотезы

Определение

Положительное формальное содержание B_+ положительного понятия (A_+, B_+) называется:

- *положительной (+) предгипотезой*, если $\forall (A_-, B_-) \in K_-$ $(B_+ \neq B_-)$, т. е. оно не является формальным содержанием ни одного отрицательного понятия;
- *положительной (+) гипотезой*, если $\forall (g, g^-) \in K_-$ $(B_+ \not\subseteq g^-)$, т. е. оно не является подмножеством содержания понятия какого-либо отрицательного примера g;

Гипотезы

Определение

Положительное формальное содержание B_+ положительного понятия (A_+, B_+) называется:

- *положительной (+) предгипотезой*, если $\forall (A_-, B_-) \in K_-\ (B_+ \neq B_-)$, т. е. оно не является формальным содержанием ни одного отрицательного понятия;
- *положительной (+) гипотезой*, если $\forall (g, g^-) \in K_-\ (B_+ \not\subseteq g^-)$, т. е. оно не является подмножеством содержания понятия какого-либо отрицательного примера g;
- *фальсифицированной положительной (+) гипотезой*, если $\exists (g, g^-) \in K_-\ (B_+ \subseteq g^-)$.

Гипотезы

Определение

Положительное формальное содержание B_+ положительного понятия (A_+, B_+) называется:

- *положительной (+) предгипотезой*, если $\forall (A_-, B_-) \in K_-\ (B_+ \neq B_-)$, т. е. оно не является формальным содержанием ни одного отрицательного понятия;
- *положительной (+) гипотезой*, если $\forall (g, g^-) \in K_-\ (B_+ \not\subseteq g^-)$, т. е. оно не является подмножеством содержания понятия какого-либо отрицательного примера g;
- *фальсифицированной положительной (+) гипотезой*, если $\exists (g, g^-) \in K_-\ (B_+ \subseteq g^-)$.

Отрицательные $(-)$ предгипотезы, гипотезы, фальсифицированные гипотезы определяются аналогично.

Гипотеза является также и предгипотезой.

Классификация с помощью гипотез

Гипотезы используются для классификации новых объектов.

Классификация с помощью гипотез

Гипотезы используются для классификации новых объектов.

Простейшее решающее правило

Пусть $g \notin \{G_+ \cup G_-\}$ — новый неопределённый объект.

Классификация с помощью гипотез

Гипотезы используются для классификации новых объектов.

Простейшее решающее правило

Пусть $g \notin \{G_+ \cup G_-\}$ — новый неопределённый объект.
Если его формальное содержаниеg' содержит хотя бы одну

- $+$-гипотезу и не содержит ни одной отрицательной гипотезы, то он относится к положительному классу;
- $-$-гипотезу и не содержит ни одной положительной гипотезы, то он относится к отрицательному классу.

Классификация с помощью гипотез

Гипотезы используются для классификации новых объектов.

Простейшее решающее правило

Пусть $g \notin \{G_+ \cup G_-\}$ — новый неопределённый объект.
Если его формальное содержаниеg' содержит хотя бы одну

- $+$-гипотезу и не содержит ни одной отрицательной гипотезы, то он относится к положительному классу;
- $-$-гипотезу и не содержит ни одной положительной гипотезы, то он относится к отрицательному классу.

Отказ от классификации происходит, если g':

- либо не содержит никаких гипотез (недостаток данных);
- либо содержит как положительные, так и отрицательные гипотезы (противоречие в данных).

Многозначные контексты

В АФП предполагается двоичной информации о признаках.

Для её получения из количественных и качественных признаков используется процедура шкалирования.

Многозначный контекст — это четвёрка (G, M, Z, I), где

- G, M, Z — множества объектов, признаков и значений признаков соответственно,
- I — тернарное отношение $I \subseteq G \times M \times Z$, задающее значение $z \in Z$ признака $m \in M$ объекта $g \in G$,

причем отображение $G \times M \to Z$ функционально.

Многозначные контексты

В АФП предполагается двоичной информации о признаках.

Для её получения из количественных и качественных признаков используется процедура шкалирования.

Многозначный контекст — это четвёрка (G, M, Z, I), где

- G, M, Z — множества объектов, признаков и значений признаков соответственно,
- I — тернарное отношение $I \subseteq G \times M \times Z$, задающее значение $z \in Z$ признака $m \in M$ объекта $g \in G$,

причем отображение $G \times M \to Z$ функционально.

Шкалирование — это представление многозначных контекстов двузначными

Пример «Фрукты»: постановка задачи

Задача:

построить классификатор по целевому свойству z = *«являться фруктом»* и следующей объектно-признаковой таблице положительных и отрицательных примеров:

№	G \ M	цвет	жёсткий	гладкий	форма	фрукт
1	**яблоко**	жёлтое	нет	да	круглое	+
2	**грейпфрут**	жёлтый	нет	нет	круглый	+
3	**киви**	зелёное	нет	нет	овальное	+
4	**слива**	синяя	нет	да	овальная	+
5	**кубик**	зелёный	да	да	кубический	−
6	**яйцо**	белое	да	да	овальное	−
7	**теннисный мяч**	белый	нет	нет	круглый	−

Пример «Фрукты»: результат шкалирования

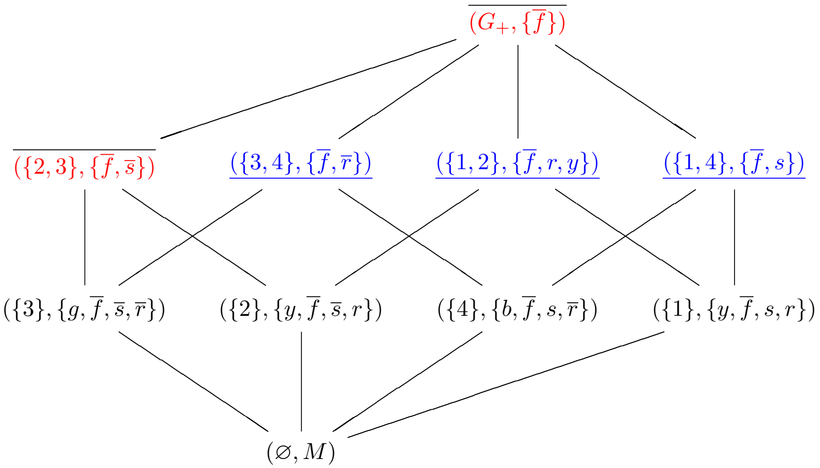
G \ M	w	y	g	b	f	$\bar{f}$	s	$\bar{s}$	r	$\bar{r}$	фрукт
1		×				×	×		×		+
2		×				×		×	×		+
3			×			×		×		×	+
4				×		×	×			×	+
5			×		×		×			×	−
6	×				×		×			×	−
7	×					×		×	×		−

$G_+ = \{1, 2, 3, 4\}$, $G_- = \{5, 6, 7\}$ $\Rightarrow$ отношение I_+ представлено верхней частью таблицы, а отношение I_- — нижней.

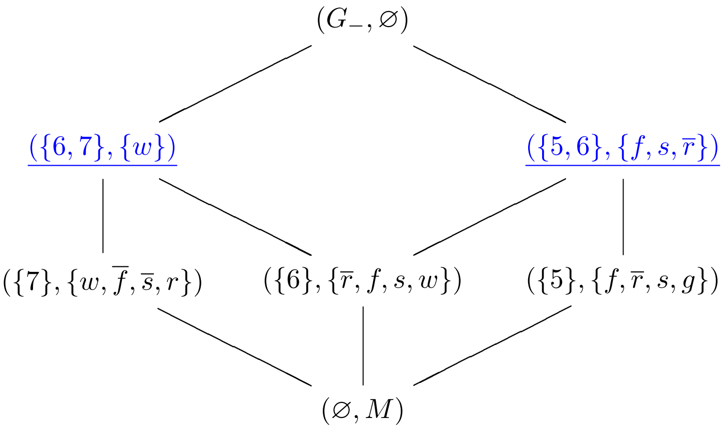
Признаки означают:

w — *белый*, y — *жёлтый*, g — *зелёный*, b — *синий*;
f — *твёрдый*, $\overline{f}$ — *мягкий*, s — *гладкий*, $\overline{s}$ — *шероховатый*;
r — *круглый*, $\overline{r}$ — *некруглый*.

Пример «Фрукты»: решётка $\mathfrak{B}(K_+)$ положительного контекста



Пример «Фрукты»: решётка $\mathfrak{B}(K_-)$ отрицательного контекста



Пример «Фрукты»: формирование гипотез

Формальные содержания

- $\{\overline{f}, \overline{r}\}$ (*мягкий, некруглый*),
  $\{\overline{f}, r, y\}$ (*мягкий, круглый, жёлтый*) и
  $\{\overline{f}, s\}$ (*мягкий, гладкий*) являются $+$-гипотезами;

Пример «Фрукты»: формирование гипотез

Формальные содержания

- $\{\overline{f}, \overline{r}\}$ (*мягкий, некруглый*),
  $\{\overline{f}, r, y\}$ (*мягкий, круглый, жёлтый*) и
  $\{\overline{f}, s\}$ (*мягкий, гладкий*) являются $+$-гипотезами;
- $\{\overline{f}, \overline{s}\}$ (*мягкий, шероховатый*) является фальсифицированной $+$-гипотезой, т.к. она — часть содержания $\{w, \overline{f}, \overline{s}, r\}$ отрицательного примера 7 (теннисный мяч);

Пример «Фрукты»: формирование гипотез

Формальные содержания

- $\{\overline{f}, \overline{r}\}$ (*мягкий, некруглый*),

  $\{\overline{f}, r, y\}$ (*мягкий, круглый, жёлтый*) и

  $\{\overline{f}, s\}$ (*мягкий, гладкий*) являются $+$-гипотезами;

- $\{\overline{f}, \overline{s}\}$ (*мягкий, шероховатый*) является фальсифицированной $+$-гипотезой, т.к. она — часть содержания $\{w, \overline{f}, \overline{s}, r\}$ отрицательного примера 7 (теннисный мяч);

- $\{w\}$ (*белый*) и

  $\{f, s, \overline{r}\}$ (*твёрдый, гладкий, некруглый*) являются $-$-гипотезами.

Пример «Фрукты»: классификация

Неопределённый объект g

- ***мирабель*** будет классифицирован как *фрукт*, т.к. его формальное содержание *жёлтый*, *мягкий*, *гладкий* ($\{y, \overline{f}, s\}$) содержит положительную гипотезу $\{\overline{f}, s\}$ и не содержит ни одной из отрицательн гипотез;

Пример «Фрукты»: классификация

Неопределённый объект g

- ***мирабель*** будет классифицирован как *фрукт*, т.к. его формальное содержание *жёлтый, мягкий, гладкий* $(\{y, \overline{f}, s\})$ содержит положительную гипотезу $\{\overline{f}, s\}$ и не содержит ни одной из отрицательных гипотез;
- ***кусок сахара*** со свойствам *белый, некруглый, твёрдый* будет классифицирован как *не-фрукт*;

Пример «Фрукты»: классификация

Неопределённый объект g

- ***мирабель*** будет классифицирован как *фрукт*, т.к. его формальное содержание *жёлтый, мягкий, гладкий* ($\{y, \overline{f}, s\}$) содержит положительную гипотезу $\{\overline{f}, s\}$ и не содержит ни одной из отрицательн гипотез;
- ***кусок сахара*** со свойствам *белый, некруглый, твёрдый* будет классифицирован как *не-фрукт*;
- ***брикет пломбира*** со свойствами *белый, мягкий, некруглый* вызовет отказ от классификации, поскольку $g^\tau = \{w, \overline{f}, \overline{r}\}$ содержит как положительную гипотезу $\{\overline{f}, \overline{r}\}$, так и отрицательную гипотезу $\{w\}$.

Пример «Фрукты»: дополнение

Если считать, что теннисный мяч — зелёный, то $\mathfrak{B}(K_{-})$:

$$\begin{tikzcd}[column sep=small]
 & (G_{-}, \varnothing) \arrow[dl, no head] \arrow[dr, no head] & \\
\color{red}{\overline{(\{5,7\},\{g\})}} \arrow[d, no head] \arrow[dr, no head] & & \color{blue}{\underline{(\{5,6\},\{f,s,\overline{r}\})}} \arrow[dl, no head] \arrow[d, no head] \\
(\{7\},\{g,\overline{f},\overline{s},r\}) \arrow[dr, no head] & (\{5\},\{\overline{r},f,s,g\}) \arrow[d, no head] & (\{6\},\{f,\overline{r},s,w\}) \arrow[dl, no head] \\
 & (\varnothing, M) &
\end{tikzcd}$$

Пример «Фрукты»: дополнение...

При таком изменении свойств объекта № 7 изменятся только отрицательный контекст.

Теперь

- $\{g\} = \{5, 7\}'$ является фальсифицированной —-гипотезой, поскольку она содержится в формальном содержании $\{g, \overline{f}, \overline{s}, \overline{r}\}$ положительного понятия $\{3\}$.
- $\{f, s, \overline{r}\} = \{5, 6\}'$ является —-гипотезой.

Пример «Фрукты»: дополнение...

При таком изменении свойств объекта № 7 изменятся только отрицательный контекст.

Теперь

- $\{g\} = \{5,7\}'$ является фальсифицированной —-гипотезой, поскольку она содержится в формальном содержании $\{g, \overline{f}, \overline{s}, \overline{r}\}$ положительного понятия $\{3\}$.
- $\{f, s, \overline{r}\} = \{5,6\}'$ является —-гипотезой.

Поэтому

- объекты со свойствами *жёлтый, мягкий, гладкий* и *белый, мягкий, некруглый* будет классифицированы как *фрукт*;
- на объекте с единственным свойством *белый* произойдёт отказ от классификации.

Раздел I

1. Конечные поля или поля Галуа
   - Поля вычетов по модулю простого числа
   - Вычисление элементов в конечных полях
   - Линейная алгебра над конечным полем
   - Корни многочленов над конечным полем
   - Существование и единственность поля Галуа из p^n элементов
   - Циклические подпространства
   - Задачи
   - Что надо знать
2. Коды, исправляющие ошибки
   - Основная задача теории кодирования
   - Циклические коды

Раздел II

Раздел III

- Линеаризация
- Что надо знать

5 Алгебраические решётки

- Решётки: определение, основные свойства
- Модулярные и дистрибутивные решётки
- Применение теории решёток к задаче классификации
- Что надо знать

- Решёточно упорядоченное множество, алгебраические решётки и их эквивалентность. Примеры.
- Гомоморфизмы решёток, связь порядкового и решёточного гомоморфизмов. Сечения Макнила.
- Идеалы решёток. Модулярные и дистрибутивные решётки. Критерии модулярности и дистрибутивности решётки.
- Неразложимые элементы решёток и представление произвольных элементов решётки через неразложимые. Изоморфизм ч.у. множества и неразложимых элементов решётки его порядковых идеалов.
- Фундаментальная теорема о конечных дистрибутивных решётках.
- Задача классификация по прецедентам. Закон обратного отношения между содержанием и объёмом понятия. Соответствия Галуа.

- Анализ формальных понятий (АФП). Формальные объём и содержание. Решётка формальных понятий.
- Гипотезы АФП. Простейшее решающее правило классификации.

Лекции по курсу «Прикладная алгебра» для III потока ф-та ВМК МГУ ЗАВЕРШЁНЫ

Лекции по курсу «Прикладная алгебра» для III потока ф-та ВМК МГУ ЗАВЕРШЁНЫ

До встречи на экзамене!