

Определения АП

Материал из Прикладная алгебра

Содержание

- 1 Понятие группы, подгруппы, фактор-группы, индекса группы по подгруппе. Примеры. Теорема Лагранжа.
 - 1.1 Группа
 - 1.1.1 Свойства
 - 1.2 Факторгруппа
 - 1.3 Индекс подгруппы в группе
 - 1.4 Теорема Лагранжа
 - 1.5 Примеры
- 2 Понятие циклической группы. Структура подгрупп циклической группы. Количество порождающих элементов.
 - 2.1 Циклическая группа
 - 2.1.1 Свойства
 - 2.1.2 Пример
 - 2.2 Функция Эйлера
- 3 Понятие кольца, подкольца, фактор-кольца, евклидова кольца, идеала в кольце. Примеры.
 - 3.1 Кольцо
 - 3.1.1 Свойства
 - 3.1.2 Дополнительные требования
 - 3.1.3 Подкольцо
 - 3.2 Идеал
 - 3.2.1 Свойства
 - 3.3 Факторкольцо
 - 3.3.1 Примеры:
 - 3.4 Евклидово кольцо
 - 3.4.1 Примеры:
- 4 Расширенный алгоритм Евклида и его применение.
 - 4.1 Алгоритм
 - 4.2 Python
 - 4.3 Применение
- 5 Понятие поля. Построение конечных полей с помощью неприводимых многочленов (привести пример). Полиномиальное и степенное представление элементов поля.
 - 5.1 Поле
 - 5.1.1 Характеристика поля
 - 5.1.2 Свойства:
 - 5.1.3 Примеры полей:
 - 5.2 Построение поля Галуа
 - 5.2.1 Пример построения поля $GF(9)$
 - 5.2.2 Таблица сложения в $GF(9)$
 - 5.2.3 Таблица умножения в $GF(9)$
 - 5.3 Степенное представление элементов поля
- 6 Алгоритм нахождения всех корней многочлена $f(x)$ над полем $\mathbb{F}_p$
- 7 Минимальные многочлены для элементов конечного поля. Алгоритм нахождения минимального многочлена.
 - 7.1 Построение:
- 8 Теорема Хэмминга. Пример построения кода Хэмминга.
- 9 Определение
 - 9.1 Теорема Хэмминга
 - 9.2 Пример
- 10 Коды БЧХ: определение, примеры кодов с исправлением одной, двух и трех ошибок.
 - 10.1 Построение БЧХ кодов:
 - 10.2 Пример кода, исправляющего 1 ошибку
 - 10.3 Пример кода, исправляющего 2 ошибки
 - 10.4 Пример кода, исправляющего 3 ошибки
- 11 Понятие действия группы на множестве, фиксатор и стабилизатор. Примеры.
 - 11.1 Действие слева
 - 11.2 Действие справа
 - 11.3 Комментарии
 - 11.4 Фиксатор
 - 11.5 Стабилизатор
- 12 Лемма Бернсайда и её применение.
 - 12.1 Лемма Бернсайда
 - 12.2 Пример
- 13 Цикловой индекс действия группы
- 14 Группы симметрий правильных многоугольников (диэдральные группы) и группы вращений правильных многогранников. Примеры. Их цикловые индексы.
- 15 Теорема Редфилда-Пойа и её применение
 - 15.1 Цикловой индекс действия группы

- 15.2 Теорема Редфилда-Пойа
- 15.3 Пример
- 16 Идеалы и фильтры частично упорядоченного множества. Конусы. Точные грани.
 - 16.1 Определение
- 17 Идеал частично упорядоченного множества
- 18 Фильтр частично упорядоченного множества
- 19 Конус
- 20 Точные грани
- 21 Теорема Шпильрайна. Линейное продолжение частично упорядоченного множества
- 22 Определение
 - 22.1 Теорема Шпильрайна
- 23 Спектр и размерность частично упорядоченного множества
 - 23.1 Определение
 - 23.2 Спектр частично упорядоченного множества
 - 23.3 Размерность
- 24 Фундаментальная теорема о конечных дистрибутивных решётках.
 - 24.1 Определения
 - 24.2 Фундаментальная теорема о конечных дистрибутивных решётках
- 25 Соответствия Галуа.
 - 25.1 Определения

Понятие группы, подгруппы, фактор-группы, индекса группы по подгруппе. Примеры. Теорема Лагранжа.

Группа

Непустое множество G с заданной на нём бинарной операцией $*$: $G \times G \rightarrow G$ называется группой $(G, *)$, если выполнены следующие аксиомы:

1. **ассоциативность**: $\forall (a, b, c \in G) : (a * b) * c = a * (b * c)$
2. **наличие нейтрального элемента**: $\exists e \in G \quad \forall a \in G : (e * a = a * e = a)$
3. **наличие обратного элемента**: $\forall a \in G \quad \exists a^{-1} \in G : (a * a^{-1} = a^{-1} * a = e)$

- Подгруппа — подмножество H группы G , которое является группой относительно операции, определённой в G .
- Подгруппа N группы G называется **нормальной**, если она инвариантна относительно сопряжений, то есть для любого элемента n из N и любого g из G , элемент gng^{-1} лежит в N :

Свойства

- Свойство сократимости $\{a, b, c\} \in G, a \neq b \rightarrow c * a \neq c * b$

Факторгруппа

Пусть G — группа, и H — её нормальная подгруппа. Тогда на классах смежности H в G

$$aH = \{ah \mid h \in H\}$$

можно ввести умножение:

$$(aH)(bH) = abH$$

Легко проверить что это умножение не зависит от выбора элементов в классах смежности, то есть если $aH = a'H$ и $bH = b'H$, то $abH = a'b'H$. Это умножение определяет структуру группы на множестве классов смежности, а полученная группа G/H называется факторгруппой G по H .

Индекс подгруппы в группе

Индекс подгруппы H в группе G — число классов смежности в каждом (правом или левом) из разложений группы G по этой подгруппе H (в бесконечном случае — мощность множества этих классов).

Индекс подгруппы H в группе G обычно обозначается $[G : H]$.

Теорема Лагранжа

Пусть группа G конечна и H — её подгруппа. Тогда порядок G равен порядку H , умноженному на количество её левых или правых классов смежности (индекс). $|G| = |H| * (G : H)$. Обратное утверждение неверно.

Примеры

- **Целые числа с операцией сложения.** $(\mathbb{Z}, +)$ — коммутативная группа с нейтральным элементом 0.
- **Положительные рациональные числа с операцией умножения.** Произведение рациональных чисел — снова рациональное число, обратный элемент к рациональному числу представляется обратной дробью, имеется ассоциативность и единица.
- **Циклические группы** состоят из степеней $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ одного элемента **a**. Такие группы всегда коммутативны. Примеры таких групп — упомянутые уже

целые числа по сложению и группа корней из единицы.

- **Симметрическая группа** группа перестановок.

Понятие циклической группы. Структура подгрупп циклической группы. Количество порождающих элементов.

Циклическая группа

Группа $(G, \cdot)$ называется **циклической**, если она может быть *порождена* одним элементом *a*, то есть все её элементы являются степенями *a*. Обозначение: $G = \langle a \rangle$.

Любая конечная циклическая группа порядка *n* изоморфна аддитивной группе классов вычетов $\mathbb{Z}_n$. Отсюда вытекает, что, с точностью до изоморфизма, существует только одна конечная циклическая группа данного порядка.

Свойства

- Любая подгруппа циклической группы тоже циклична. Циклической будет и всякая фактор-группа циклической группы G/H .
- У циклической группы порядка *n* существует ровно $\varphi(n)$ порождающих элементов, где φ — функция Эйлера
- У циклических подгрупп всегда найдется единственная подгруппа, порядок которой равен порядку делителя.

Пример

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

порядок	подгруппа	k	количество порождающих
0	{0}	1	1
1	{1,2,3,4,5,0}	6	2
2	{2,4,0}	3	2
3	{3,0}	2	1
4	{4,2,0}	3	2
5	{5,4,3,2,1,0}	6	2

берем порядок, складываем с собой. получаем подгруппу.

Функция Эйлера

Функция Эйлера $\varphi(n)$ — мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших *n* и взаимно простых с ним. При этом полагают, что число 1 взаимно просто со всеми натуральными числами, и $\varphi(1) = 1$.

Понятие кольца, подкольца, фактор-кольца, евклидова кольца, идеала в кольце. Примеры.

Кольцо

Кольцо — это множество *R*, на котором заданы две бинарные операции: + и × (называемые **сложением** и **умножением**), со следующими свойствами, выполняющимися для любых *a, b, c* ∈ *R*:

Свойства

- По сложению абелева группа
 - По умножению дистрибутивность (левая и правая)
1. $a + b = b + a$ — коммутативность сложения;
 2. $a + (b + c) = (a + b) + c$ — ассоциативность сложения;

3. $\exists 0 \in R (a + 0 = 0 + a = a)$ — существование нейтрального элемента относительно сложения;
4. $\forall a \in R \exists b \in R (a + b = b + a = 0)$ — существование противоположного элемента относительно сложения;
5. $(a \times b) \times c = a \times (b \times c)$ — ассоциативность умножения
6. $\begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a \end{cases}$ — дистрибутивность.

Дополнительные требования

- Отсутствие делителей нуля (целостное кольцо)
- Наличие единицы по умножению
- Коммутативность по умножению
- Обратный элемент по умножению

Если все свойства выполнены, то получим поле.

Подкольцо

Подмножество $A \subset R$ называется **подкольцом** R , если A само является кольцом относительно операций, определенных в R . По определению, оно непусто, поскольку содержит нулевой элемент. Эквивалентно, непустое подмножество $A \subset R$ является подкольцом, если для любых x и y из A , $x + y$, xy и $-x$ также принадлежат A .

Идеал

Для кольца R идеалом I называется подкольцо, замкнутое относительно умножения на элементы из R . При этом идеал называется **левым** (соответственно **правым**), если он замкнут относительно умножения слева (соответственно справа) на элементы из R . Идеал, являющийся одновременно левым и правым, называется **двусторонним**. *Двусторонний идеал* часто называется просто *идеалом*. В коммутативном случае все эти три понятия совпадают и всегда применяется термин *идеал*.

Свойства

- По сложению подгруппа группы кольца
- $\forall i \in I, r \in R \rightarrow r * i \in I$

Факторкольцо

Пусть I — двусторонний идеал кольца R . Определим на R отношение эквивалентности:

$$a \sim b \text{ тогда и только тогда, когда } a - b \in I.$$

Класс эквивалентности элемента a обозначается как $[a]$ или $a + I$ и называется классом смежности по модулю идеала.

Факторкольцо R/I — это множество классов смежности элементов R по модулю I , на котором следующим образом определены операции сложения и умножения:

Примеры:

- Пусть $\mathbb{Z}$ — кольцо целых чисел, $n\mathbb{Z}$ — идеал, состоящий из чисел, кратных n . Тогда $\mathbb{Z}/n\mathbb{Z}$ — кольцо вычетов по модулю n .
- Рассмотрим кольцо многочленов с действительными коэффициентами $\mathbb{R}[x]$ и идеал, состоящий из многочленов, кратных $x^2 + 1$. Факторкольцо $\mathbb{R}[x]/(x^2 + 1)$ изоморфно полю комплексных чисел: класс $[x]$ соответствует мнимой единице. Действительно, в факторкольце элементы $x^2 + 1$ и 0 эквивалентны, то есть $x^2 = -1$.
- Обобщая предыдущий пример, факторкольца часто используют для построения расширений полей. Пусть K — некоторое поле и $f(x)$ — неприводимый многочлен в $K[x]$. Тогда $K[x]/(f(x))$ является полем, и это поле содержит по крайней мере один корень многочлена $f(x)$ — класс смежности элемента x .
- Важный пример использования предыдущей конструкции — построение конечных полей. Рассмотрим конечное поле $\mathbb{Z}/2\mathbb{Z}$ из двух элементов и в этом контексте обычно обозначается как $\mathbb{F}_2$. Многочлен $x^2 + x + 1$ неприводим над этим полем (так как не имеет корней), следовательно, факторкольцо $\mathbb{F}_2[x]/(x^2 + x + 1)$ является полем. Это поле состоит из четырёх элементов: 0 , 1 , x и $x+1$. Все конечные поля можно построить аналогичным образом.

Евклидово кольцо

Евклидово кольцо — это область целостности (ассоциативное коммутативное кольцо без делителей нуля) R , для которой определена **евклидова функция** (*евклидова норма*) $d: R \rightarrow \mathbb{N}_0 \cup \{-\infty\}$, причём $d(a) = -\infty \Leftrightarrow a = 0$ и возможно деление с остатком, по норме меньшим делителя, то есть для любых $a, b \in R$, $b \neq 0$ имеется представление $a = bq + r$, для которого $d(r) < d(b)$ или $r = 0$. В Евклидовом кольце работает алгоритм Евклида.

Примеры:

- Кольцо целых чисел $\mathbb{Z}$. Пример евклидовой функции — $|\cdot|$.
- Произвольное поле K является евклидовым кольцом с нормой, равной 1 для всех элементов, кроме 0.
- Кольцо многочленов одной переменной $K[x]$ над полем K . Пример евклидовой функции — степень Deg .

Расширенный алгоритм Евклида и его применение.

Алгоритм

```

 $r_0 = a$ 
 $x_0 = 1$ 
 $y_0 = 0$ 
 $r_1 = b$ 
 $x_1 = 0$ 
 $y_1 = 1$ 
...
 $r_{i+1} = r_{i-1} - q_i r_i$ 
 $x_{i+1} = x_{i-1} - q_i x_i$ 
 $y_{i+1} = y_{i-1} - q_i y_i$ 
...
```

Алгоритм завершается, когда $r_{i+1} = 0$.

Python

def egcd(a, b):

```

if a == 0:
    return (b, 0, 1)
else:
    g, y, x = egcd(b % a, a)
    return (g, x - (b // a) * y, y)
```

Применение

- Решение уравнений $a * x + b * y = GCD(a, b)$
- Обратный элемент в полях Галуа $\mathbb{F}_p[x]/(a(x))$. Пусть нужно найти обратный элемент $y(x)$ к $b(x)$.
 - $y(x) * b(x) = 1 \iff a(x) * x(x) + b(x) * y(x) = 1$

Алгоритм Евклида применим для евклидовых колец. Пример такого кольца - кольцо многочленов.

Понятие поля. Построение конечных полей с помощью неприводимых многочленов (привести пример). Полиномиальное и степенное представление элементов поля.

Поле

Поле — алгебра над множеством F , образующая коммутативную группу по сложению $+$ над F с нейтральным элементом 0 и коммутативную группу по умножению над ненулевыми элементами $F \setminus \{0\}$, при выполняющемся свойстве дистрибутивности умножения относительно сложения.

Характеристика поля

Пусть $\mathbb{F}$ - произвольное поле. 1 - единица $\mathbb{F}$. В конечном поле всегда найдется первое k , что $\sum_{i=1}^k 1 = 0$. Число k будем называть характеристикой поля $\mathbb{F}$.

Свойства:

- Характеристика поля всегда 0 или простое число.
 - Поле характеристики 0 содержит подполе, изоморфное полю рациональных чисел $\mathbb{Q}$.
 - Поле простой характеристики p содержит подполе, изоморфное полю вычетов $\mathbb{Z}_p$.
- Количество элементов в конечном поле всегда равно p^n — степени простого числа.
 - При этом для любого числа вида p^n существует единственное (с точностью до изоморфизма) поле из p^n элементов, обычно обозначаемое $\mathbb{F}_{p^n}$.
- В поле нет делителей нуля.
- Любая конечная подгруппа мультипликативной группы поля является циклической. В частности, мультипликативная группа

ненулевых элементов конечного поля $\mathbb{F}_q$ изоморфна $\mathbb{Z}_{q-1}$.

Примеры полей:

- $\mathbb{Q}$ — рациональные числа,
- $\mathbb{R}$ — вещественные числа,
- $\mathbb{C}$ — комплексные числа,
- $\mathbb{Z}_p$ — поле вычетов по модулю p , где p — простое число.
- $\mathbb{F}_q$ — конечное поле из $q = p^k$ элементов, где p — простое число, k — натуральное. Все конечные поля имеют такой вид.
- $\mathbb{F}(x)$ — поле рациональных функций вида $f(x)/g(x)$, где f и g — многочлены над некоторым полем $\mathbb{F}$ (при этом $g \neq 0$, а f и g не имеют общих делителей, кроме констант).

Неприводимый многочлен — многочлен, неразложимый на нетривиальные (неконстантные) многочлены. В поле $\mathbb{R}$ существуют неприводимые многочлены 1-й и 2-й степени (с отрицательным дискриминантом). В поле $\mathbb{C}$ существуют неприводимые многочлены 1-й

Построение поля Галуа

Поле $\text{GF}(p^n)$ при $n > 1$ строится как факторкольцо $\mathbb{K} = \mathbb{Z}_p[x]/\langle f(x) \rangle$, где $f(x)$ — неприводимый многочлен степени n над полем $\mathbb{Z}_p$. Таким образом, для построения поля из p^n элементов достаточно отыскать многочлен степени n , неприводимый над полем $\mathbb{Z}_p$. Элементами поля $\mathbb{K}$ являются все многочлены степени меньше n с коэффициентами из $\mathbb{Z}_p$. Арифметические операции (сложение и умножение) проводятся по модулю многочлена $f(x)$, то есть, результат соответствующей операции — это остаток от деления на $f(x)$ с приведением коэффициентов по модулю p .

Пример построения поля $\text{GF}(9)$

Для построения поля $\text{GF}(9) = \text{GF}(3^2)$ необходимо найти многочлен степени 2, неприводимый над $\mathbb{Z}_3$. Такими многочленами являются:

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

Возьмём, например, $x^2 + 1$, тогда искомого поле есть $\text{GF}(9) = \mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$. Если вместо $x^2 + 1$ взять другой многочлен, то получится новое поле, изоморфное старому.

Таблица сложения в $\text{GF}(9)$

$$\text{GF}(9) = \mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$$

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

Таблица умножения в $\text{GF}(9)$

$$\text{GF}(9) = \mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$$

$\times$	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	0	2	1	$2x$	$2x + 2$	$2x + 1$	x	$x + 2$	$x + 1$
x	0	x	$2x$	2	$x + 2$	$2x + 2$	1	$x + 1$	$2x + 1$
$x + 1$	0	$x + 1$	$2x + 2$	$x + 2$	$2x$	1	$2x + 1$	2	x
$x + 2$	0	$x + 2$	$2x + 1$	$2x + 2$	1	x	$x + 1$	$2x$	2
$2x$	0	$2x$	x	1	$2x + 1$	$x + 1$	2	$2x + 2$	$x + 2$
$2x + 1$	0	$2x + 1$	$x + 2$	$x + 1$	2	$2x$	$2x + 2$	x	1
$2x + 2$	0	$2x + 2$	$x + 1$	$2x + 1$	x	2	$x + 2$	1	$2x$

Степенное представление элементов поля

Заметим, что

- $(x + 1)^1 = x + 1$
- $(x + 1)^2 = 2x$
- $(x + 1)^3 = 2x + 1$
- $(x + 1)^4 = 2$
- $(x + 1)^5 = 2x + 2$
- $(x + 1)^6 = x$
- $(x + 1)^7 = x + 2$
- $(x + 1)^8 = 1$

Следовательно, $x + 1$ является *примитивным элементом* построенного поля. Если a - примитивным элемент поля $\text{GF}(q)$, то любой другой элемент поля может быть получен как степень a^k , где k - целое число, взаимно простое с $q - 1$.

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

- Разложим многочлен $f(x)$ на неприводимые множители над $\mathbb{F}_p$
 - $f(x) = g_1(x) * g_2(x) * \dots * g_k(x)$
- Для каждого многочлена $g_i(x)$, $i \in \{1, \dots, k\}$ рассмотреть расширение $\mathbb{F}_p[x]/\langle g_i(x) \rangle$, в котором он будет иметь корни $\alpha, \alpha^p, \dots, \alpha^{p^{\deg(g_i)-1}}$
- Записать эти корни как многочлены из $\mathbb{F}_p[x]/\langle g_i(x) \rangle$
- Объединить все корни в общем расширении $\mathbb{F}_p^m$, где $m = \text{LCM}(\deg(g_1), \dots, \deg(g_k))$

Источник: 148 слайд (311 страница)

Минимальные многочлены для элементов конечного поля. Алгоритм нахождения минимального многочлена.

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

- Многочлен $m(x)$ называется минимальным многочленом, если $m(x)$ - нормированный многочлен минимальной степени, для которого β является корнем.

Построение:

Пусть задано поле $\mathbb{F} = \mathbb{F}_p[x]/\langle a(x) \rangle$, где $a(x) = a_0 + a_1 * x + a_2 * x^2 + \dots + a_n * x^n$ - неприводимый многочлен. Тогда для элемента $x \in \mathbb{F}$ многочлен $a_n^{-1} * a(x)$ - минимальный.

Теорема Хэмминга. Пример построения кода Хэмминга.

Определение

Пусть n - длина кода, g - максимальное допустимое число ошибок.

Теорема Хэмминга

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

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{2*r}} \leq t \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r}}$$

Пример

Построим код Хэмминга длины 7. Выпишем таблицу: $n = 2^q - 1 \rightarrow q = 3, r = 1$ Матрица состоит из единичной матрицы, размерности $2^q - q - 1$ и матрицы из бинарных наборов(различных) длины q , содержащих не менее 2-х единиц.

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

Складывая строки произвольным образом (mod 2), получим 16 возможных сообщений. При их получении можно будет исправить одну ошибку.

Коды БЧХ: определение, примеры кодов с исправлением одной, двух и трех ошибок.

БЧХ коды - класс циклических кодов, исправляющих кратные (2 и более ошибок). БЧХ код задается порождающим полиномом. Для его построения необходимо задать длину кода и требуемое минимальное расстояние $d \leq n$.

Построение БЧХ кодов:

- Строим поле $\mathbb{F}_2^n = \mathbb{F}_2[x]/\langle f \rangle$, где f - неприводимый многочлен степени $n = 2^m - 1$.
- Выберем в циклической группе $\mathbb{F}_2^{n*}$ примитивный элемент $\alpha \in \mathbb{F}_2^{n*}$ и рассмотрим его степени: $\alpha, \alpha^2, \dots, \alpha^{2*r}$, где r - число ошибок, которые нужно исправить.
- В разложении многочлена $x^n - 1$ выберем такие неприводимые многочлены, чтобы каждая из указанных степеней была корнем одного из них (это не всегда возможно). Тогда:
 - ϕ есть результат перемножения этих многочленов
 - коды - коэффициенты многочленов из идеала (ϕ)
 - эти коды исправляют r ошибок

Пример кода, исправляющего 1 ошибку

Рассмотрим поле $\mathbb{F}_2^3 = \mathbb{F}_2[x]/(x^3 + x + 1)$, $r=3, m=2$. Многочлен $x^3 + x + 1$ - примитивный над $\mathbb{F}_2$. Порождающий полином $x^3 + x + 1$, т.к пусть α - его произвольный корень, тогда остальные корни α^2, α^4 и они входят в один смежный класс.

Пример кода, исправляющего 2 ошибки

Рассмотрим поле $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(x^{15} - 1)$. $\alpha, \alpha^2, \alpha^3, \alpha^4$

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

Пример кода, исправляющего 3 ошибки

$r = 3, m = 4, f(x) = x^{15} - 1$ Следовательно, нужно найти многочлены, корнями которых будут первые $2 * r = 6$ степеней порождающего элемента α

	если многочлен имеет корень	то у него есть корни
1	α	$\alpha^2, \alpha^4, \alpha^8$
2	α^3	$\alpha^2, \alpha^4, \alpha^8$
3	α^5	α^{10}

Перемножим полученные многочлены, получим многочлен 10-й степени. (первые 2 - четвертой, последний - второй). Идеал по модулю этого многочлена дает 5 степеней свободы, следовательно, построенный код будет 5-мерным пространством.

Понятие действия группы на множестве, фиксатор и стабилизатор. Примеры.

Гомоморфизм групп - Отображение групп $f : (G, *) \rightarrow (H, \times)$ такое, что $f(a * b) = f(a) \times f(b)$ для произвольных a и b в G .

Симметрической группой множества X называется группа всех перестановок X (то есть биекций $X \rightarrow X$) относительно

операции композиции.

Инверсная группа — построение в теории групп, сменяющее аргументы бинарной групповой операции местами, используемое для определения правого действия.

Действие слева

Говорят, что группа G действует слева на множестве M , если задан гомоморфизм $\Phi: G \rightarrow S(M)$ из группы G в симметрическую группу $S(M)$ множества M . Для краткости $(\Phi(g))(m)$ часто записывают как gm , $g \cdot m$ или $g.m$. Элементы группы G называются в этом случае *преобразованиями*, а сама группа G — **группой преобразований** множества M .

Другими словами, группа G действует на множестве M , если задано отображение $G \times M \rightarrow M$, обозначаемое $(g, m) \mapsto gm$, такое что

- $(gh)m = g(hm)$ для всех $g, h \in G, m \in M$ и
- $em = m$, где e — нейтральный элемент группы G . Можно сказать, что единица группы соотносит каждому элементу M его же; такое преобразование называется **тождественным**.

Действие справа

Аналогично, **правое действие** группы G на M задается гомоморфизмом $\rho: G^{op} \rightarrow S(M)$, где G^{op} — инверсия группы G . При этом часто используют сокращенное обозначение: $\rho(g)(m) =: mg$. При этом аксиомы гомоморфизма записываются следующим образом:

- $m(gh) = (mg)h$,
- $me = m$.

Комментарии

- Любое правое действие группы G — это левое действие группы G^{op} . Также, так как каждая группа изоморфна своей инверсной группе (изоморфизмом является, например, отображение $g \mapsto g^{-1}$), то из каждого правого действия можно с помощью такого изоморфизма получить левое действие. Поэтому, как правило, исследуются только левые действия.

Фиксатор

Зафиксируем перестановки и найдем все элементы множества, которые перестановка оставит на месте. Множество таких элементов - фиксатор. $Fix(g) = \{m \in M : g(m) = m\} \subseteq M$

Стабилизатор

Зафиксируем элементы и найдем все перестановки, которые оставляют данный элемент неподвижным. Множество таких перестановок - стабилизатор. $Stab(m) = \{g \in G : g(m) = m\} \subseteq G$

Лемма Бернсайда и её применение.

Подмножество

$$Gm = \{gm \mid g \in G\} \subset M$$

называется **орбитой** элемента $m \in M$.

Действие группы G на множестве M определяет на нём отношение эквивалентности

$$\forall n, m \in M (n \sim_G m) \iff (\exists g \in G : gn = m) \iff (Gn = Gm).$$

При этом классами эквивалентности являются орбиты элементов. Поэтому, если общее число классов эквивалентности равно k , то

$$M = Gm_1 \sqcup Gm_2 \sqcup \dots \sqcup Gm_k,$$

где $m_1, m_2, \dots, m_k \in M$ попарно неэквивалентны. Для транзитивного действия $k = 1$.

Лемма Бернсайда

Пусть G — конечная группа, действующая на множестве X . Для любого элемента g из G будем обозначать через $Fix(g)$ множество элементов X , оставляемых на месте g . Лемма Бёрнсайда даёт формулу числа орбит группы G , обозначаемого $C(G)$:

$$C(G) = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Пример

- Составляются слова длины $l \geq 2$ из алфавита $A = a_1, a_2, \dots, a_m$. Слова считаются эквивалентными, если они получаются одно из другого перестановкой крайних букв. Определить число S неэквивалентных слов.

Решение: Пусть T - множество слов длины l в алфавите A . $N = |T| = m^l$. Представим эквивалентности как орбиты некоторого действия подходящей группы G на T . Поскольку $g^2 = e$, то подходящей группой будет $G = \mathbb{Z}_2 = \{e, g\}$. Действие g переставляет в слове две крайние буквы. Число S неэквивалентных слов есть число классов эквивалентности $C(G)$ действия $\mathbb{Z}_2 : T$.

$$|Fix(e)| = |T| = m^l, |Fix(g)| = m^{l-2} * m = m^{l-1}$$

$$S = C(\mathbb{Z}_2) = \frac{1}{2} * \sum_{g \in G} |Fix(g)| = \frac{m^l + m^{l-1}}{2} = \frac{m^{l-1} * (m+1)}{2} l = 3, m = 2, S = 6$$

Цикловой индекс действия группы

Существует универсальный способ вычисления числа орбит $C(G) = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$. Сопоставим каждой перестановке $g \in \mathbb{G}$ вес $w(g)$ по правилу:

$$Type(g) = \leq v_1, v_2, v_3, \dots, v_n \geq \text{ где } v_i - \text{ количество циклов длины } i \text{ для перестановки } g. w(g) = x_1^{v_1} * \dots * x_n^{v_n}$$

Цикловой индекс группы G определяется как многочлен от n переменных $x_1, x_2, \dots, x_n$

$$P = \frac{1}{|G|} \sum_{g \in G} x_1^{v_1(g)} \cdot x_2^{v_2(g)} \cdot \dots \cdot x_n^{v_n(g)}$$

Группы симметрий правильных многоугольников (диэдральные группы) и группы вращений правильных многогранников. Примеры. Их цикловые индексы.

$D_3 = S_3$ (для треугольника = симметрической группе для 3 элементов)

Рассматривает многоугольник. Рассмотрим преобразования, которые его переводят в самого себя

- Отражения
- Повороты

Задача: группа октаэдра (не будет) только куб посчитать цикловой индекс

Вычислены цикловые индексы и есть формула для произвольного n (<http://mathworld.wolfram.com/DihedralGroup.html>)

Теорема Редфилда-Пойа и её применение

Цикловой индекс действия группы

Существует универсальный способ вычисления числа орбит $C(G) = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$. Сопоставим каждой перестановке $g \in \mathbb{G}$ вес $w(g)$ по правилу:

$$Type(g) = \langle v_1, v_2, v_3, \dots, v_n \rangle, \text{ где } v_i - \text{ количество циклов длины } i \text{ для перестановки } g. w(g) = x_1^{v_1} * \dots * x_n^{v_n}$$

Цикловой индекс группы G определяется как многочлен от n переменных $x_1, x_2, \dots, x_n$

$$P = \frac{1}{|G|} \sum_{g \in G} x_1^{v_1(g)} \cdot x_2^{v_2(g)} \cdot \dots \cdot x_n^{v_n(g)}$$

Теорема Редфилда-Пойа

К множеству $\mathbb{T}$, $|\mathbb{T}| = N$, группе $\mathbb{G}$, $|\mathbb{G}| = n$ и действию $\mathbb{G}\alpha : \mathbb{T}$ добавим множество $\mathbb{R} = \{c_1, c_2, \dots, c_r\}$ меток и совокупность функций $F = R^T$ приписывания элементам меток. $\mathbb{G}$, действуя на $\mathbb{T}$, действует и на R^T . Дадим вес элементам $\mathbb{R}$:

$$w(c_i) = y_i \forall i = 1, 2, \dots, r$$

Цикловой индекс действия группы G на R^T есть $W(F) = P(\mathbb{G}\alpha : R^T) = P(\mathbb{G}\alpha : T, x_1, x_2, \dots, x_N)$ причем $x_k = y_1^k + \dots + y_r^k$

Теорему Редфилда-Пойа можно использовать для вычисления числа разметок данного типа (содержащих данное количество элементов конкретного типа). Лемму Бернсайда можно использовать для вычисления общего количества неэквивалентных разметок.

Пример

Задача об ожерельях - 5 бусин, 3 цвета(красный, зеленый, синий). Ожерелья считаются одинаковыми, если они совпадают при их повороте или перевороте. Сколько существует различных ожерелий, содержащих 2 красные бусины?

$$x_1 = y_1 + y_2 + y_3, x_2 = y_1^2 + y_2^2 + y_3^2, \dots, x_k = y_1^k + y_2^k + y_3^k$$

$$w(\text{КРАСНЫЙ}) = y_1, w(\text{СИНИЙ}) = y_2, w(\text{ЗЕЛЕНый}) = y_3$$

$$y_1 = y, y_2 = y_3 = 1$$

$$x_1 = y + 2, x_2 = y^2 + 2, \dots, x_5 = y^5 + 2$$

$$P(x_1, x_2, \dots, x_5) = \frac{1}{10} * (x_1^5 + 4 * x_5 + 5 * x_1 * x_2^2) \text{ (было посчитано в простой задаче на ожерелья)}$$

$$P(y) = \sum_{i=1}^5 u_i * y^i$$

$$P(y) = \frac{1}{10} * (u_0 + u_1 * y + u_2 * y^2 + \dots + u_5 * y^5) = \frac{1}{10} * ((y + 2)^5 + 4 * (y^5 + 2) + 5 * (y + 2) * (y^2 + 2)^2)$$

$$P(y) = \frac{1}{10} * (\dots + (10 * 8 + 5 * 2 * 4) * y^2 + \dots) \rightarrow u_2 = 12$$

Идеалы и фильтры частично упорядоченного множества. Конусы. Точные грани.

Определение

Порядком, или **частичным порядком**, на множестве P называется бинарное отношение $\leq$ на P (определяемое некоторым множеством $R_{\leq} \subset M \times M$), удовлетворяющее следующим условиям

- *Рефлексивность*: $\forall a (a \leq a)$
- *Транзитивность*: $\forall a, b, c (a \leq b) \& (b \leq c) \Rightarrow a \leq c$
- *Антисимметричность*: $\forall a, b (a \leq b) \& (b \leq a) \Rightarrow a = b$

Частично упорядоченным множеством называется пара $\langle P, \leq \rangle$, где P — множество, а $\leq$ — отношение частичного порядка на P .

Идеал частично упорядоченного множества

Подмножество J элементов частично упорядоченного множества $\langle P, \leq \rangle$ называется его идеалом(порядковым), если:
 $(x \in J) \& (y \leq x) \rightarrow y \in J$

Фильтр частично упорядоченного множества

Подмножество F элементов P называется его фильтром(порядковым), если: $(x \in F) \& (x \leq y) \rightarrow y \in F$

Конус

Пусть $\langle P, \leq \rangle$ частично упорядоченное множество и $A \subseteq P$. Множества A^{Δ} и A^{∇} определяемые условиями:

- $A^{\Delta} = \{x \in P | \forall a \in A (a \leq x)\}$
- $A^{\nabla} = \{x \in P | \forall a \in A (x \leq a)\}$

называются верхними и нижними конусами множества A , а их элементы верхними и нижними гранями соответственно.

Точные грани

Пусть $\langle P, \varphi \rangle$ частично упорядоченное множество и $A \subseteq P$

- Наименьший элемент в A^{Δ} называется точной верхней гранью множества A .
- Наибольший элемент в A^{∇} называется точной нижней гранью множества A .

Теорема Шпильрайна. Линейное продолжение частично упорядоченного множества

Определение

- **Линейно упорядоченное множество** или **цепь** — частично упорядоченное множество, в котором для любых двух элементов a и b имеет место $a \leq b$ или $b \leq a$.
- **Линеаризация**.

Теорема Шпильрайна

- Любой частичный порядок $\leq$ может быть продлен до линейного на этом же множестве.
- Каждый порядок есть пересечение всех своих линейных продолжений (линеаризацией)

Спектр и размерность частично упорядоченного множества

Определение

Рассмотрим вероятностное пространство на множестве всех линейаризаций частично-упорядоченного множества $(P, \leq)$, в котором каждая линейаризация равновероятна. В этом пространстве рассматривают события E вида $x \leq y$, $(x \leq y) \& (x \leq z)$ и т.д.

Вероятность такого события $Pr[E] = \frac{\text{число линейаризаций, в которых имеет место } E}{e(P)}$

Спектр частично упорядоченного множества

$$Spec(P) = \{Pr[a \leq b] | a, b \in P, a \neq b\}$$

Свойства:

- спектр симметричен относительно $\frac{1}{2}$, поскольку $Pr[a \leq b] = 1 - Pr[b \leq a]$
- $\{0, \frac{1}{2}, 1\}$ - единственный трехэлементный спектр

Размерность

Наименьшее число линейных порядков, дающих в пересечении данное частично упорядоченное множество P , называется его размерностью $dim(P)$

Фундаментальная теорема о конечных дистрибутивных решётках.

Определения

Частично упорядоченное множество, для которого для любых двух элементов a, b существуют $Inf\{a, b\}$, $Sup\{a, b\}$ называют решеточно упорядоченным. Решетка называется полной, если любое подмножество ее элементов имеет точные верхнюю и нижнюю грани.

Решётка может быть также определена как алгебра с двумя бинарными операциями (они обозначаются $\vee$ и $\wedge$ или $+$ и $\cdot$), удовлетворяющая следующим тождествам

- $a \vee a = a$
 $a \wedge a = a$
- $a \vee b = b \vee a$
 $a \wedge b = b \wedge a$
- $(a \vee b) \vee c = a \vee (b \vee c)$
 $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
- $a \wedge (a \vee b) = a$
 $a \vee (a \wedge b) = a$

Связь между этими двумя определениями устанавливается при помощи формул:

$$a \vee b = \sup(a, b),$$
$$a \wedge b = \inf(a, b),$$

и обратно. При этом для любых элементов a и b эквивалентны следующие утверждения:

$$a \leq b;$$
$$a \wedge b = a;$$
$$a \vee b = b.$$

$Irr(L)$ - множество неразложимых в объединение элементов.

$Irr(x) = \{y \in Irr(L) | y \leq x\}$ - множество неразложимых элементов в L , содержащихся в x .

Фундаментальная теорема о конечных дистрибутивных решётках

Всякая конечная дистрибутивная решетка L изоморфна решетке порядковых идеалов частично упорядоченного множества ее неразложимых элементов $L = J(Irr(L))$

Соответствия Галуа.

Определения

Антимонотонность - $a, b \in P, a \leq b \rightarrow \phi(a) \geq \phi(b)$

Пусть P, Q - частично упорядоченные множества. Пара отображений $(\phi, \psi), \phi : P \rightarrow Q, \psi : Q \rightarrow P$, удовлетворяющих свойствам:

- ϕ, ψ антимонотонны.
- $p\phi\psi \geq p, q\psi\phi \geq q$ где $\phi\psi, \psi\phi$ операторы замыкания на P и Q соответственно.

называются соответствием Галуа между P и Q . Свойство: $\phi = \phi\psi\phi, \psi = \psi\phi\psi$

Источник — «http://bagnikita.dyndns.org/pa/index.php?title=Определения_All&oldid=178»

Категория: Определения

-
- Последнее изменение этой страницы: 22:18, 17 января 2014.
 - К этой странице обращались 3 раз.
 - Содержимое доступно по лицензии Общественное достояние (если не указано иное).