МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Институт прикладной математики и компьютерных наук
Кафедра «Прикладная математика и информатика»

Утверждено на заседании кафедры
«Прикладная математика и информатика»
24 января 2022 г., протокол № 5

Заведующий кафедрой

_____М.В. Грязев

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по проведению практических занятий по дисциплине (модулю) «Прикладная алгебра»

основной профессиональной образовательной программы высшего образования – программы бакалавриата

по направлению подготовки
01.03.02 Прикладная математика и информатика

с направленностью (профилем)
Прикладная математика и информатика

Форма обучения: очная

Идентификационный номер образовательной программы: 010302-01-22

Тула 2022 год

Разработчик методических указаний

Иванов В.И., профессор каф. ПМиИ, д.ф.-м.н., профессор 

(ФИО, должность, ученая степень, ученое звание) *(подпись)*

I. Цели и задачи практических занятий

Целью освоения дисциплины «Прикладная алгебра» является получение новых знаний по теории матриц, теории конечных полей и по их применениям в численных методах и теории кодирования.

Задачами дисциплины являются:

- изучение основных понятий, определений и утверждений теории матриц, теории конечных полей,
- приобретение навыков решения практических задач по теории матриц, теории конечных полей,
- знакомство с применением теории матриц, теории конечных полей в численных методах и теории кодирования.

Целями и задачами практических занятий по прикладной алгебре являются приобретение навыков решения практических задач по теории матриц, теории конечных полей, построению БЧХ-кодов и закрепление основных понятий, определений и свойств объектов прикладной алгебры.

№ занятия	№ раздела	Тема	Кол-во часов
	1	**Матрицы и их применение**	16
1,2	1.2	Теория Фредгольма для СЛАУ.	4
3,4	1.3	Нормальное решение, псевдорешение СЛАУ. Псевдообратная матрица.	4
5.6	1.4,1.5	LU-разложения матрицы. QR-разложение матрицы.	4
7,8	1.6,1.7	Сингулярное и полярное разложения матрицы. Возмущения СЛАУ. Число обусловленности.	4
	2	**Алгебраическая теория кодирования**	**16**
9,10	2.1	Алгоритм Евклида. Обратные элементы в Z_p	4
11,12	2.2	Алгоритм Евклида в кольце многочленов **F**[x] . Неприводимые многочлены в $Z_p[x]$	4
13,14	2.3,2.4	Алгебраическая структура конечного поля. Изоморфизм конечных полей.	4
15,16	2.5,2.6	Линейные двоичные коды. Код Хемминга. Построение циклических кодов.	4

II. Методические указания к проведению практических занятий

Занятия 1, 2
Теория Фредгольма для СЛАУ

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

Пусть матрица $A=\begin{pmatrix} 3/2 & -1/2 \\ -1/2 & 3/2 \end{pmatrix}$. Рассматривается система линейных уравнений $(E-\lambda A)x=y$. При каких λ система имеет единственное решение для любого y? При каких λ и y система имеет бесконечно много решений? При каких λ и y решений нет?

Решение

Для решения задачи воспользуемся теорией Фредгольма. Для этого запишем 4 системы:

$$1)\ (E-\lambda A)x=y,$$
$$2)\ (E-\lambda A)x=0,$$
$$3)\ (E-\lambda A^T)x=y,$$
$$4)\ (E-\lambda A^T)x=0.$$

Здесь A^T - транспонированная матрица. Теория Фредгольма сводится к трем утверждениям:

Теорема 1. Следующие четыре условия эквивалентны:

а) система 1) имеет решение (единственное) при любой правой части у;

б) система 2) имеет только нулевое решение;

в) система 3) имеет решение (единственное) при любой правой части у;

г) система 4) имеет только нулевое решение.

Эквивалентность первого и четвертого утверждений известна, как альтернатива Фредгольма: либо система 1) имеет единственное решение для любой правой части, либо система 4) имеет не нулевое решение.

Теорема 2. Системы 2), 4) имеют одинаковое число линейно независимых решений.

Теорема 3. Система 1) имеет хотя бы одно решение тогда и только тогда, когда правая часть у ортогональна всем решениям уравнения 4).

Исследуем систему 4). Так как $A^T=A$, то оно запишется в следующем виде

$$\begin{cases}(1-\frac{3}{2}\lambda)x_1+\frac{1}{2}\lambda x_2=0\\ \frac{1}{2}\lambda x_1+(1-\frac{3}{2}\lambda)x_2=0.\end{cases}$$

Эта система имеет ненулевое решение только в случае, когда

$$\begin{vmatrix}1-\frac{3}{2}\lambda & \frac{1}{2}\lambda\\ \frac{1}{2}\lambda & 1-\frac{3}{2}\lambda\end{vmatrix}=0.$$

Вычисляя определитель, получим квадратное уравнение $2\lambda^2-3\lambda+1=0.$ Его корни

$$\lambda_1=1,\lambda_2=\frac{1}{2}.$$

Таким образом, при $\lambda\neq 1,\frac{1}{2}$ система 1) имеет единственное решение для любой правой части y.

Если $\lambda=1$, то система 4) сводится к одному уравнению $x_1-x_2=0$. Оно имеет одно линейно независимое решение $(1,1)$. По теоремам 1, 3 при $\lambda=1$ и $y\perp(1,1)$ система 1) имеет бесконечно много решений, а при $\lambda=1$ и y, не ортогональном вектору $(1,1)$, не имеет решений.

Пусть теперь $\lambda=\frac{1}{2}$. В этом случае система 4) сводится к уравнению $x_1+x_2=0.$ Оно имеет одно линейно независимое решение $(1,-1)$. По теоремам 1, 3 при $\lambda=\frac{1}{2}$ и $y\perp(1,-1)$ система 1) имеет бесконечно много решений, а при $\lambda=\frac{1}{2}$ и y, не ортогональном вектору $(1,-1)$, не имеет решений.

Задачи для самостоятельного решения

1. Пусть матрица $A=\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}$. Рассматривается система линейных уравнений $(E-\lambda A)x=y$. При каких λ система имеет единственное решение для любого y? При каких λ и y система имеет бесконечно много решений? При каких λ и y решений нет?

2. Пусть матрица $A=\begin{pmatrix}3 & -2\\ -2 & 3\end{pmatrix}$. Рассматривается система линейных уравнений $(E-\lambda A)x=y$. При каких λ система имеет единственное решение для любого y? При каких λ и y система имеет бесконечно много решений? При каких λ и y решений нет?

Домашнее задание

1. Пусть матрица $A=\begin{pmatrix} 2 & -4 \\ -4 & 2 \end{pmatrix}$. Рассматривается система линейных уравнений $(E-\lambda A)x=y$. При каких λ система имеет единственное решение для любого y? При каких λ и y система имеет бесконечно много решений? При каких λ и y решений нет?

2. Пусть матрица $A=\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. Рассматривается система линейных уравнений $(E-\lambda A)x=y$. При каких λ система имеет единственное решение для любого y? При каких λ и y система имеет бесконечно много решений? При каких λ и y решений нет?

Занятия 3, 4
Нормальное решение, псевдорешение СЛАУ. Псевдообратная матрица

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

Пусть матрица $A=\begin{pmatrix} 2 & -1 \\ -2 & 1 \end{pmatrix}$. Рассматривается система $Ax=y$. Проверить, что однородная сопряженная система имеет не нулевые решения. Для $y=(1,-1)$, при котором система имеет решение, описать все решения и среди них выделить нормальное решение. Для $y=(1,1)$, при котором система не имеет решения, описать все псевдорешения и среди них выделить нормальное псевдорешение. Записать пседообратную матрицу.

Решение

Сопряженная однородная система имеет вид

$$\begin{cases} 2x_1-2x_2=0 \\ -x_1+x_2=0. \end{cases}$$

Она эквивалентна одному уравнению $x_1-x_2=0$. Оно имеет одно линейно независимое решение $(1,1)$. Поэтому для правой части $y=(1,-1)$ исходная система имеет решения, а для $y=(1,1)$ - нет. Для правой части $y=(1,-1)$ исходная система эквивалентна одному уравнению $2x_1-x_2=1$. Его общее решение имеет вид

$$\begin{cases} x_1 = \dfrac{1+t}{2} \\ x_2 = t, \end{cases}$$

где $t \in \mathbb{R}$. Функция $f(t) = x_1^2 + x_2^2 = \left(\dfrac{1+t}{2}\right)^2 + t^2$ имеет минимум при $t = -\frac{1}{5}$, поэтому нормальное решение имеет вид

$$\begin{cases} x_1 = \dfrac{2}{5} \\ x_2 = \dfrac{-1}{5}. \end{cases}$$

При $y = (1,1)$ система $Ax = y$ решений не имеет. Ее псевдорешения – это решения системы $A^T Ax = A^T y$. Она всегда имеет решение. Решим эту систему для произвольного $y = (y_1, y_2)$. Система запишется так

$$\begin{cases} 8x_1 - 4x_2 = 2y_1 - 2y_2 \\ -4x_1 + 2x_2 = -y_1 + y_2 \end{cases}.$$

Система сводится к одному уравнению $4x_1 - 2x_2 = y_1 - y_2$. Его общее решение имеет вид

$$\begin{cases} x_1 = \dfrac{y_1 - y_2}{4} + t \\ x_2 = 2t. \end{cases}$$

При $y = (1,1)$ псевдорешения выглядят так

$$\begin{cases} x_1 = t \\ x_2 = 2t. \end{cases}$$

Рассмотрим функцию $f(t) = x_1^2 + x_2^2 = \left(\dfrac{y_1 - y_2}{4} + t\right)^2 + 4t^2$. Она имеет минимум при $t = -\dfrac{y_1 - y_2}{20}$. Тогда нормальные пседорешения будут равны

$$\begin{cases} x_1 = \dfrac{y_1 - y_2}{5} \\ x_2 = -\dfrac{y_1 - y_2}{10}. \end{cases}$$

Если $y = (1,1)$, то нормальное псевдорешение запишется так

$$\begin{cases} x_1 = 0 \\ x_2 = 0. \end{cases}$$

Остается записать псевдообратную матрицу

$$A^+ = \begin{pmatrix} \dfrac{1}{5} & \dfrac{-1}{5} \\ \dfrac{-1}{10} & \dfrac{1}{10} \end{pmatrix} = \frac{1}{10} A^T.$$

Отметим, что нормальное решение для $y=(1,-1)$ и нормальное псевдорешение для $y=(1,1)$ получаются путем умножения на псевдообратную матрицу.

Задачи для самостоятельного решения

1. Пусть матрица $A=\begin{pmatrix}1 & -2\\ -1 & 2\end{pmatrix}$. Рассматривается система $Ax=y$. Проверить, что однородная сопряженная система имеет не нулевые решения. Для $y=(1,-1)$, при котором система имеет решение, описать все решения и среди них выделить нормальное решение. Для $y=(1,1)$, при котором система не имеет решения, описать все псевдорешения и среди них выделить нормальное псевдорешение. Записать пседообратную матрицу.

2. Пусть матрица $A=\begin{pmatrix}3 & 1\\ -3 & -1\end{pmatrix}$. Рассматривается система $Ax=y$. Проверить, что однородная сопряженная система имеет не нулевые решения. Для $y=(1,-1)$, при котором система имеет решение, описать все решения и среди них выделить нормальное решение. Для $y=(1,1)$, при котором система не имеет решения, описать все псевдорешения и среди них выделить нормальное псевдорешение. Записать пседообратную матрицу.

Домашнее задание

1. Пусть матрица $A=\begin{pmatrix}2 & -3\\ -2 & 3\end{pmatrix}$. Рассматривается система $Ax=y$. Проверить, что однородная сопряженная система имеет не нулевые решения. Для $y=(1,-1)$, при котором система имеет решение, описать все решения и среди них выделить нормальное решение. Для $y=(1,1)$, при котором система не имеет решения, описать все псевдорешения и среди них выделить нормальное псевдорешение. Записать пседообратную матрицу.

2. Пусть матрица $A=\begin{pmatrix}1 & 2\\ -1 & -2\end{pmatrix}$. Рассматривается система $Ax=y$. Проверить, что однородная сопряженная система имеет не нулевые решения. Для $y=(1,-1)$, при котором система имеет решение, описать все решения и среди них выделить нормальное решение. Для $y=(1,1)$, при котором система не имеет решения, описать все псевдорешения и среди них выделить нормальное псевдорешение. Записать пседообратную матрицу.

Занятия 5, 6
LU и QR-разложения матрицы

План занятия

1. Повторение теоретического материала

2. Подробное решение типоой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

1. Для матрицы $A=\begin{pmatrix}1 & -1\\ 1 & 2\end{pmatrix}$ получить LU-разложение, где L - нижняя треугольная матрица, а U - верхняя треугольная матрица.

Решение

Такое разложение возможно для квадратной матрицы порядка m, если все ведущие миноры порядков $1,\ldots,\ m-1$ отличны от нуля. В нашем случае

$$A\begin{pmatrix}1\\ 1\end{pmatrix}=1, A\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}=3.$$

Если l_{ij} - элементы матрицы L, а u_{ij} - элементы матрицы U, то $l_{12}=0, u_{21}=0.$

Справедливы формулы

$$l_{11}u_{11}=A\begin{pmatrix}1\\ 1\end{pmatrix}, l_{22}u_{22}=\frac{A\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}}{A\begin{pmatrix}1\\ 1\end{pmatrix}}, l_{21}=l_{11}\frac{A\begin{pmatrix}2\\ 1\end{pmatrix}}{A\begin{pmatrix}1\\ 1\end{pmatrix}}, u_{12}=u_{11}\frac{A\begin{pmatrix}1\\ 2\end{pmatrix}}{A\begin{pmatrix}1\\ 1\end{pmatrix}}.$$

Если $l_{11}=l_{22}=1$, то $u_{11}=1, u_{22}=3, l_{21}=1, u_{12}=-1.$ Таким образом искомое разложение имеет вид

$$A=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 3\end{pmatrix}.$$

Простым перемножением убеждаемся в справедливости полученного разложения.

Типовая задача

2. Для матрицы $A=\begin{pmatrix}1 & -1\\ 1 & 2\end{pmatrix}$ получить QR-разложение, где Q - унитарная (ортогональная) матрица, а R - верхняя треугольная матрица.

Решение

Ортогональная матрица второго порядка имеет вид

$$O=\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}.$$

Вычислим произведение OA

$$OA=\begin{pmatrix}\cos\alpha-\sin\alpha & -\cos\alpha-2\sin\alpha\\ \cos\alpha+\sin\alpha & -\sin\alpha+2\cos\alpha\end{pmatrix}.$$

Потребуем, чтобы $\cos\alpha+\sin\alpha=0$. Можно положить $\cos\alpha=\frac{1}{\sqrt{2}}, \sin\alpha=-\frac{1}{\sqrt{2}}$. Тогда

$$O=\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix},\ OA=\begin{pmatrix} \sqrt{2} & \frac{1}{\sqrt{2}} \\ 0 & \frac{3}{\sqrt{2}} \end{pmatrix}.$$

Так как $O^{-1}=O^T$, то полагаем $Q=O^{-1}=O^T$ и получаем искомое разложение

$$A=\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} \sqrt{2} & \frac{1}{\sqrt{2}} \\ 0 & \frac{3}{\sqrt{2}} \end{pmatrix}.$$

Задачи для самостоятельного решения

1. Для матрицы $A=\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ получить LU-разложение.
2. Для матрицы $A=\begin{pmatrix} 1 & -1 \\ 1 & 3 \end{pmatrix}$ получить LU-разложение.
3. Для матрицы $A=\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ получить QR-разложение.
4. Для матрицы $A=\begin{pmatrix} 1 & -1 \\ 1 & 3 \end{pmatrix}$ получить QR-разложение.

Домашнее задание

1. Для матрицы $A=\begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$ получить LU-разложение.
2. Для матрицы $A=\begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}$ получить LU-разложение.
3. Для матрицы $A=\begin{pmatrix} 3 & -1 \\ 1 & 1 \end{pmatrix}$ получить QR-разложение.
4. Для матрицы $A=\begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}$ получить QR-разложение.

Занятия 7, 8
Сингулярное и полярное разложения матрицы. Возмущения СЛАУ. Число обусловленности

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи

3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

1. Для матрицы $A=\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ найти сингулярные числа и получить сингулярное и полярное разложения.

Решение

Сингулярные числа матрицы A - это квадратные корни из собственных значений матрицы

$$A^TA=\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}.$$

Таким образом, сингулярные числа равны $\rho_1=\rho_2=\sqrt{2}$. Сингулярное разложение матрицы имеет вид $A=U\Lambda V$, где U,V - ортогональные матрицы,

$$\Lambda=\begin{pmatrix}\sqrt{2} & 0\\ 0 & \sqrt{2}\end{pmatrix}$$

- диагональная матрица с сингулярными числами на главной диагонали. Матрицы U,V строятся с помощью сингулярных базисов. Матрица A^TA - симметричная и у нее существует ортонормированный базис из собственных векторов. В нашем случае это $e_1=(1,0),e_2=(0,1).$ Он образует первый сингулярный базис. Второй сингулярный ортонормированный базис образуют векторы

$$l_1=\frac{1}{\rho_1}Ae_1=(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}),l_2=\frac{1}{\rho_2}Ae_2=(-\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}).$$

Столбцы матрицы U образуют координаты второго сингулярного базиса, а столбцы матрицы V^T - первого сингулярного базиса. Имеем

$$U=\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix},V=V^T=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

Поэтому сингулярное разложение матрицы A имеет вид

$$A=U\Lambda V=U=\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\sqrt{2} & 0\\ 0 & \sqrt{2}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

Полярное разложение матрицы A - это ее представление в виде произведения $A=HO$, где H - эрмитова (симметричная) матрица, а O - ортогональная матрица. Его можно получить из сингулярного разложения: $H=U\Lambda U^T,O=UV.$ Итак, полярное разложение имеет вид

$$A=\begin{pmatrix}\sqrt{2} & 0\\ 0 & \sqrt{2}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}.$$

Типовая задача

2. Для матрицы $A=\begin{pmatrix}1 & -2\\ 0 & 1\end{pmatrix}$ найти число обусловленности, используя евклидову, спектральную, 1- норму и ∞-норму матрицы.

Решение

Для матрицы $A=(a_{ij})$ евклидова норма вычисляется по формуле $\|A\|_E=\sqrt{\sum_i\sum_j a_{ij}^2}$, спектральная норма $\|A\|$ - набольшее сингулярное число, 1-норма вычисляется по формуле $\|A\|_1=\max_j\sum_i|a_{ij}|$, ∞-норма вычисляется по формуле $\|A\|_\infty=\max_i\sum_j|a_{ij}|$. Число обусловленности матрицы ν равно произведению норм матрицы и ее обратной матрицы. Легко убедиться, что

$$A^{-1}=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix},$$

поэтому $\|A\|_E=\|A^{-1}\|_E=\sqrt{6}$, $\|A\|_1=\|A^{-1}\|_1=3$, $\|A\|_\infty=\|A^{-1}\|_\infty=3$ и $\nu_E=6$, $\nu_1=\nu_\infty=9$. Матрица

$$A^TA=\begin{pmatrix}1 & -2\\ -2 & 5\end{pmatrix}.$$

Ее собственные значения являются корнями уравнения

$$\begin{vmatrix}1-\lambda & -2\\ -2 & 5-\lambda\end{vmatrix}=0.$$

Они равны $3\pm2\sqrt{2}$, поэтому наибольшее сингулярное число матрицы A $\rho(A)=\sqrt{3+2\sqrt{2}}$. Аналогично

$$(A^{-1})^TA^{-1}=\begin{pmatrix}5 & 2\\ 2 & 1\end{pmatrix},\ \rho(A^{-1})=\sqrt{3+2\sqrt{2}}\ .$$

Отсюда $\|A\|=\|A^{-1}\|=\sqrt{3+2\sqrt{2}}$ и $\nu=3+2\sqrt{2}$ - это наименьшее число обусловленности.

Задачи для самостоятельного решения

1. Для матрицы $A=\begin{pmatrix}1 & -1\\ 1 & 2\end{pmatrix}$ найти сингулярные числа и получить сингулярное и полярное разложения.

2. Для матрицы $A=\begin{pmatrix}2 & -1\\ 1 & 1\end{pmatrix}$ найти сингулярные числа и получить сингулярное и полярное разложения.

3. Для матрицы $A=\begin{pmatrix}1 & -1\\ 1 & 2\end{pmatrix}$ найти число обусловленности, используя евклидову, спектральную, 1- норму и ∞-норму матрицы.

4. Для матрицы $A=\begin{pmatrix}2 & -1\\ 1 & 1\end{pmatrix}$ найти число обусловленности, используя евклидову, спектральную, 1- норму и ∞-норму матрицы.

Домашнее задание

1. Для матрицы $A=\begin{pmatrix}2 & 1\\ -1 & 2\end{pmatrix}$ найти сингулярные числа и получить сингулярное и полярное разложения.

3. Для матрицы $A=\begin{pmatrix}1 & -1\\ 1 & 3\end{pmatrix}$ найти число обусловленности, используя евклидову, спектральную, 1- норму и ∞-норму матрицы.

4. Для матрицы $A=\begin{pmatrix}2 & 1\\ -1 & 2\end{pmatrix}$ найти число обусловленности, используя евклидову, спектральную, 1- норму и ∞-норму матрицы.

Занятие 9, 10
Алгоритм Евклида. Обратные элементы в Zp

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

1. Найти наибольший общий делитель d чисел a и b и его представление в форме

$$d = u\cdot a + v\cdot b \quad (u,v\in\mathbb{Z}), \tag{1}$$

если $a = 420, b = 4752.$

Решение

Используя вычислительную схему алгоритма Евклида, получаем следующую таблицу:

m	n	u'	v'	u	v	Деление	q
4752	420	1	0	0	1	$4752=11\cdot 420+132$	11
420	132	0	1	1	-11	$420=3\cdot 132+24$	3
132	24	1	-11	-3	34	$420=5\cdot 24+12$	5
24	12	-3	34	16	-181	$24=2\cdot 12$	конец

Последнее значение переменной n и есть наибольший общий делитель:

$$(4752, 420)=12,$$

и представление его в форме (1) имеет вид

$$12=16\cdot 4752+ (-181)\cdot 420.$$

Типовая задача

2. В поле $\mathbb{Z}_{569}$ найти элемент, обратный к 52.

Решение

Число 569 – простое, поэтому для любого x от 1 до 568 $(x, 569)=1$. Найдя с помощью вычислительной схемы алгоритма Евклида представление

$$1=u\cdot 569+ v\cdot x,$$

Получим, согласно определению операций в поле $\mathbb{Z}_{569}$, **что** $v\cdot x=1$, то есть $v = x^{-1}$. Вычисления сведены в таблицу:

m	n	u'	v'	u	v	Деление	q
569	52	1	0	0	1	$569=10\cdot 52+49$	10
52	49	0	1	1	-10	$52=1\cdot 49+3$	1
49	3	1	-10	-1	11	$49=16\cdot 3+1$	16
3	1	-1	11	17	-186	$3=3\cdot 1$	конец

$$1=17\cdot 569+ (-186)\cdot 52, \qquad 52^{-1} = -186 - 383 (\mathrm{mod}\, 569).$$

Задачи для самостоятельного решения

1. Найти наибольший общий делитель d чисел a и b и его представление в форме

$$d = u \cdot a + v \cdot b \quad (u, v \in \mathbb{Z}),$$

если

1) $a = 308, b = 7154$**, 2)** $a = 840, b = 17952.$

2. В поле $\mathbb{Z}_{677}$ найти элемент, обратный к 123.

3. В поле $\mathbb{Z}_{673}$ найти элемент, обратный к 100.

Домашнее задание

1. Найти наибольший общий делитель d чисел a и b и его представление в форме

$$d = u \cdot a + v \cdot b \quad (u, v \in \mathbb{Z}),$$

если

1) $a = 560, b = 4488$**, 2)** $a = 280, b = 8976.$

2. В поле $\mathbb{Z}_{661}$ найти элемент, обратный к 102.

3. В поле $\mathbb{Z}_{659}$ найти элемент, обратный к 23.

Занятия 11,12
Алгоритм Евклида в кольце многочленов F[x]. Неприводимые многочлены в Zp[x]

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

1. Найти наибольший общий делитель $d(x)$ многочленов $a(x)$ и $b(x)$ из кольца $\mathbb{Z}[x]$ и его представление в форме

$$d(x) = u(x) \cdot a(x) + v(x) \cdot b(x), \quad (u(x), v(x) \in \mathbb{Z}[x]),$$

если $a(x) = x^4 - 3x^2 - 4$, $b(x) = x^3 + x^2 + 4.$

Решение

Так как правила сложения и умножения для многочленов те же самые, что и для целых чисел (аксиомы кольца), решение этой задачи ничем не отличается от предыдущей.

Начальная установка:

$$m(x) = x^4 - 3x^2 - 4,\ n(x) = x^3 + x^2 + 4,$$

$$u(x) = 1, v(x) = 0\ ,\ u_1(x) = 0,\ v_1(x) = 1.$$

Деление:

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

Пересчет 6 величин:

$$m(x) = x^3 + x^2 + 4,\ n(x) = -2x^2 - 4x\ ,$$

$$u(x) = 0\ ,\ v(x) = 1,\ u_1(x) = 1,\ v_1(x) = -x + 1.$$

Заметим, что по определению наибольшего общего делителя многочленов его старший коэффициент равен единице. Поэтому, если многочлены умножать на константы (элементы основного поля, в данном примере поля Q рациональных чисел), то их наибольший общий делитель не меняется. Например, в нашем случае

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

На основании этого изменим вычислительную схему следующим образом: при появлении остатка, старший коэффициент которого не равен 1, при пересчете на следующий шаг разделим остаток на старший коэффициент. Очевидно, что при этом на то же число надо разделить многочлены $u_1(x)$ и $v_1(x)$.

С учетом этого замечания, продолжим вычисления со следующими 6 многочленами:

$$m(x) = x^3 + x^2 + 4, n(x) = x^2 + 2x,$$

$$u(x) = 0,\ v(x) = 1,\ u_1(x) = -1/2,\ v_1(x) = -(1/2)x - 1/2.$$

(Многочлены $n(x)$, $u_1(x)$, $v_1(x)$ поделены на -2.)

Деление:

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

Пересчет 6 величин:

$$m(x) = x^2 + 2x, n(x) = 2x + 4, u(x) = -1/2,$$

$$v(x) = (1/2)x - 1/2,\ u_1(x) = (1/2)x - 1/2,\ v_1(x) = -(1/2)x^2 + x + 1/2.$$

Деление на старший коэффициент:

$$m(x) = x^2 + 2x, n(x) = x + 2, u(x) = -1/2,$$

$$v(x) = (1/2)x - 1/2,\ u_1(x) = (1/4)x - 1/4,\ v_1(x) = -(1/4)x^2 + (1/2)x + 1/4.$$

При следующем делении $x^2 + 2x = x(x+2)$ получаем нулевой остаток. Следовательно,

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

Типовая задача

2. В кольце многочленов $\mathbb{Z}_3[x]$ найти все неприводимые многочлены третьей степени.

Решение

Элементы поля $\mathbb{Z}_3 = \{0,1,2\}$ будем обозначать $\mathbb{Z}_3 = \{0,1,-1\}$, так как $2 = -1 (\mathrm{mod}\, 3)$. Многочлен 3-й степени имеет вид

$$p(x) = a_3x^3 + a_2x^2 + a_1x + a_0,$$

где $a_i \in \mathbb{Z}_3$ и $a_3 \neq 0$. Так как многочлены, получающиеся один из другого умножением на не нулевую константу (то есть на -1), естественно не различать, то будем считать, что $a_3 = 1$.. Если $a_0 = 0$, то многочлен разложим

$$p(x) = x^3 + a_2\,x^2 + a_1\,x = (x^2 + a_2\,x + a_1)\cdot x,$$

поэтому $a_0 = \pm 1$.

Итак, будем далее рассматривать многочлены вида

$$p(x) = x^3 + a_2\,x^2 + a_1\,x \pm 1. \qquad (2)$$

Нетрудно подсчитать, что таких многочленов 18 штук. Чтобы выбрать среди них неприводимые, заметим, что если многочлен 3-й степени приводим, то он представляется в виде произведения многочленов 1-й и 2-й степени:

$$x^3 + a_2\,x^2 + a_1\,x + a_0 = (x+b)(x^2 + b_2\,x + b_1).$$

в этом случае число $-b$ будет корнем многочлена. Обратно, если многочлен 3-й степени имеет корень c в поле $\mathbb{Z}_3$, то он по теореме Безу делится на $x-c$ и, следовательно, приводим. Таким образом, из 18 многочленов вида (2) надо отбросить те, которые имеют корень в поле $\mathbb{Z}_3$. Так как $a_0 \neq 0$, то 0 не является корнем этих многочленов и будем далее проверять только ± 1. Разделим 18 многочленов на два класса: с $a_0 = 1$ и с $a_0 = -1$.

$$1.\ p(x) = x^3 + a_2x^2 + a_1x + 1. \qquad (3)$$

Для многочленов вида (3), имеющих корень $x = 1$, имеем

$$1 + a_2 + a_1 + 1 = 0 \text{ или } a_1 + a_2 = 1.$$

Этому условию удовлетворяют следующие пары (a_2, a_1):

$$(1,0), (0,1), (-1,-1) \qquad (4)$$

Для многочленов вида (3), имеющих корень $x = -1$, имеем

$$-1 + a_2 - a_1 + 1 = 0 \text{ или } a_2 = a_1.$$

Этому условию удовлетворяют следующие пары (a_2, a_1):

$$(0,0), (1,1), (-1,-1). \qquad (5)$$

$$2.\ p(x)=x^3+a_2x^2+a_1x-1 \qquad (6)$$

Для многочленов вида (6), имеющих корень $x=1$, имеем

$$1+a_2+a_1-1=0 \text{ или } a_2=-a_1.$$

Этому условию удовлетворяют следующие пары (a_2,a_1):

$$(0,0),(1,-1),(-1,1). \qquad (7)$$

Для многочленов вида (6), имеющих корень $x=-1$, имеем

$$-1+a_2-a_1-1=0 \text{ или } a_2-a_1=-1.$$

Этому условию удовлетворяют следующие пары (a_2,a_1):

$$(0,1),(1,-1),(-1,0). \qquad (8)$$

Отбрасывая многочлены, коэффициенты которых встречаются в списках (4), (5) и (7), (8), получаем следующие 8 неприводимых многочленов

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

Задачи для самостоятельного решения

1. Найти наибольший общий делитель $d(x)$ многочленов $a(x)$ и $b(x)$ из кольца $\mathbb{Q}[x]$ и его представление в форме

$$d(x)=u(x)\cdot a(x)+v(x)\cdot b(x),\ \ (u(x),v(x)\in\mathbb{Q}[x]),$$

если

$$1)\ a(x)=x^6+1,\ b(x)=x^4+1,\quad 2)\ a(x)=x^4+x^2+1,\ b(x)=x^2-x-1.$$

2. В кольце многочленов $\mathbb{Z}_3[x]$ найти все неприводимые многочлены второй степени.

3. В кольце многочленов $\mathbb{Z}_{19}[x]$ найти все неприводимые многочлены второй степени, имеющие вид x^2+a.

Домашнее задание

1. Найти наибольший общий делитель $d(x)$ многочленов $a(x)$ и $b(x)$ из кольца $\mathbb{Q}[x]$ и его представление в форме

$$d(x)=u(x)\cdot a(x)+v(x)\cdot b(x),\ \ (u(x),v(x)\in\mathbb{Q}[x]),$$

если

$$1)\ a(x)=x^3+1,\ b(x)=x^4-1,\quad 2)\ a(x)=x^6+1,\ b(x)=x^4-1.$$

2. В кольце многочленов $\mathbb{Z}_2[x]$ найти все неприводимые многочлены пятой степени.

3. В кольце многочленов $\mathbb{Z}_{11}[x]$ найти все неприводимые многочлены четвертой степени, имеющие вид $x^4 + a$.

Занятие 13, 14
Алгебраическая структура конечного поля. Изоморфизм конечных полей

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

1. Для поля $\mathbb{Z}_5(\alpha), \alpha^2 = 3$ 1) найти примитивный элемент и записать все элементы как степени примитивного; 2) определить мультипликативные порядки всех элементов; 3) найти для каждого элемента его минимальный многочлен; 4) решить систему $(1+\alpha)x - y = 1, -x + \alpha y = 1 + \alpha.$

Решение

Поле состоит из 25 элементов вида $a + b\alpha$, где a и b - элементы $\mathbb{Z}_5 = \{-2, -1, 0, 1, 2\}$. Эти элементы складываются и умножаются как многочлены от α, при умножении α^2 заменяется на $3 = -2$.

1) Согласно главной структурной теореме в каждом конечном поле имеется примитивный элемент, степени которого дают все ненулевые элементы поля. Этот элемент, таким образом, имеет мультипликативный порядок, равный 24; наоборот, любой элемент 24-го порядка является примитивным. Порядки остальных элементов являются делителями 24, то есть могут равняться 1,2,3,4,6,8 или 12.

Элемент α, при помощи которого построено поле, примигивным не является, так как

$$\alpha^2 = -2, \alpha^4 = (-2)^2 = 4 = -1, \alpha^8 = (-1)^2 = 1.$$

Отсюда следует, что α – элемент 8-го порядка.

Эффективного способа отыскания в конечном поле примитивного элемента не известно. Приходится перебирать элементы, выясняя их порядок. Рассмотрим, например, элемент $\beta = \alpha + 1$. Имеем

$$\beta^2 = 1 + 2\alpha + \alpha^2 = -1 + 2\alpha,$$
$$\beta^3 = (-1 + 2\alpha)(1 + \alpha) = -1 + \alpha - 4 = \alpha,$$

то есть $ord(\beta^3) = ord(\alpha) = 8$. Пусть порядок $ord(\beta) = n$. Так как $ord(\beta^3) = \frac{n}{(n,3)}$, то $n = 24$, то есть β - примитивный элемент. В таблице ненулевые элементы выражены как степени β.

Поле $Z_5(\alpha), \alpha^2 = -2$

β^k	Элемент поля	β^k	Элемент поля	β^k	Элемент поля	β^k	Элемент поля
β^0	1	β^6	-2	β^{12}	-1	β^{18}	2
β^1	$1+\alpha$	β^7	$-2-2\alpha$	β^{13}	$-1-\alpha$	β^{19}	$2+2\alpha$
β^2	$-1+2\alpha$	β^8	$2+\alpha$	β^{14}	$1-2\alpha$	β^{20}	$-2-\alpha$
β^3	α	β^9	-2α	β^{15}	$-\alpha$	β^{21}	2α
β^4	$-2+\alpha$	β^{10}	$-1-2\alpha$	β^{16}	$2-\alpha$	β^{22}	$1+2\alpha$
β^5	$1-\alpha$	β^{11}	$-2+2\alpha$	β^{17}	$-1+\alpha$	β^{23}	$2-2\alpha$

2) Порядок элемента β^k равен $\frac{24}{(24,k)}$. Отсюда находим

элементы 1-го порядка: β^0;
элементы 2-го порядка: β^{12};
элементы 3-го порядка: β^8, β^{16};
элементы 4-го порядка: β^6, β^{18};
элементы 6-го порядка: β^4, β^{20};
элементы 8-го порядка: $\beta^3, \beta^9, \beta^{15}, \beta^{21}$;
элементы 12-го порядка: $\beta^2, \beta^{10}, \beta^{14}, \beta^{22}$;
элементы 24-го порядка: $\beta, \beta^5, \beta^7, \beta^{11}, \beta^{13}, \beta^{17}, \beta^{19}, \beta^{23}$.

3) Минимальным многочленом элемента конечного поля характеристики p называется многочлен наименьшей степени $\square_p[x]$, корнем которого является данный элемент. Если поле с стоит из p^n элементов, то все элементы поля являются корня ми многочлена $x^{p^n} - x$. Отсюда следует, что минимальные многочлены - это неприводимые множители многочлена $x^{p^n} - x$.

Для решения задачи используются два факта из теории:

1. Степени вепривoдимых делителей многочлена $x^{p^n} - x$ являются делителями числа n;

2. Если элемент γ является корнем многочлена $p(x) \in \mathbb{Z}_p[x]$, то элемент γ^p также является корнем многочлена $p(x)$).

В данной задаче $n = 2$, поэтому все минимальные многочлены имеют первую или вторую степень; $p = 5$, поэтому, если элемент является корнем многочлена, то и пятая степень элемента также является корнем того же многочлена.

Для элементов -2, -1, 0,1,2, входящих в простое подполе $\mathbb{Z}_5$, минимальными многочленами будут многочлены 1-й степени $x + 2$, $x + 1$, x, $x - 1$, $x - 2$, соответственно. Для остальных 20 элементов минимальные многочлены имеют вторую степень и могут быть вычислены следующим образом. Пусть требуется найти минимальный многочлен $x^2 + ax + b$ элемента γ. Вторым корнем этого многочлена будет γ^5, отсюда по формулам Виета

$$a = -(\gamma + \gamma^5), b = \gamma\gamma^5 = \gamma^6.$$

Для вычислений используем таблицу нашего поля из решения 1). Например, для отыскания минимального многочлена элемента β действуем так. Вторым корнем минимального многочлена является β^5. По таблице находим

$$\beta + \beta^5 = 1 + \alpha + 1 - \alpha = 2, \beta\beta^5 = -2.$$

Следовательно, минимальный многочлен равен $x^2 = 2x - 2$. Вычисления сведем в таблицу.

Элементы γ, γ^5	$\gamma + \gamma^5$	$\gamma \cdot \gamma^5$	Минимальный многочлен
β, β^5	2	-2	$x^2 - 2x - 2$
β^2, β^{10}	-2	-1	$x^2 + 2x - 1$
β^3, β^{15}	0	2	$x^2 + 2$
β^4, β^{20}	1	1	$x^2 - x + 1$
β^7, β^{11}	1	2	$x^2 - x + 2$
β^8, β^{16}	-1	1	$x^2 + x + 1$
β^9, β^{21}	0	-2	$x^2 - 2$
β^{13}, β^{17}	-2	-2	$x^2 + 2x - 2$
β^{14}, β^{22}	2	-1	$x^2 - 2x - 1$
β^{19}, β^{23}	-1	2	$x^2 + x + 2$

4) Решить систему

$$\begin{cases} (1+\alpha)x - y = 1 \\ -x + \alpha y = 1 + \alpha \end{cases}$$

Найдем решение по правилу Крамера, используя для вычислений таблицу поля $\mathbb{Z}_5(\alpha), \alpha^2 = -2$, построенную выше при решении пункта 1).

Имеем

$$\Delta = \begin{vmatrix} 1+\alpha & -1 \\ -1 & \alpha \end{vmatrix} = \alpha + \alpha^2 - 1 = 2 + \alpha,$$

$$\Delta_x = \begin{vmatrix} 1 & -1 \\ 1+\alpha & \alpha \end{vmatrix} = 1 + 2\alpha, \Delta_y = \begin{vmatrix} 1+\alpha & 1 \\ -1 & 1+\alpha \end{vmatrix} = 2\alpha.$$

Чтобы выполнить деление, представим операнды как степени примитивного элемента β:

$$x = \frac{\Delta_x}{\Delta} = \frac{1+2\alpha}{2+\alpha} = \frac{\beta^{22}}{\beta^8} = \beta^{14} = 1 - 2\alpha$$

$$y = \frac{\Delta_y}{\Delta} = \frac{2\alpha}{2+\alpha} = \frac{\beta^{21}}{\beta^8} = \beta^{13} = -1 - \alpha.$$

Типовая задача

2. Установить изоморфизм полей

$$F_1 = \mathbb{Z}_2(\alpha), \alpha^5 = \alpha^2 + 1 \text{ **и** } F_2 = \mathbb{Z}_2(\beta), \beta^5 = \beta^3 + \beta^2 + \beta + 1.$$

Решение

Изоморфизмом полей F_1 и F_2 называется отображение

$$\varphi : F_1 \to F_2$$

одного поля на другое, при которой сохраняются операции:

$$\varphi(x+y) = \varphi(x) + \varphi(y), \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y).$$

Из этого определения можно вывести такие простые следствия. Так как нулевой элемент поля определяется аксиомой

$$x + 0 = x,$$

то, применив к этому равенству отображение φ, получим

$$\varphi(x) = \varphi(x) + \varphi(0).$$

Так как φ — биекция. то когда x пробегает одно поле, $\varphi(x)$. пробегает другое. Следовательно, $\varphi(0)$ - нулевой элемент второго поля, то есть при изоморфизме ноль должен отображаться в ноль. Совершенно так же устанавливается, что единица отображается в единицу. (Если характеристика поля $p > 2$, то, продолжая рассуждение, можно установить, что каждый элемент простого подполя $\mathbb{Z}_p$ отображается в себя).

Элементами поля F_1 являются многочлены 4-й степени от α с коэффициентами из $\mathbb{Z}_2 = \{0,1\}$:

$$a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4.$$

Элементы поля F_2 — такие же многочлены от β. Пусть φ — искомый изоморфизм, тогда из определения изоморфизма и указанных простых следствий получим

$$\varphi(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4) = a_0 + a_1\varphi(\alpha) + a_2(\varphi(\alpha))^2 + a_3(\varphi(\alpha))^3 + a_4(\varphi(\alpha))^4. \quad (1)$$

Таким образом, изоморфизм φ полностью определяется заданием образа элемента α.

Выясним каким должен быть этот образ. Так как

$$\alpha^5 + \alpha^2 + 1 = 0,$$

то в силу изоморфизма должно выполняться

$$(\varphi(\alpha))^5 + (\varphi(\alpha))^2 + 1 = 0.$$

Многочлен $x^5 + x^2 + 1$, корнем которого является α и $\varphi(\alpha)$, это минимальный многочлен этих элементов. Итак, при изоморфизме образующий элемент α первого поля должен отображаться в элемент второго поля, имеющий тот же самый минимальный многочлен.

Обратно, пусть $\varphi(\alpha) = \gamma$ и $\gamma^5 + \gamma^2 + 1 = 0$. Так как многочлен $x^5 + x^2 + 1$ неприводим, то элементы поля F_2 $1, \gamma, \gamma^2, \gamma^3, \gamma^4$ линейно независимы (над $\square_2$) и все элементы F_2 могут быть представлены как многочлены 4-й степени от γ. Эти многочлены складываются и перемножаются по обычным правилам с заменой γ^5 на $\gamma^2 + 1$. То есть F_1 и F_2 отличаются только обозначением образующего элемента и их изоморфизм очевиден.

Замечание. Набор минимальных многочленов элементов конечного поля из p^n элементов определяется однозначно, независимо от того, как построено поле. — это неприводимые делители многочлена деления круга $x^{p^n} - x$. Поэтому для каждого элемента одного поля всегда найдется элемент другого, имеющий тот же самый минимальный многочлен. Отсюда, в частности, вытекает, что два конечных поля с одинаковым числом элементов всегда изоморфны.

Итак, чтобы установить требуемый изоморфизм, надо в поле F_2 найти корень многочлена $x^5 + x^2 + 1$.

Один из способов решения этой задачи - подставить элемент F_2 с неопределенными коэффициентами в многочлен:

$$(b_0 + b_1\beta + b_2\beta^2 + b_3\beta^3 + b_4\beta^4)^5 + (b_0 + b_1\beta + b_2\beta^2 + b_3\beta^3 + b_4\beta^4)^2 + 1 = 0$$

После выполнения в левой части действий по законам поля F_2 (то есть с заменой β^5 на $\beta^3 + \beta^2 + \beta + 1$) получается система относительно коэффициентов, которую можно решить, перебирая 32 возможных набора этих коэффициентов.

В виду некоторой сложности этого способа в данном примере (для других полей он может оказаться вполне приемлемым), будем решать поставленную задачу иначе: просматривать по очереди элементы F_2 и определять их минимальные многочлены, пока не встретим нужного.

Для вычислений удобно предварительно составить таблицу поля F_2 (см. таблицу).

k	β^k	k	β^k
0	1	16	$1+\beta+\beta^2+\beta^3+\beta^4$
1	β	17	$1+\beta^4$
2	β^2	18	$1+\beta^2+\beta^3$
3	β^3	19	$\beta+\beta^3+\beta^4$
4	β^4	20	$1+\beta+\beta^3+\beta^4$
5	$1+\beta+\beta^2+\beta^3$	21	$1+\beta^3+\beta^4$
6	$\beta+\beta^2+\beta^3+\beta^4$	22	$1+\beta^2+\beta^3+\beta^4$
7	$1+\beta+\beta^4$	23	$1+\beta^2+\beta^4$
8	$1+\beta^3$	24	$1+\beta^2$
9	$\beta+\beta^4$	25	$\beta+\beta^3$
10	$1+\beta+\beta^3$	26	$\beta^2+\beta^4$
11	$\beta+\beta^2+\beta^4$	27	$1+\beta+\beta^2$
12	$1+\beta$	28	$\beta+\beta^2+\beta^3$
13	$\beta+\beta^2$	29	$\beta^2+\beta^3+\beta^4$
14	$\beta^2+\beta^3$	30	$1+\beta+\beta^2+\beta^4$
15	$\beta^3+\beta^4$		

Поле $\square_2(\beta)$, $\beta^5=\beta^3+\beta^2+\beta+1$

Элемент β является корнем многочлена

$$x^5+x^3+x^2+x+1.$$

Остальными корнями этого многочлена являются элементы

$$\beta^2,\beta^4,\beta^8,\beta^{16}.$$

Эти элементы далее не рассматриваем.

Найдем минимальный многочлен элемента $\gamma=\beta^2$. Используя таблицу поля, вычислим последовательные степени γ:

$$\begin{aligned}
a_0 \quad & \gamma^0=1\\
a_1 \quad & \gamma^1=\beta^3\\
a_2 \quad & \gamma^2=\beta+\beta^2+\beta^3+\beta^4\\
a_3 \quad & \gamma^3=\beta+\beta^4\\
a_4 \quad & \gamma^4=1+\beta\\
a_5 \quad & \gamma^5=\beta^3+\beta^4
\end{aligned}$$

Умножая эти равенства на указанные слева коэффициенты и приравнивая нулю коэффициенты при β^0, …, β^4 в правой части, получаем линейную систему для a_i:

$$\begin{gathered}
a_0+a_4=0\\
a_2+a_3+a_4=0\\
a_2=0\\
a_1+a_2+a_5=0
\end{gathered}$$

$$a_2 + a_3 + a_5 = 0$$

Учитывая, что $a_0 = 1$ (иначе получится приводимый многочлен) без труда находим решение

$$a_1 = 1, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 1.$$

Таким образом, минимальным многочленом элемента β^3 является многочлен $x^5 + x^4 + x^3 + x + 1$.. Остальные его корни — $\beta^6, \beta^{12}, \beta^{17}, \beta^{24}$ — в дальнейших пробах не участвуют.

Найдем минимальный многочлен элемента $\gamma = \beta^5$. Действуя

аналогично имеем

$$\begin{aligned}
a_0 \quad & \gamma^0 = 1 \\
a_1 \quad & \gamma^1 = 1 + \beta + \beta^2 + \beta^3 \\
a_2 \quad & \gamma^2 = 1 + \beta + \beta^3 \\
a_3 \quad & \gamma^3 = \beta^3 + \beta^4 \\
a_4 \quad & \gamma^4 = 1 + \beta + \beta^3 + \beta^4 \\
a_5 \quad & \gamma^5 = \beta + \beta^3
\end{aligned}$$

Система

$$\begin{gathered}
a_0 + a_1 + a_2 + a_4 = 0 \\
a_1 + a_2 + a_4 + a_5 = 0 \\
a_1 = O \\
a_1 + a_2 + a_3 + a_4 + a_5 = 0 \\
a_3 + a_4 = 0
\end{gathered}$$

Снова полагая $a_0 = 1$, находим решение

$$a_1 = 0, a_2 = 1, a_3 = 0, a_4 = 0, a_5 = 1.$$

Таким образом, минимальным многочленом элемента β^5 является многочлен $x^5 + x^2 + 1$. Он совпадает с минимальным многочленом элемента а из поля РЬ Следовательно, нужный изоморфизм φ получится, если положить $\varphi(\alpha) = \beta^3 + \beta^2 + \beta + 1$. Образ любого элемента можно вычислить с помощью соотношения (1).

Задачи для самостоятельного решения

1. Для поля $\square_5(\alpha), \alpha^2 = \alpha - 1$ 1) найти примитивный элемент и записать все элементы как степени примитивного; 2) определить мультипликативные порядки всех элементов; 3) найти для каждого элемента его минимальный многочлен; 4) решить систему $\alpha x + y = 1, x + \alpha y = \alpha^2$.

2. Для поля $\square_7(\alpha), \alpha^2 + 5\alpha + 2 = 0$ 1) найти примитивный элемент и записать все элементы как степени примитивного; 2) определить мультипликативные поряд-

ки всех элементов; 3) найти для каждого элемента его минимальный многочлен; 4) решить систему $\alpha x + y = 1, x + \alpha y = \alpha^2$.

3. Установить изоморфизм полей

$$F_1 = \mathbb{Z}_5(\alpha), \alpha^2 = 2 \text{ и } F_2 = \mathbb{Z}_5(\beta), \beta^2 = \beta + 3.$$

4. Установить изоморфизм полей

$$F_1 = \mathbb{Z}_3(\alpha), \alpha^3 = \alpha^2 + \alpha + 1 \text{ и } F_2 = \mathbb{Z}_3(\beta), \beta^3 = \beta^2 + 2.$$

Домашнее задание

1. Для поля $\mathbb{Z}_5(\alpha), \alpha^2 = 2\alpha + 1$ 1) найти примитивный элемент и записать все элементы как степени примитивного; 2) определить мультипликативные порядки всех элементов; 3) найти для каждого элемента его минимальный многочлен; 4) решить систему $\alpha x + y = 1, x + \alpha y = \alpha^2$.

2. Для поля $\mathbb{Z}_7(\alpha), \alpha^2 = \alpha + 3$ 1) найти примитивный элемент и записать все элементы как степени примитивного; 2) определить мультипликативные порядки всех элементов; 3) найти для каждого элемента его минимальный многочлен; 4) решить систему $\alpha x + y = 1, x + \alpha y = \alpha^2$.

3. Установить изоморфизм полей

$$F_1 = \mathbb{Z}_5(\alpha), \alpha^2 = 2\alpha + 2 \text{ и } F_2 = \mathbb{Z}_5(\beta), \beta^2 = \beta + 3.$$

4. Установить изоморфизм полей

$$F_1 = \mathbb{Z}_3(\alpha), \alpha^3 = \alpha^2 + 2 \text{ и } F_2 = \mathbb{Z}_3(\beta), \beta^3 = \beta^2 + 2.$$

Занятия 15,16
Линейные коды. Построение циклических кодов

План занятия

1. Повторение теоретического материала
2. Подробное решение типовой задачи
3. Самостоятельное решение задач
4. Получение домашнего задания

Типовая задача

1. Построить линейный код Хемминга длины 7, исправляющий одну ошибку.

Решение

7-разрядный код Хэмминга представляет собой линейный код с проверочной матрицей:

$$H = \begin{pmatrix} 0 & 0 & 01 & 1 & 11 \\ 0 & 1 & 10 & 0 & 11 \\ 1 & 0 & 10 & 1 & 01 \end{pmatrix}.$$

Его слова являются решениями линейной однородной системы $Hx = 0$ или

$$\begin{cases} x_4 + x_5 + x_6 + x_7 = 0 \\ x_2 + x_3 + x_6 + x_7 = 0 \\ x_1 + x_3 + x_5 + x_7 = 0. \end{cases}$$

Ее общее решение имеет вид

$$x_4 = x_5 + x_6 + x_7$$
$$x_2 = x_3 + x_6 + x_7$$
$$x_1 = x_3 + x_5 + x_7.$$

Придавая x_3, x_5, x_6, x_7 значения 0,1, получим 16 слов кода

$$c_1 = 0111100, c_2 = 0010110, c_3 = 1111111, c_4 = 1010101,$$
$$c_5 = 1011010, c_6 = 0011001, c_7 = 0110011, c_8 = 0000000,$$
$$c_9 = 1001100, c_{10} = 1000110, c_{11} = 0001111, c_{12} = 0100101,$$
$$c_{13} = 0101010, c_{14} = 1101001, c_{15} = 1000011, c_{16} = 1110000.$$

Кодовое расстояние для линейного кода вычисляется по формуле $d(C) = \min\limits_{c_i \neq 0} \|c_i\|$, где $\|c\|$ - вес Хэмминга слова c, равный числу единиц в нем. В нашем случае $d(C) = 3$, поэтому этот код исправляет одну ошибку.

2. Построить БЧХ-код со следующими параметрами: длина кодовых слов – 23, количество исправляемых ошибок – 2. Для построения кода необходимо 1) вычислить основные параметры кода: мощность и кодовое расстояние; 2) найти порождающий и проверочный многочлены кода; 3) описать алгоритм кодирования и построить схему, производящую кодирование, используя сдвиговые регистры и функциональные элементы; 4) описать алгоритм декодирования.

Решение

Кодом длины n называется произвольное подмножество $C \subseteq \{0,1\}^n$. Различаются коды по двум их основным характеристикам:

- $|C|$, этот параметр определяет скорость передачи информации по каналу связи: если канал передает 1 бит за единицу времени, то кодированную информацию канал будет передавать с меньшей скоростью $|C|/2^n$ бит за единицу времени.
- $d(C) = \min\limits_{x \neq y} d(x, y)$ — кодовое расстояние, этот параметр определяет возможности исправления ошибок кодом C : если $d(C) > 2e$, то код исправляет e ошибок.

Для построения кодов на множестве двоичных слов $\{0,1\}^n$ вводят различные алгебраические структуры: с их помощью дается описание кода и исследуются его параметры.

Такой структурой для кодов Боуза, Чаудхури, Хоквингема (БЧХ-кодов) является кольцо многочленов

$$\mathbf{Z}_2[x]/(x^n + 1) = \{a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}\}, \qquad (1)$$

Элементами кольца являются всевозможные многочлены степени не выше n — 1 с коэффициентами 0,1 (остатки от деления на $x^n + 1$). Операции над многочленами производятся по обычным правилам с заменой результата остатком от деления на $x^n + 1$.

В виду очевидной биекции

$$a_0\, a_1\, a_2\, \ldots a_{n-1} \;\mapsto\; a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} = a(x),$$

двоичных слов и многочленов не будем их далее различать и говорить, например, так: код состоит из многочленов $a(x), b(x), \ldots$, имея в виду соответствующие двоичные слова.

БЧХ-код определяется как совокупность всевозможных многочленов кольца (1), кратных некоторому фиксированному многочлену $g(x)$:

$$C_g = \{c(x) \mid c(x) = g(x) \cdot f(x)\}\,.$$

Многочлен $g(x)$ называется *порождающим*. Многочлен $f(x)$ может быть любым, но нетрудно убедиться, что произведение $g(x)f(x)$ дает различные элементы кольца (1) только для многочленов $f(x)$, степень (deg) которых удовлетворяет неравенству

$$\deg f(x) \le n - 1 - \deg g(x)\,.$$

Таким образом, определение БЧХ-кода можно уточнить (1):

$$C_g = \{c(x) \mid c(x) = g(x) \cdot f(x),\ \deg f(x) \le n - 1 - \deg g(x)\}\,.$$

Порождающий многочлен $g(x)$ БЧХ-кода является делителем многочлена $x^n + 1$. Многочлен $h(x) = \dfrac{x^n + 1}{g(x)}$ называется *проверочным:* код можно определить как совокупность всех таких многочленов, которые будучи умноженными на проверочный многочлен дают ноль.

Корректирующие возможности БЧХ-кода определяются корнями порождающего многочлена. Так как $g(x) \mid x^n + 1$, то корнями порождающего многочлена являются так называемые *корни n-й степени из единицы,* то есть элементы γ такие, что $\gamma^n = 1$. Корни n-й степени из единицы имеются в некотором поле, так как для каждого многочлена можно построить поле его разложения. Среди корней n-й степени из единицы имеется *примитивный* β, его степени

$$1 = \beta^0, \beta, \beta^2, \ldots, \beta^{n-1}$$

все различны и дают все решения уравнения x^n — 1.

Основная теорема о БЧХ-кодах: если корнями порождающего многочлена g являются элементы

$$\beta, \beta^3, \ldots, \beta^{2e-1}\,,$$

то БЧХ-код C_g будет исправлять e ошибок.

Возвращаемся к решению задачи. Построение кода разбивается на ряд этапов.

1. Определение поля, содержащего корни 23-й степени из 1.

Предварительно определяется мультипликативный порядок числа 2 по модулю 23. Имеем по модулю 23:

$$2^1 = 2\ 2^2 = 4\ 2^3 = 8\ 2^4 = 16\ 2^5 = 9\ 2^6 = 18$$
$$2^7 = 13\ 2^8 = 3\ 2^9 = 6\ 2^{10} = 12\ 2^{11} = 1.$$

То, что $2^{11} = 1 \bmod 23$ означает, что $23 \mid 2^{11} - 1$. Действительно, $2^{11} - 1 = 2047 = 23 \cdot 89$.

Рассмотрим поле $GF(2^{11})$. Его можно построить как $\mathbb{Z}_2(\alpha)$, где α - корень неприводимого многочлена 11-й степени. Им является многочлен $x^{11} + x^2 + 1$. Итак, если поле определить как $\mathbb{Z}_2(\alpha)$, $\alpha^{11} = \alpha^2 + 1$, то α будет примитивным элементом поля, то есть иметь 2047-й порядок.

Рассмотрим в построенном поле элемент $\beta = \alpha^{89}$. Имеем $\beta^{23} = \alpha^{89 \cdot 23} = 1$. Следовательно, β - корень 23-й степени из единицы, причем примитивный, что следует из примитивности α.

2. Построение порождающего многочлена.

Найдем многочлен, корнем которого является α^{89} (то есть β). Это многочлен $x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$.

Используя тот факт, что если некоторый элемент является корнем многочлена из $\mathbb{Z}_2[x]$, то и квадрат этого элемента так же будет корнем, получаем, что найденный многочлен имеет следующие корни

$$\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^9, \beta^{18}, \beta^{13}, \beta^3, \beta^6, \beta^{12}.$$

Следовательно, полагая

$$g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1,$$

будем иметь

$$g(\beta) = g(\beta^3) = 0.$$

Следовательно, по основной теореме БЧХ-код с порождающим многочленом $g(x)$ будет исправлять 2 ошибки.

3. Код и его параметры.

По формуле (11)

$$C = \{c(x) \mid c(x) = g(x) \cdot f(x),\ \deg f(x) \le 11\}.$$

Здесь

$$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{22} x^{22};$$
$$g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1;$$
$$f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_{11} x^{11}.$$

Различные кодовые точки получаются при разных выборах многочлена f. Так как он имеет 12 двоичных коэффициентов, то $|C| = 2^{12}$.

По основной теореме $d(C) > 5$.

Проверочный многочлен кода

$$h(x) = \frac{x^{23}+1}{g(x)} = x^{12} + x^{10} + x^7 + x^4 + x^3 + x^2 + x + 1.$$

4. Процедура и схема кодирования.

Кодирование происходит следующим образом:

- "длинная" двоичная последовательность, которую надо передать по каналу связи, разбивается на блоки по 12 символов;

$$\ldots f_{13} f_{12} \mid f_{11} f_{10} \ldots f_2 f_1 f_0 \ .$$

- каждый блок рассматривается как многочлен

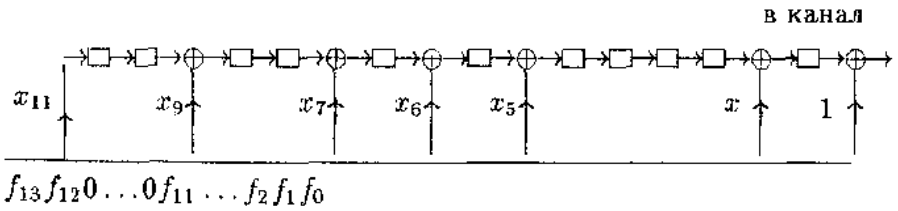
$$f(x) = f_{11}x^{11} + f_{10}x^{10} \ldots f_2 x^2 + f_1 x + f_0 \ .$$

- операция кодирования состоит в том, что этот многочлен умножается на порождающий многочлен кода

$$c(x) = f(x) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) :$$

$$\begin{array}{rcccccccccccccccccccccc}
 & & & & & & & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 \\
 & & & & & & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 & \\
 & & & & & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 & & \\
+ & & & & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 & & & \\
 & & & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 & & & & \\
 & & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 & & & & & \\
 & & & & & f_{11} & f_{10} & f_9 & f_8 & f_7 & f_6 & f_5 & f_4 & f_3 & f_2 & f_1 & f_0 & & & & & & \\
\hline
c_{22} & c_{21} & c_{20} & c_{19} & c_{18} & c_{17} & c_{16} & c_{15} & c_{14} & c_{13} & c_{12} & c_{11} & c_{10} & c_9 & c_8 & c_7 & c_6 & c_5 & c_4 & c_3 & c_2 & c_1 & c_0
\end{array}$$

Это умножение эффектно реализуется на сдвиговом регистре



(см.рисунок).

Умножение на порождающий многочлен

Чтобы 12 информационных разрядов прошли через регистр, превратившись в 23 разряда кода, блоки кодируемой последовательности "прокладываются" блоками из 11 нулей.

5. Декодирование.

$$\tilde{c}\,(x) = \tilde{c}_0 + \tilde{c}_1\, x + \ldots + \tilde{c}_{22}\, x^{22}$$

1° . Для принятого многочлена
вычисляются синдромы

$$S_1 = \bar{c}(\beta)\ ,\ S_2 = S_1^2\ ,\ S_3 = \bar{c}(\beta^3)\ ,\ S_4 = S_2^2\ .$$

2°. К многочленам x^5 и $S(x) = 1 + S_1 x + S_2 x^2 + S_3 x^3 + S_4 x^4$ применяется алгоритм Евклида (с вычислением U, V, U_1, V_1) до шага k, на котором степень получившегося остатка не превосходит 2 (при этом степень предыдущего остатка больше 2).

3° . Вычисляется многочлен локаторов ошибок $\sigma(x)$: если $V(x)$ — многочлен, рассчитанный на k-ом шаге, то

$$\sigma(x) = \frac{V_k(x)}{V_k(0)}\ ;$$

4° . Элементы β^j, $j = 0,1,2,...,22$ поочередно подставляются в многочлен локаторов ошибок; если $\sigma(\beta^j) = 0$; то c_{23-j} исправляется (заменяется на противоположный).

Замечание. Все упомянутые выше вычисления ведутся в поле $GF(2^{11})$.

Задачи для самостоятельного решения

1. Построить линейный код Хемминга длины 15, исправляющий одну ошибку.
2. Построить БЧХ-код со следующими параметрами: длина кодовых слов – 27, количество исправляемых ошибок – 3. Для построения кода необходимо 1) вычислить основные параметры кода: мощность и кодовое расстояние; 2) найти порождающий и проверочный многочлены кода; 3) описать алгоритм кодирования и построить схему, производящую кодирование, используя сдвиговые регистры и функциональные элементы; 4) описать алгоритм декодирования.

Домашнее задание

1. Построить линейный код Хемминга длины 31, исправляющий одну ошибку.
2. Построить БЧХ-код со следующими параметрами: длина кодовых слов – 21, количество исправляемых ошибок – 3. Для построения кода необходимо 1) вычислить основные параметры кода: мощность и кодовое расстояние; 2) найти порождающий и проверочный многочлены кода; 3) описать алгоритм кодирования и построить схему, производящую кодирование, используя сдвиговые регистры и функциональные элементы; 4) описать алгоритм декодирования.

Библиографический список

1. Ефимов Н.В. Линейная алгебра и многомерная геометрия: учебное издание. – 4-е изд., стер. М.: Физматлит, 2005. – 464с.
2. Икрамов Х.Д. Задачник по линейной алгебре: учебн. пособие. – 2-е изд., испр. СПб.: Лань, 2006. – 319с.

3. Гантмахер Ф.Р. Теория матриц. – 5-е изд. М.: Физматлит, 2004. – 560с.
4. Глаголев В.В. Алгебраическая теория кодирования: учебн. пособие. Тула: Изд-во ТулГУ, 2004. – 116с.
5. Кострикин А.И. Введение в алгебру. Ч.1. Основы алгебры. – 2-е изд., испр. М.: Физматлит, 2004. – 272с.
6. Кострикин А.И. Введение в алгебру. Ч.2. Линейная алгебра. – 3-е изд. М.: Физматлит, 2004. – 368с.
7. Методические указания к самостоятельной работе студента по дисциплине «Прикладная алгебра». Тула: ТулГУ, 2011. — (Кафедральный ресурс).