Прикладная алгебра

Лекции для групп 320–328 (III поток)
5-й семестр 2013/2014 уч. года

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.


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

Раздел I

Раздел II

- Коды БЧХ
- Что надо знать

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 = порядок аддитивной группы поля $\Bbbk$ =

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

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

Примеры: $\mathbb{Q}$, $\mathbb{R}$.

Может ли бесконечное поле иметь положительную характеристику?

Может ли бесконечное поле иметь положительную характеристику?

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

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

Может ли бесконечное поле иметь положительную характеристику?

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

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

Может ли бесконечное поле иметь положительную характеристику?

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

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

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

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

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

   Сложение — дроби можно приводить к общему знаменателю и складывать:

$$P/Q + U/V = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV).$$

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

Может ли бесконечное поле иметь положительную характеристику?

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

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

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

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

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

   Сложение — дроби можно приводить к общему знаменателю и складывать:

$$P/Q + U/V = (PV)/(QV) + (QU)/(QV) = (PV + QU)/(QV).$$

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

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

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 $\mathbb{F}_p$

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

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

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

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.*

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

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

Утверждение

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

Функция Эйлера

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

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

Функция Эйлера

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

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

Свойства:

- $\varphi(n) \leqslant n - 1$ 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

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

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

Неприводимые многочлены

Утверждение

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

Теорема

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

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

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

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

Свойства корней многочленов

Утверждение

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

Свойства корней многочленов

Утверждение

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

Доказательство

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

Основная теорема алгебры

Лемма

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

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

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

Теорема (основная теорема алгебры)

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

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

Неприводимые многочлены:

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

Неприводимые многочлены:

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

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

Неприводимые многочлены:

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

в поле $\mathbb{R}$ —

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

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

Неприводимые многочлены:

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

в поле $\mathbb{R}$ —

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

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

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

Теорема (критерий Эйзенштейна)

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

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

Теорема (критерий Эйзенштейна)

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

Пример

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

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

Теорема (критерий Эйзенштейна)

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

Пример

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

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

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

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

Пример ($p = 2$)

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

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

Пример ($p = 2$)

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

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$.
Ищем неприводимый многочлен в виде $x^2 + ax + 1$.

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

Пример ($p = 2$)

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

Вторая степень: $x^2 + ax + b$

Ясно, что $b = 1$, иначе $x^2 + ax = x(x + a)$.
Ищем неприводимый многочлен в виде $x^2 + ax + 1$.
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

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

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:

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

Какие из них неприводимы?

Неприводимые многочлены над $\mathbb{F}_3$

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

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

Какие из них неприводимы? Все!

Неприводимые многочлены над $\mathbb{F}_3$

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

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

Какие из них неприводимы? Все!

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

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

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

Построение конечных полей

— с использованием неприводимых многочленов.

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

Утверждение

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

Построение конечных полей...

Доказательство

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

Построение конечных полей...

Доказательство

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

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

Вопрос

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

Построение конечных полей...

Доказательство

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

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

Вопрос

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

Теорема

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

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

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

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

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

$$(x+1)+(x+2) = 2x, \qquad (x)\cdot(2x) = 1,$$
$$(2x+1)+(x) = 1, \qquad (2x+1)\cdot(x) = x+1.$$

Построение поля $\mathbb{F}_3^2$...

Заметим, что

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

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

Построение поля $\mathbb{F}_3^2$...

Заметим, что

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

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

Вопрос

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

Построение поля $\mathbb{F}_3^2$...

Заметим, что

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

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

Вопрос

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

Ответ: получится поле, изоморфное построенному.

Раздел I

Раздел II

- Коды БЧХ
- 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: $r_{-1} = r_0q_1 + r_1$ — 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 $n+1$: $r_{n-1} = r_nq_{n+1} + 0$ — 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

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

Шаг (-2): $r_{-2} = 252;$

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

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

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

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

$\text{НОД}(252, 105) = 21.$

Алгоритм Евклида: пример

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

Шаг (-2): $r_{-2} = 252;$

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

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

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

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

$\text{НОД}(252, 105) = 21.$

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

Теорема Безу и расширенный алгоритм Евклида

Теорема (Безу)

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

Теорема Безу и расширенный алгоритм Евклида

Теорема (Безу)

Если $d = НОД(a, b)$, *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 $d = НОД(a, b)$, 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

$$d = НОД(a, b) = ax + ay,$$

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

$$r_i = r_{i-2} - q_i r_{i-1} = (a x_{i-2} + b y_{i-2}) - q_i (a x_{i-1} + b y_{i-1}) =$$
$$= a(x_{i-2} - q_i x_{i-1}) + b(y_{i-2} - q_i y_{i-1}) = a x_i + b y_i.$$

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* $4x = 1.$ $(*)$

Задача

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

Решение

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

Задача

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

Решение

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

Решение

1. $4x = k \cdot 101 + 1 = 102, 203, 304, \ldots;$ $x = 304/4 = 76.$ *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, $\deg g < \deg f \;\Rightarrow\; \text{НОД}(f, g) = 1$.

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. $r_{-2}(x)=x^4+x^3+x^2+3,$
$r_{-1}(x)=x^2+x+3,$
$y_{-2}(x)=0,$
$y_{-1}(x)=1.$

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

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

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

Раздел II

- Коды БЧХ
- Что надо знать

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

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

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

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

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

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

L4: $1 \cdot v = v$ (унитальность).

Координатное пространство

Пример

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

Получившаяся структура — векторное пространство.
Его называют *n-мерным координатным пространством* над полем $\Bbbk$.

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

Раздел II

- Коды БЧХ
- Что надо знать

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

Минимальные многочлены: пример построения

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

1. $a_0\overline{1} + a_1\overline{x} + \ldots + a_n\overline{x}^n = \overline{a_0 + a_1 x + \ldots + a_n x^n} \equiv_p \overline{0}$, 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 $f(x) = c_0 + c_1 x + \ldots + c_n x^n$.
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 непривод**имые** 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 $F \stackrel{\text{def}}{=} \mathbb{F}_p/(\varphi)$ — 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 β, β^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, $\ldots$, $\beta^{p^{n-1}}$:

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*.

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 $f(x)$:

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

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

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

Если $f(x)$ —

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

Раздел I

Раздел II

- Коды БЧХ
- Что надо знать

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 $i = 1, \ldots, d_n$ 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 ($\sum_{m|n} m \cdot d_m = p^n$).

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

- Коды БЧХ
- 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:*
$$I_\varphi \stackrel{\text{def}}{=} \{t \cdot \varphi\} \lhd \mathbb{F}_p[x]/(f).$$
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 $g \cdot \overline{x}$, $g \cdot \overline{x^2}$, $\ldots$ *— 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

- Коды БЧХ
- Что надо знать

Задача (Теорема Вильсона)

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

Задача (Теорема Вильсона)

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

Решение

$p = 2$: — *утверждение тривиально.*

Задача (Теорема Вильсона)

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

Решение

$p = 2$: — *утверждение тривиально.*

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

По теореме Виета их произведение равно свободному члену -1.

Задача

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

Задача

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

Решение

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

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

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

Задача

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

Задача

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

Решение

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

Задача

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

Задача

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

Решение

Можно, например, использовать интерполяционный многочлен Лагранжа:

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

Задача

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

Задача

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

Решение

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

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

Задача

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

Задача

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

Решение

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

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

Задача

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

Задача

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

Решение

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

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

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

Ответ: $(x^2 + 1)(x^2 + x + 2)$.

Задача

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

Задача

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

Решение

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

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

Задача

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

Задача

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

Решение

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

Задача

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

Задача

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

Решение

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

Задача

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

Задача

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

Решение

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

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

Задача

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

Задача

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

Решение

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

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

Задача

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

Задача

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

Решение

1. $f(x) = x^2 + x - 1$, $f(0) = 6$, $f(1) = 1$, $f(2) = 5$, $f(3) = 4$, $f(4) = 6$, $f(5) = 1$, $f(6) = 6 \Rightarrow$
   многочлен $f(x)$ *— неприводим в* $\mathbb{F}_7$ *и* F *— поле* $(= \mathbb{F}_7^2)$.

Задача

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

Решение

1. $f(x) = x^2 + x - 1$, $f(0) = 6$, $f(1) = 1$, $f(2) = 5$, $f(3) = 4$, $f(4) = 6$, $f(5) = 1$, $f(6) = 6 \Rightarrow$
   многочлен $f(x)$ *— неприводим в* $\mathbb{F}_7$ *и* F *— поле* $(= \mathbb{F}_7^2)$.
2.

$$\mathbb{F}_7^2 = \{ ax + b \mid a, b \in \mathbb{F}_7,\ x^2 = 1 - x = 6x + 1 \}$$

$$(ax + b) \cdot (6x + 1) = \ldots = (2a + 6b)x + (6a + b) = 1$$

$$\begin{cases} 6a + b = 1 \\ a + 3b = 0 \end{cases} \Rightarrow \begin{cases} a = 1 \\ b = 2 \end{cases}$$

Проверка: $(6x + 1)(x + 2) = 6x^2 + 13x + 2 = 1 + 7x = 1.$

Задача

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

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

Задача

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

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

Решение

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

1. $x^4 = x + 1$

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

Ответ: 3.

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

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

Задача

Найти количество неприводимых многочленов

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

Задача

Найти количество неприводимых многочленов

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

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

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

Задача

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

Решение

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

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

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

Задача

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

Задача

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.*

Раздел I

Раздел II

- Коды БЧХ
- Что надо знать

- Конечное поля 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?
- 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

- Коды БЧХ
- Что надо знать

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

Бóльшая 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

Бóльшая 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

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

Доказательство

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

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

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

Кодовое расстояние

Определение

Минимальное расстояние между словами кода называется *кодовым расстоянием*.

Утверждение

Множество C *образует код с исправлением не 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*

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

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

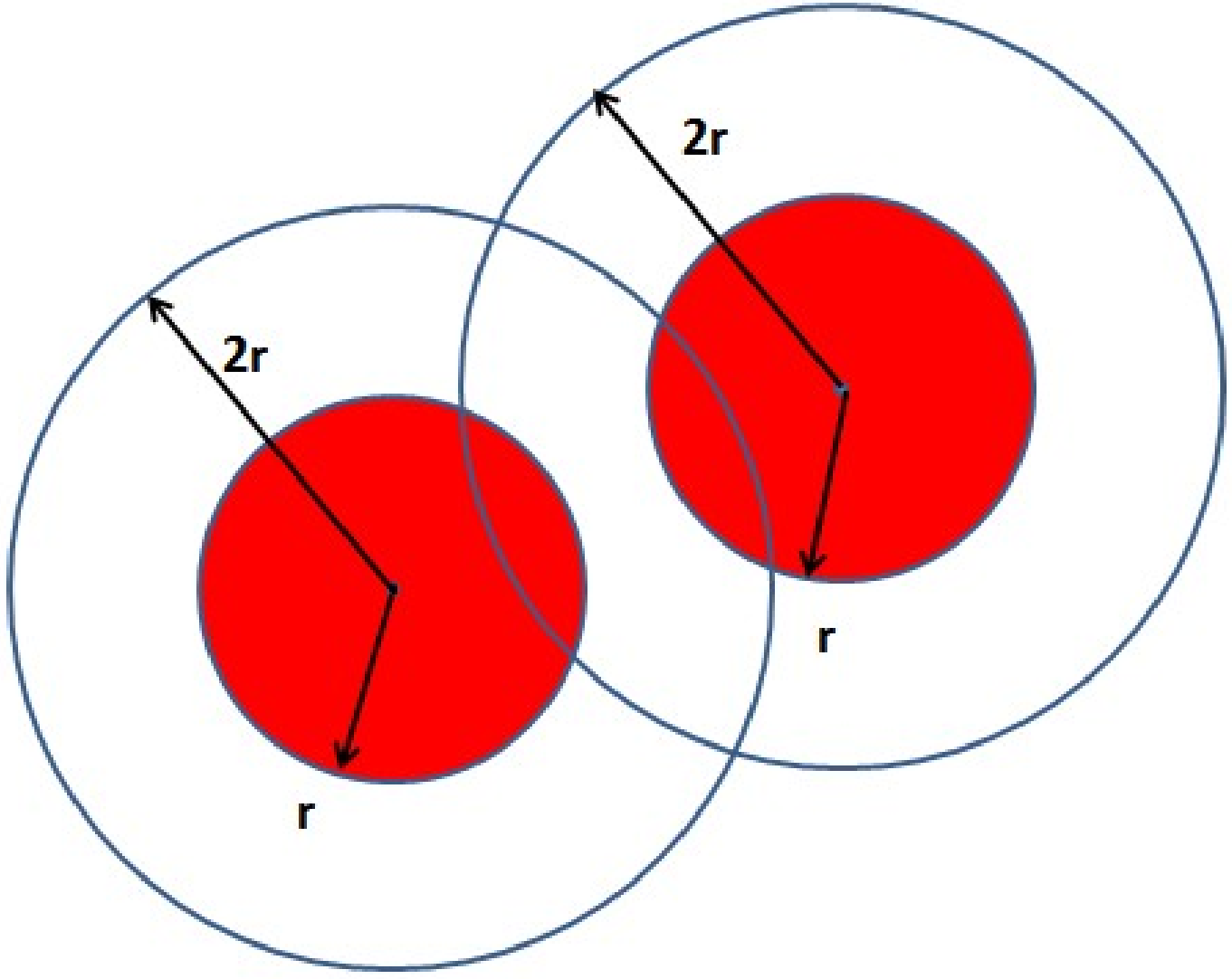

Рис. 1. К теореме Хэмминга

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:

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

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

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 ($m = 3$):

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

Складывая по $\mathrm{mod}\,2$ произвольные совокупности строк, получаем 16 различных бинарных наборов, которыми можно закодировать 16 сообщений: например,

$$\text{10 цифр} \,|\, \text{разделитель} \,|\, = \,|\, + \,|\, - \,|\, \times \,|\, \div .$$

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

- Коды БЧХ
- Что надо знать

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

- Коды БЧХ
- Что надо знать

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 α, α^2, $\ldots$, α^{2r} (как и φ).

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

Значит, надо доказать следующее

Утверждение

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

Оценка кодового расстояния...

Доказательство

Рассмотрим многочлен

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

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

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

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

Теория решения СЛАУ конечным полем ничем не отличается от привычной теории решения СЛАУ над $\mathbb{R}$ (она вовсе не зависит от поля задания). В частности, линейная зависимость между столбцами квадратной матрицы равносильна обращению в нуль определителя этой матрицы.

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

Получим квадратную матрицу

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

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

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

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

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

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

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

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

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

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

Что дальше?

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

Раздел I

Раздел II

- Коды БЧХ
- Что надо знать

- 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.