Построение конечного поля с 2^n элементами

Александра Игоревна Кононова

МИЭТ

15 декабря 2022 г. — актуальную версию можно найти на
`https://gitlab.com/illinc/otik`

Конечные поля (поля Галуа)

Конечное поле или поле Галуа

Поле, состоящее из конечного числа элементов. $\mathbb{F}_q$ или $\mathrm{GF}(q)$, где q — число элементов (мощность).

$q = p^n$, где p — простое число (**характеристика** поля), $n \in \mathbb{N}$.

С точностью до изоморфизма:

для $q = p$ $\quad \mathrm{GF}(q) = \mathbb{Z}_p$

для $q = p^n$ $\quad \mathrm{GF}(q)$ — расширение поля $\mathbb{Z}_p$

Многочлены над полем

Многочлен степени $n \in \mathbb{N} \cup \{0\}$ над полем $\mathcal{F}$

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

$$a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{F}$$

$p(x) = q(x)$, если равны их коэффициенты при одинаковых степенях x.

$x^k \cdot x^m = x^{k+m} (k, m \in \mathbb{N} \cup \{0\}), \quad x^0 \equiv 1.$

Множество всех многочленов $\mathcal{F}[x]$ — коммутативное кольцо (ассоциативно-коммутативное кольцо с единицей — при другом наборе аксиом кольца).

Делимость многочленов

$\forall p(x), q(x) \in \mathcal{F}[x] \;\; \exists s(x), r(x) \in \mathcal{F}[x]:$
$p(x) = s(x) \cdot q(x) + r(x)$

причём $\deg r(x) < \deg q(x)$ или $r(x) = 0$.

Многочлен $s(x)$ называется **частным** (неполным частным), а многочлен $r(x)$ — **остатком** от деления $p(x)$ на $s(x)$.

Частное и остаток определяются однозначно.

Справедлива теорема Безу (и её следствия): остаток от деления $f(x)$ на $(x - a)$ равен $f(a)$.

Неприводимые многочлены

Если для любого разложения
$p(x) = s(x) \cdot q(x), \quad p(x), s(x), q(x) \in \mathcal{F}[x]$

либо $\deg s(x) = 0$, либо $\deg q(x) = 0$,

многочлен $p(x)$ называется **неприводимым** (простым) в кольце $\mathcal{F}[x]$ (или над полем $\mathcal{F}$).

Примеры

	x^2+1	x^2+x+1
Над $\mathbb{Z}_2$	$(x+1)(x+1)$	неприводим
Над $\mathbb{Z}_3$	неприводим	$(x+2)(x+2)$
Над $\mathbb{R}$	неприводим	неприводим
Над $\mathbb{C}$	$(x+i)(x-i)$	$(x+\frac{1+i\sqrt{3}}{2})(x+\frac{1-i\sqrt{3}}{2})$

Классы вычетов многочленов

Класс вычетов по модулю многочлена $g(x)$ содержит все многочлены $\mathcal{F}[x]$, которые имеют один и тот же остаток при делении на $g(x)$.

Если $g(x)$ неприводим в $\mathcal{F}[x]$, множество классов вычетов (фактор-кольцо $\mathcal{F}[x]/g(x)$) — **поле.**

Поле $\mathcal{F}[x]/g(x)$ — расширение $\mathcal{F}$, полученное добавлением корня $g(x)$ (примитивное расширение) — фиктивного $c \notin \mathcal{F}$, что $g(c) = 0$.

Примитивные расширения $\mathbb{R}$

Многочлен $g(x) = x^2 + 1$ неприводим над $\mathbb{R}$.

Поле $\mathbb{C}$ — примитивное расширение $\mathbb{R}$, полученное добавлением фиктивного корня $x^2 + 1$ — «мнимой единицы» $i \notin \mathbb{R}$.

x, $x + 1$, $x + 2$, $x^2 + 4$ *и* $x^2 + x + 1$ *также неприводимы над* $\mathbb{R}$. *Как будут выглядеть примитивные расширения?*

Не все многочлены без корней неприводимы:
над $\mathbb{R}$ $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$

Над $\mathbb{C}$ неприводимы только линейные многочлены $x - a$;

над $\mathbb{R}$ — линейные и некоторые квадратичные многочлены $\Longrightarrow$ расширения $\mathbb{R}$ изоморфны $\mathbb{C}$.

Примитивные расширения $\mathbb{Z}_2$

Многочлен $g(x) = x^2 + x + 1$ неприводим над $\mathbb{Z}_2$.

Пусть $i \notin \mathbb{Z}_2$ — фиктивный корень $x^2 + x + 1$.

$$i^2 + i + 1 = 0$$

Элементы примитивного расширения $0, 1, i, i + 1$.
$i^2 = -(i + 1) = i + 1$

Поле $\mathrm{GF}(4)$

Полиномиальное представление	Числовое представление	Степени		
		0	1	2
1	1	1	1	1
i	2	1	i (2)	$i+1$ (3)
$i+1$	3	1	$i+1$ (3)	i (2)

Из обобщённой малой теоремы Ферма $a^3 = 1$ для всех ненулевых a.

i и $i+1$ — примитивные элементы, наименьший i:

$$\begin{aligned} 1 &= 1 &&= i^0 \\ 2 &= i &&= i^1 \\ 3 &= i+1 &&= i^2 \end{aligned}$$

Сложение и умножение в $\mathrm{GF}(4)$

Сложение — сложение многочленов с учётом $1+1=0$ (побитовое по модулю 2)

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

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

Умножение — умножение степеней примитивного элемента с учётом $i^3=1$

$\cdot$	0	1	i	i^2
0	0	0	0	0
1	0	1	i	i^2
i	0	i	i^2	1
i^2	0	i^2	1	i

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

Разрежённые полиномы, неприводимые по модулю 2 (порождающие табличные)

$x^2 + x + 1$
$x^3 + x + 1$
$x^4 + x + 1$
$x^5 + x + 1$
$x^6 + x + 1$
$x^7 + x^3 + 1$
$x^8 + x^4 + x^3 + x^2 + 1$ (RS)
$x^8 + x^4 + x^3 + x + 1$ (AES)
$x^9 + x^4 + 1$

$x^{10} + x^3 + 1$
$x^{11} + x^2 + 1$
$x^{12} + x^3 + 1$
$x^{13} + x^4 + x^3 + x + 1$
$x^{14} + x^5 + 1$
$x^{15} + x + 1$
$x^{16} + x^5 + x^3 + x + 1$
$\dots$
$x^{32} + x^7 + x^3 + x^2 + 1$

$\dots$
$x^{64} + x^4 + x^3 + x + 1$
$\dots$
$x^{128} + x^7 + x^2 + x + 1$
$\dots$
$x^{256} + x^{10} + x^5 + x^2 + 1$
$\dots$
$x^{512} + x^8 + x^5 + x^2 + 1$

Наименьший примитивный элемент расширения: i (2) (для большинства).

Для используемого в AES $x^8 + x^4 + x^3 + x + 1$ примитивный элемент $i + 1$ (3).

Таблица степеней GF(8), порождающий полином $x^3 + x + 1$

Полиномиальное представление			Степени							
			0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
	1	**1**	1	1	1	1	1	1	1	1
	x	**2**	1	2	4	3	6	7	5	1
	x+1	**3**	1	3	5	4	7	2	6	1
	x^2	**4**	1	4	6	5	2	3	7	1
	x^2+1	**5**	1	5	7	6	3	4	2	1
	x^2+x	**6**	1	6	2	7	4	5	3	1
	x^2+x+1	**7**	1	7	3	2	5	6	4	1

Таблица степеней GF(16)

	Степени															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9	1
3	1	3	5	15	2	6	10	13	4	12	7	9	8	11	14	1
4	1	4	3	12	5	7	15	9	2	8	6	11	10	14	13	1
5	1	5	2	10	4	7	8	14	3	15	6	13	12	9	11	1
6	1	6	7	1	6	7	1	6	7	1	6	7	1	6	7	1
7	1	7	6	1	7	6	1	7	6	1	7	6	1	7	6	1
8	1	8	12	10	15	1	8	12	10	15	1	8	12	10	15	1
9	1	9	13	15	14	7	10	5	11	12	6	3	8	4	2	1
10	1	10	8	15	12	1	10	8	15	12	1	10	8	15	12	1
11	1	11	9	12	13	6	15	3	14	8	7	4	10	2	5	1
12	1	12	15	8	10	1	12	15	8	10	1	12	15	8	10	1
13	1	13	14	10	11	6	8	2	9	15	7	5	12	3	4	1
14	1	14	11	8	9	7	12	4	13	10	6	2	15	5	3	1
15	1	15	10	12	8	1	15	10	12	8	1	15	10	12	8	1

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

$x,\ x+1,\ x+2$

Корни $x,\ x+1,\ x+2$ уже есть в $\mathbb{R}$ — расширение невозможно.

$g(x) = x^2 + 4$

$\mathbb{R}[x]/g(x)$: пары $a + b \cdot j$, где $a, b \in \mathbb{R}$,
j — фиктивный корень уравнения $x^2 + 4 = 0$ $(j^2 = -4)$.

Изоморфно $\mathbb{C}$: соответствие при $j \leftrightarrow 2i$ или при $j \leftrightarrow -2i$:

- соответствие взаимно однозначное;
- образ суммы равен сумме образов;
- образ произведения равен произведению образов.

Кроме того, $a + 0j \leftrightarrow a + 0i$, в частности $0 \leftrightarrow 0$ и $1 \leftrightarrow 1$.

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

$\mathbb{R}[x]/g(x)$: пары $a + b \cdot j$, где $a, b \in \mathbb{R}$,
j — фиктивный корень уравнения $x^2 + x + 1 = 0$ $(j^2 = -j - 1)$.

Изоморфно $\mathbb{C}$: $j \leftrightarrow -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ или $j \leftrightarrow -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Пусть $j \leftrightarrow -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, то есть $-\frac{\sqrt{3}}{3} - \frac{2\sqrt{3}}{3}j \leftrightarrow i$:

$$a + b \cdot j \quad \leftrightarrow \quad \left(a - \frac{1}{2}b\right) - \frac{\sqrt{3}}{2}b \cdot i$$
$$\left(\alpha - \frac{\sqrt{3}}{3}\beta\right) - \frac{2\sqrt{3}}{3}\beta \cdot j \quad \leftrightarrow \quad \alpha + \beta \cdot i$$

- соответствие взаимно однозначное;
- образ суммы равен сумме образов;
- образ произведения равен произведению образов.

Кроме того, $a + 0j \leftrightarrow a + 0i$, в частности $0 \leftrightarrow 0$ и $1 \leftrightarrow 1$.

$g(x) = x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$

$\mathbb{R}[x]/g(x)$ — не является полем, это кольцо с делителями нуля

$\mathbb{R}[x]/g(x)$: *четвёрки* $a + b \cdot j + c \cdot j^2 + d \cdot j^3$, где $a, b, c, d \in \mathbb{R}$,
j — фиктивный корень $x^4 + 1 = 0$ $(j^4 = -1)$; $\mathbb{C}$ — *пары* $\alpha + \beta \cdot i$.

Соответствие $j \leftrightarrow \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ не взаимно однозначно:

$$\begin{cases} -1 + \sqrt{2}j = -1 + (1 + i) = i, \\ j^2 = i, \end{cases}$$ но $-1 + \sqrt{2}j \neq j^2$ в $\mathbb{R}[x]/g(x)$.

не вз. одн. $j \leftrightarrow -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$; $j \leftrightarrow \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$; $j \leftrightarrow -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$.

Изоморфизма не может существовать: уравнение $x^2 = -1$
в $\mathbb{C}$ имеет два различных корня: $x_{1,2} = \pm i$;

в $\mathbb{R}[x]/g(x)$ — четыре: $$\begin{cases} x_{1,2} = \pm j^2, \\ x_{3,4} = \pm \frac{\sqrt{2}}{2}(j + j^3). \end{cases}$$

$g(x) = x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$

Более того: уравнение $x^4 = -1$

в $\mathbb{C}$ имеет четыре различных корня: $\begin{cases} x_{1,2} = \pm\frac{\sqrt{2}}{2}(1+i), \\ x_{3,4} = \pm\frac{\sqrt{2}}{2}(1-i); \end{cases}$

в $\mathbb{R}[x]/g(x)$ — как минимум восемь: $\begin{cases} x_{1,2} = \pm j, \\ x_{3,4} = \pm j^3, \\ x_{5,6} = \pm\frac{\sqrt{2}}{2}(1+j^2), \\ x_{7,8} = \pm\frac{\sqrt{2}}{2}(1-j^2). \end{cases}$

$g(x) = x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$

Нетривиальные ($\neq 0$) делители нуля:

$$\left(1+\sqrt{2}j+j^2\right)\left(a+bj+(-a-\sqrt{2}b)j^2+(\sqrt{2}a+b)j^3\right) = 0 \ \ \forall a, b \in \mathbb{R}$$

$$\left(1-\sqrt{2}j+j^2\right)\left(a+bj+(-a+\sqrt{2}b)j^2+(-\sqrt{2}a+b)j^3\right) = 0 \ \ \forall a, b \in \mathbb{R}$$

в частности, $(1 + \sqrt{2}j + j^2)(1 - \sqrt{2}j + j^2) = 0$.

У делителей нуля нет обратного ($\alpha^{-1}\alpha\beta = ?$) $\implies$ не поле.

В поле рациональных чисел $\mathbb{Q}$ $g(x) = x^4 + 1$ неприводим.

$\mathbb{Q}[x]/g(x)$ — поле, но не изоморфное $\mathbb{C}$:
$\mathbb{Q}[x]/g(x)$ счётно, как и $\mathbb{Q}$; а $\mathbb{C}$ континуально.

$g(x) = x^2 - 2x + 2$

$\mathbb{R}[x]/g(x)$: пары $a + b \cdot j$, где $a, b \in \mathbb{R}$,
j — фиктивный корень уравнения $x^2 - 2x + 2 = 0$ $(j^2 = 2j - 2)$.

Изоморфно $\mathbb{C}$: $j \leftrightarrow 1 - i$ или $j \leftrightarrow 1 + i$.

Пусть $j \leftrightarrow 1 + i$, то есть $-1 + j \leftrightarrow i$:

$$\begin{array}{rcl} a + b \cdot j & \leftrightarrow & (a + b) + b \cdot i \\ (\alpha - \beta) + \beta \cdot j & \leftrightarrow & \alpha + \beta \cdot i \end{array}$$

- соответствие взаимно однозначное;
- образ суммы равен сумме образов;
- образ произведения равен произведению образов.

Кроме того, $a + 0j \leftrightarrow a + 0i$, в частности $0 \leftrightarrow 0$ и $1 \leftrightarrow 1$.

Спасибо за внимание!

МИЭТ
www.miet.ru

Александра Игоревна Кононова
illinc@mail.ru
gitlab.com/illinc/raspisanie