С.Н.Тронин

КРАТКИЙ КОНСПЕКТ ЛЕКЦИЙ ПО ТЕОРИИ КОДИРОВАНИЯ

Казань — 2017

УДК

Представляется на сайте университета
по решению Редакционно-издательского совета
ФГАОУВПО <Казанский (Приволжский) федеральный университет>

методической комиссии Института математики и механики
им. Н.И.Лобачевского
Протокол №7 от 13 апреля 2017 г.

заседания кафедры алгебры и математической логики
Протокол №8 от 13 апреля 2017 г.

Автор-составитель
доктор физ.-мат. наук, доц. С.Н. Тронин

Научный редактор
доктор физ.-мат. наук, профессор С.М.Скрябин

Рецензент
кандидат физ.-мат. наук, доцент Е.К.Липачев

Краткий конспект лекций по теории кодирования: Учебно-методическое пособие / С.Н. Тронин. — Казань: Казанский (Приволжский) федеральный университет, 2017. — 36 с.

Данное учебно-методическое пособие пособие предназначено для студентов-математиков, изучающих теорию кодирования. Оно представляет собой обработанные записи лекций, неоднократно читавшихся автором студентам четвертого курса. Содержание данного пособия полностью соответствует программе курса по выбору “Теория кодирования” для студентов-математиков, действующей в Казанском (Приволжском) федеральном университете.

СОДЕРЖАНИЕ

Введение

Данное учебное пособие представляет собой краткий конспект семестрового курса по выбору, неоднократно читавшегося студентам-математикам старших курсов Казанского федерального университета. Курс носит вводный характер, более глубокие результаты должны были бы излагаться в его второй части (если бы она состоялась). Так как слушателями курса являлись студенты-математики, то основные результаты излагались с полными доказательствами. В зависимости от обстоятельств, лектору удавалось рассказать чуть больше или чуть меньше, но в основном в рамках содержащегося в данном пособии материала. Материал этот является стандартным, и его можно найти в ряде книг, которые доступны студентам Казанского университета. В частности, большинство этих книг можно найти в электронном виде в Интернете. Эти книги гораздо более объемны, чем данное пособие, и содержат все положенные подробности. Но именно их объем и подробность изложения часто создают затруднения для большинства студентов. Назначение данного пособия — показать, что является главным и минимально необходимым. Предполагается, что отсутствующие в пособии доказательства легко можно найти в книгах из списка литературы, большинство из которых доступно. Таким образом, предполагается, что студент будет использовать данное пособие как дополнение к своему рукописному конспекту (если он у него обнаружится), но при необходимости станет обращаться к толстым книгам.

Для понимания материала курса необходимы некоторые предварительные сведения. Помимо общей математической культуры в их число входят первичные понятия линейной алгебры (матрицы, ранг, системы линейных уравнений, определитель Вандермонда, векторные пространства, линейная зависимость и независимость, базисы, размерность), и общей алгебры (группы, порядки, теорема Лагранжа, кольца, поля, примеры полей).

Автор не теряет надежды, что в обозримом будущем сможет доработать данное пособие, и включить в него все доказательства, ряд важных в идейном отношении результатов, а также интересных и практически важных примеров кодов.

ГЛАВА I. КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ

1.1. Расстояние Хэмминга

Расстояние Хэмминга на множестве K^n, где K — некоторое конечное множество мощности q, определяется так: $\rho(x,y) = |\{i|x_i \neq y_i\}|$, где $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, $x, y \in K^n$.

Теорема 1.1.1. *Расстояние Хэмминга задает на K^n структуру метрического пространства.*

Лемма 1.1.1. *Пусть $a, b =\in K^n$, и $d(a,b) = t > 0$. Тогда найдутся элементы $a_0 = a, a_1, \ldots, a_t = b$ из множества K^n, такие, что $\rho(a_i, a_j) = |i-j|$ для любой пары i, j, $0 \leq i, j \leq t$.*

Начиная с этого раздела, будем называть *кодом* подмножество $C \subset K^n$. Его элементы называются *кодовыми словами* данного кода. *Минимальное кодовое растояние* $d(C)$ кода C (или просто *кодовое расстояние*) определяется как минимальное из чисел $\rho(c_i, c_j)$, где c_i, c_j — различные кодовые слова кода C.

Обозначим через $B_r(w)$ замкнутый шар в K^n с центром w.

Будем говорить, что код C исправляет не менее t ошибок, если $B_t(c_i) \cap B_t(c_j) = \emptyset$ для любых различных кодовых слов c_i и c_j.

Теорема 1.1.2. *Эквивалентны следующие три условия:*

1. *Код исправляет не менее чем t ошибок;*
2. *$d(C) \geq 2t + 1$;*
3. *Для каждого кодового слова $c \in C$ и любого $x \in B_t(c)$ ближайшим кодовым словом к x является слово c, причем это ближайшее слово является единственным.*

Таким образом, для кода, исправляющего ошибки, можно определить достаточно эффективную процедуру декодирования в ближайшее кодовое слово (другое название — декодирование по максимуму правдоподобия). Если получено некоторое сообщение, то оно сначала разбивается на блоки, равные длине кодовых слов, а потом для каждого блока (слова в алфавите K) ищется ближайшее к нему (в смысле метрики Хэмминга)

кодовое слово. Если есть гарантия, что количество искажений, приходящихся на каждый полученный по каналу связи блок, не превышает количества ошибок, исправляемого кодом, то найденное ближайшее кодовое слово будет именно тем, которое было передано.

Лемма 1.1.2. *Количество элементов в замкнутом шаре $B_t(x)$ таково:*

$$|B_t(x)| = 1 + \sum_{j=1}^{t} (q-1)^j C_n^j.$$

Теорема 1.1.3. (Граница сферической упаковки) *Код C исправляет не менее t ошибок тогда и только тогда, если*

$$|C| \cdot (1 + \sum_{k=1}^{t} (q-1)^k C_n^k) \leq q^n.$$

Если $|C| = q^k$ (случай, когда $K = GF(q)$ и C — линейный (n,k)-код), то код исправляет не менее t ошибок тогда и только тогда, если

$$1 + \sum_{k=1}^{t} (q-1)^k C_n^k \leq q^{n-k} \tag{1.1}$$

Код называется *совершенным*, если неравенство (1.1) является точным равенством.

1.2. Линейные коды

Наиболее важным является случай, когда $K = \mathbb{F}_q = GF(q)$ — конечное поле из q элементов. *Линейный код* C — это подпространство векторного пространства K^n над полем K.

Весом Хэмминга $wt(x)$ слова (вектора) $x \in K^n$ называется число ненулевых компонент x.

Теорема 1.2.1. *Если $K = \mathbb{F}_q$, то расстояние Хэмминга выражается через вес Хэмминга следующим образом:*

$$\rho(x, y) = wt(x - y).$$

Если код C линеен, то

$$d(C) = \min_{x \in C, x \neq 0} wt(x).$$

Пусть C — некоторый линейный код над полем $K = \mathbb{F}_q = GF(q)$, т.е. векторое подпространство в K^n. Число n называется *длиной* кода C. Если $k = \dim_K(C)$, то код C называется $[n, k]$-кодом. Число k будем называть *размерностью* кода. Во многих учебниках (особенно старых) это число также называется *числом информационных символов* кода. Если $d = d(C)$ — кодовое расстояние кода C, то C еще называется $[n, k, d]$-кодом. В случае, когда следует указать, над каким полем рассматривается код, говорят (и пишут), что C является $[n, k, d]_q$-кодом. Тут надо иметь в виду, что конечное поле однозначно (с точностью до изоморфизма) определяется числом q — количеством своих элементов.

Пусть $G_1, \ldots, G_k$— некоторый базис $[n, k]$-кода C (это столбцы высоты n), и пусть G есть матрица из n строк и k столбцов, i-ым столбцом которой является базисный вектор G_i. Матрица G называется *порождающей матрицей* кода C. Из свойств базиса непосредственно следует, что кодовый вектор может быть представлен в виде линейной комбинации столбцов $G_1, \ldots, G_k$ матрицы G и, наоборот, что любая линейная комбинация столбцов $G_1, \ldots, G_k$ матрицы G представляет собой кодовый вектор и, более того, различные линейные комбинации задают различные кодовые векторы.

Поскольку каждый из k коэффициентов линейной комбинации может принимать q значений, общее число кодовых слов в коде C равно q^k. Наоборот, задав матрицу G размера $n \times k$ и ранга k с элементами из поля $\mathbb{F}_q = GF(q)$, мы задаем линейный код, для которого G является порождающей матрицы.

Для задания линейных кодов используются также *проверочные* матрицы H, которые определяются следующим образом. Если C есть $[n, k]$-код, то H есть матрица размером $(n - k) \times n$, такая, что $x \in C$ тогда и только тогда, если $Hx = 0$. Ранг H должен быть в этом случае равен $n - k$.

Пусть $H = (H_1, \ldots, H_n)$, где $H_1, \ldots, H_n$ — столбцы матрицы H. Тогда существует взаимно-однозначное соответствие между кодовыми словами $x = (x_1, \ldots, x_n)^{\mathrm{T}}$, в которых ненулевыми являются лишь компоненты $x_{i_1}, \ldots, x_{i_m}$, и линейными зависимостями вида

$$x_{i_1} H_{i_1} + \cdots + x_{i_m} H_{i_m} = 0,$$

в которых все коэффициенты отличны от нуля.

Теорема 1.2.2. (Граница Синглтона) *Для произвольного* $[n,k]$*-кода* C *имеет место неравенство*

$$d(C) \leq n - k + 1.$$

Код Хэмминга $\mathcal{H}_m$ над полем $\mathbb{F}_2 = \{0,1\}$ строится следующим образом. Пусть $m \geq 2$. Рассмотрим матрицу H_m, состоящую из всех ненулевых столбцов высоты n, компонентами которых являются элементы поля $\mathbb{F}_2$. Таких столбцов будет $2^m - 1$ штук. Ранг этой матрицы равен m. Кодом Хэмминга $\mathcal{H}_m$ называется пространство решений системы уравнений

$$H_m x = 0.$$

Столбец x здесь имеет высоту $2^m - 1$, так что длина кода равна $2^m - 1$. Размерность пространства решений системы $H_m x = 0$ равна $2^m - 1 - m$ (количество переменных минус ранг матрицы системы), и, таким образом, код Хэмминга $\mathcal{H}_m$ является $[2^m - 1, 2^m - 1 - m]$-кодом.

Теорема 1.2.3. *Кодовое расстояние кода Хэмминга* $\mathcal{H}_m$ *равно трем. Таким образом, код Хэмминга истправляет одну ошибку. Кроме того, код Хэмминга является совершенным.*

Пусть $C^\perp$ — множество всех векторов (столбцов из K^n) u таких, что для любого $v \in C$ выполнено равенство $(u,v) = u^{\mathrm{T}} v = 0$ (т.е. $\sum\limits_{i=1}^{n} u_i v_i = 0$), где т означает транспонирование. Множество $C^\perp$ является подпространством пространства K^n. Это подпространство называется *кодом, двойственным к коду* C.

Лемма 1.2.1. *Если* C *есть* $[n,k]$*-код, то* $\dim(C^\perp) = n - k$*, и поэтому* $C^\perp$ *есть* $[n, n-k]$*-код.*

Очевидно, что $(C^\perp)^\perp = C$.

Теорема 1.2.4. *Пусть* C *есть* $[n,k]$*-код с порождающей матрицей* G *и проверочной матрицей* H*. Тогда* $C^\perp$ *есть код с порождающей матрицей* H^{T} *и проверочной матрицей* G^{T}*.*

Коды, двойственные к кодам Хэмминга, называются *симплексными кодами.*

Теорема 1.2.5. *Пусть* C *— симплексный код, двойственный к* $[2^m - 1, 2^m - m - 1]$*-коду Хэмминга. Тогда каждое ненулевое кодовое слово этого кода имеет один и тот же вес* 2^{m-1}*.*

Пусть даны два кода одинаковой длины, $C_1, C_2 \subseteq K^n$. Эти коды называются *эквивалентными*, если существует изоморфизм векторных пространств $\psi : C_1 \to C_2$, обладающий следующим свойством: для каждого кодового слова $v \in C_1$ выполнятся равенство: $wt(v) = wt(\psi(v))$.

Эквивалентные коды имеют одинаковые длины, размерности, и минимальные кодовые расстояния.

Лемма 1.2.2. *Если код C имеет порождающую матрицу G, то код C', чья порождающая матрица G' может быть получена из G с помощью элементарных преобразований со столбцами, а также с помощьюю перестановок строк матрицы, и умножений строк на ненулевые элементы поля, будет эквивалентным коду C.*

Если H — проверочная матрица кода C, то код C'', проверочная матрица которого может быть получена из H элементарными преобразованиями со строками, а также с помощью перестановок столбцов и умножений столбцов на ненулевые элементы поля, будет эквивалентен коду C.

Теорема 1.2.6. *Каждый линейный $[n, k]$-код эквивалентен коду C' с порождающей матрицей вида:*

$$\begin{pmatrix} E \\ Q \end{pmatrix},$$

где E есть единичная $n \times n$-матрица. В качестве проверочной матрицы для кода C' можно взять матрицу:

$$\begin{pmatrix} Q & -E \end{pmatrix}.$$

Код C' с порождающей матрицей указанного в предыдущей теореме вида называется *систематическим*.

В заключение сформулируем один общий факт, справедливый для произвольных линейных кодов.

Теорема 1.2.7. (Граница Плоткина) *Для произвольного $[n, k, d]_q$-кода справедливо неравенство:*

$$d \leq \frac{nq^{k-1}(q-1)}{q^k - 1}.$$

1.3. Декодирование линейных кодов

Общая идея о декодировании в ближайшее кодовое слово в случае линейных кодов допускает существенное уточнение.

Пусть K — некоторое конечное поле, $|K| = q$, C — $[n, k, d]_q$-код, $d \geq 2t + 1$, H — проверочная матрица кода C. Матрицу H можно рассматривать как линейное отображение

$$S : K^n \longrightarrow K^{n-k}, \quad S(x) = Hx.$$

Если $x \in K^n$ (напомним, что элементы из K^n называются словами длины n в алфавите K), то элемент $S(x) = Hx$ называется *синдромом* слова x. Код C — это в точности множество тех слов, синдромы которых равны нулю, $C = Ker(S)$.

Лемма 1.3.1. *Для любых слов $x, y \in K^n$ и любого t справедливо равенство:*

$$B_t(x + y) = x + B_t(y).$$

Пусть $B_t(0) = \{0, v_1, \ldots, v_r\}$, $C = \{c_1 = 0, c_2, \ldots, c_{q^k}\}$.

Лемма 1.3.2. *Пусть $d \geq 2t + 1$ (т.е. код C исправляет не менее t ошибок). Тогда для любых $x, y \in B_t(0)$ при $x \neq y$ смежные классы $x + C$ и $y + C$ различны (т.е. не пересекаются).*

Лемма 1.3.3. *Пусть $d \geq 2t + 1$. Тогда для любого $v \in B_t(0)$ и любого $c \in C$, $c \neq 0$ выполнно неравенство $wt(x) < wt(v + c)$.*

Предположение, что $d \geq 2t + 1$, будет действовать до конца этого параграфа.

Слово из смежного класса $x+C$, имеющее наименьший вес Хэмминга среди всех слов данного класса, называется *лидером* этого смежного класса. Таким образом, предыдущую лемму можно переформулировать так: в каждом из смежных классов $C = 0 + C$, $v_1 + C$, $\ldots$, $v_r + C$ существует лидер (притом только один), и это элемент из $B_t(0)$.

Пользуясь доказанными выше утверждениями, можно расположить множество слов из K^n в виде следующей таблицы, строками которой будут смежные классы по подпространству C, а в каждом столбце, начинающемся с кодового слова c, в первых (сверху вниз) $r + 1$ строках располагаются элементы замкнутого шара $B_t(c)$. В частности, в первых

$r+1$ стоках первого столбца расположены элементы $B_t(0)$, причем каждый такой элемент имеет вес Хэмминга, строго меньший весов Хэмминга всех остальных элементов той же строки, т.е. лидер соответствующего смежного класса.

0	c_2	c_3	$\dots$	c_{q^k}
v_1	v_1+c_2	v_1+c_3	$\dots$	$v_1+c_{q^k}$
v_2	v_2+c_2	v_2+c_3	$\dots$	$v_2+c_{q^k}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
v_r	v_r+c_2	v_r+c_3	$\dots$	$v_r+c_{q^k}$
v_{r+1}	$v_{r+1}+c_2$	$v_{r+1}+c_3$	$\dots$	$v_{r+1}+c_{q^k}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$

Построенная только что таблица называется *стандартным расположением* слов из K^n. Начиная с $r+2$-й строки представителей смежных классов можно выбирать произвольно, но лучше делать это так, чтобы в первом слева столбце всегда находились лидеры смежных классов. Напомним еще раз, что если мы выбираем элементы $v_1,\dots,v_r$ таким образом, что $\{0,v_1,\dots,v_r\}=B_t(0)$, и код C исправляет не менее t ошибок, то для первых $r+1$ строк лидеры смежных классов оказываются в первом столбце автоматически.

Теперь можно сформулировать алгоритм декодирования. Пусть в результате процесса передачи информации по каналу связи был принят вектор (слово) $y\in K^n$. Предположим, что было сделано не более t ошибок.

1) Вычисляем синдром $S(y)=Hy$;

2) Находим лидера смежного класса $y+C$ — ээлемент $v\in B_t(0)$, такой, что $S(v)=S(y)$. Это осуществляется перебором $r+1$ элементов $B_t(8)$;

3) Слово y декодируется в слово $c=y-v$.

В случае, если нет гарантии, что при передаче данных происходит не более t ошибок в каждом передаваемом слове длины n, алгоритм можно "усовершенствовать" следующим образом. В пункте 2) надо перебирать элементы множества всех лидеров смежных классов (которые должны быть заранее вычислены), и искать среди них такой v, который обладает

свойством $S(v) = S(y)$. Результатом декодирования будет слово $c = y - v$, но теперь уже отсутствует гарантия, что декодирование осуществлено правильно.

1.4. Коды МДР

Рассмотрим $[n,k]$-код C. Если $d(C) = n - k + 1$, то C называетя *разделимым кодом с максимально достижимым расстоянием*, или *кодом с максимальным расстоянием*, или сокращенно *кодом МДР*.

Теорема 1.4.1. *Код C с проверочной матрицей H (размера $(n-k)\times n$) является кодом МДР тогда и только тогда, если любые $n-k$ столбцов матрицы H линейно независимы.*

Теорема 1.4.2. *Код, двойственный к коду МДР, сам является кодом МДР.*

Теорема 1.4.3. *Код C с проверочной матрицей H (размера $(n-k)\times n$) является кодом МДР тогда и только тогда, если любые $n-k$ столбцов матрицы H линейно независимы, и тогда ии только тогда, если любые k строк порождающей матрицы G линейно независимы.*

Теорема 1.4.4. *Пусть C есть $[n,k]$-код, являющийся кодом МДР, $d = n - k + 1$ — его минимальное кодовое расстояние. Тогда для любых $1 \le i_1 < i_2 < \ldots < i_d \le n$ существует кодовое слово (столбец) веса d, ненулевые компоненты которого расположены в заранее выбранных позициях (строках) $i_1, i_2, \ldots, i_d$ (в остальных позициях должны стоять нули).*

Верно и обратное. Если $[n,k,d]$-код C таков, что для любого набора номеров строк $1 \le i_1 < i_2 < \ldots < i_d \le n$ существует кодовое слово (столбец) веса d, ненулевые компоненты которого расположены в заранее выбранных позициях (строках) $i_1, i_2, \ldots, i_d$, то этот код является кодом МДР.

Как следствие, отсюда выводится, что количество A_d кодовых слов веса d в коде МДР равно $C_n^d(q-1)$.

Теорема 1.4.5. *Если C есть $[n,k]$-код МДР над $GF(q)$, и $d = d(C) = n - k + 1 > 2$, то*

$$q - 1 \ge \max\{k, n-k\}.$$

1.5. Циклические коды

Векторное пространство K^n можно представлять в разных формах. Например, это пространство естественным образом изоморфно пространству V_n всех многочленов из $K[x]$, степени которых строго меньше n. Изоморфизм осуществляется следующим образом:

$$v = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{n-1} \end{pmatrix} \leftrightarrow v(x) = \sum_{i=0}^{n-1} v_i x^i.$$

В дальнейшем мы будем по мере необходимости переходить от одного из этих пространств к другому, используя описанный выше изоморфизм.

Имеется два эквивалентных определения *циклических кодов*. Согласно первому определению, линейный код $C \subseteq K^n$ называется циклическим, если из того, что

$$v = (v_0, v_1, \ldots, v_{n-2}, v_{n-1})^{\mathrm{T}}$$

принадлежит коду C, следует, что вектор (слово в алфавите K)

$$Pv = (v_{n-1}, v_0, v_1, \ldots, v_{n-2})^{\mathrm{T}}$$

также принадлежит коду C. Это кодовое слово называется *циклическим сдвигом* слова v.

Согласно второму определению, код C как подпространство в пространстве V_n (подпространстве всех многочленов из $K[x]$, степени которых строго меньше n) является циклическим, если существует многочлен $g(x) \in V_n$, $deg(g) = n - k$, обладающий следующими свойствами: $g(x)|x^n - 1$ и $C = \{f(x)g(x)|f(x) \in K[x], deg(f) \leq k - 1\}$. Многочлен g, определенный с точностью до ненулевого множителя — элемента из K, называется *порождающим многочленом* кода C.

Теорема 1.5.1. *Оба определения циклического кода эквивалентны. Точнее, циклические коды в смысле первого определения взаимно-однозначно переходят в циклические коды в смысле второго определения при описанном выше изоморфизме $K^n \cong V_n$.*

Кроме того, циклические коды находятся во взаимно-однозначном соответствии с идеалами факторалгебры $K[x]/(x^n - 1)$.

Как известно, ограничение гомоморфизма естественной проекции $K[x] \to K[x]/(x^n-1)$ на подпространство V_n является изоморфизмом векторных пространств. Взаимно-однозначное соответствие между циклическими кодами и идеалами $K[x]/(x^n-1)$ строится по этому изоморфизму.

Лемма 1.5.1. *Базисом циклического кода с порождающим многочленом $g(x)$, имеющим степень $n-k$, являются многочлены $g, xg, x^2g, \ldots, x^{k-1}g$.*

Итак, $\dim(C) = n - deg(g)$. Если $[n,k]$-код C является циклическим, то степень его порождающего многочлена равна $n-k$, и наоборот, если многочлен $g(x)$ имеет степень $n-k$, и является делителем многочлена x^n-1, то он является порождающим многочленом циклического $[n,k]$-кода.

Лемма 1.5.2. *Пусть C есть циклический (n,k)-код с порождающим многочленом*

$$g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}.$$

Тогда порождающая матрица кода C такова:

$$\begin{pmatrix}
g_0 & & & & & & \\
g_1 & g_0 & & & & & \\
g_2 & g_1 & g_0 & & & & \\
\vdots & g_2 & g_1 & \ddots & & & \\
 & \vdots & g_2 & \ddots & \ddots & & \\
\vdots & & \vdots & \ddots & \ddots & g_0 & \\
g_{n-k} & \vdots & & & \ddots & g_1 & g_0 \\
 & g_{n-k} & \vdots & & & g2 & g_1 \\
 & & g_{n-k} & & & \vdots & g_2 \\
 & & & \ddots & & & \vdots \\
 & & & & \ddots & \vdots & \vdots \\
 & & & & & g_{n-k} & g_{n-k-1} \\
 & & & & & & g_{n-k}
\end{pmatrix}$$

Если $x^n - 1 = g(x)h(x)$, то $h(x)$ называется *проверочным многочленом* кода C.

Теорема 1.5.2. *Код, двойственный к циклическому коду, сам является циклическим. Если* $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ *является проверочным многочленом данного кода (т.е.* $gh = x^n - 1$*), то порождающим многочлено двойственного кода является многочлен*

$$x^k h(1/x) = h_k + h_{k-1} x + \cdots + h_0 x^k.$$

Важным моментом доказательства является тождество:

$$(P^{n-1} u, v) = (v, Pu).$$

Следствие 1.5.1. *Проверочной матрицей для циклического кода с проверочным многчленом* $h(x)$ *будет матрица:*

$$\begin{pmatrix}
h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0 & & & & \\
 & h_k & k_{k-1} & \cdots & \cdots & h_1 & h_0 & & & \\
 & & \ddots & \ddots & & & \ddots & \ddots & & \\
 & & & h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0 & \\
 & & & & h_k & h_{k-1} & \cdots & \cdots & h_1 & h_0
\end{pmatrix}$$

ГЛАВА II. КОНЕЧНЫЕ ПОЛЯ

2.1. Алгебры и многочлены

Все рассматриваемые кольца предполагаются ассоциативными и с единицей.

Пусть K — коммутативное кольцо. *K-алгеброй* называется кольцо R вместе с гомоморфизмом колец $\varphi : K \to R$, причем должно выполняться следующее условие: для любого $\lambda \in K$ и для каждого $r \in R$

$$\varphi(\lambda)r = r\varphi(\lambda).$$

Это условие автоматически выполняется, если кольцо R также является коммутативным. Оно позволяет определить на R структуру K-модуля (левого или правого — все равно):

$$K \times R \to R, \quad (\lambda, r) \mapsto \lambda r = \varphi(\lambda)r.$$

Все идеалы R (левые, правые, двухсторонние) при этом автоматически оказываются K-подмодулями. Гомоморфизм φ будем называть *структурным гомоморфизмом* K-алгебры R.

Гомоморфизмом K-алгебр $f : R_1 \to R_2$ называется такой гомоморфизм колец с единицей, который одновременно является гомоморфизмом K-модулей.

Пусть $\varphi_1 : K \to R_1$ и $\varphi_2 : K \to R_2$ — структурные гомоморфизмы алгебр R_1 и R_2. Тогда $f : R_1 \to R_2$ является гомоморфизмом алгебр тогда и только тогда, если $f\varphi_1 = \varphi_2$.

Рассмотрим несколько примеров алгебр.

Пример 2.1.1. Пусть R — коммутативное кольцо, и $K \subseteq R$ — его подкольцо. Тогда R становится K-алгеброй, причем структурным гомоморфизмом является само включение $K \subseteq R$. В частности, нас будет интересовать случай, когда $R = K[x]$ — кольцо многочленов от одного переменного над коммутативным кольцом K. Это кольцо является K-алгеброй, и мономы $1, x, x^2, \ldots, x^n, \ldots$ можно рассматривать как базис свободного K-модуля, так как любой многочлен является их линейной комбинацией:

$$a_0 \cdot 1 + a_1 \cdot x + \cdots + a_n \cdot x^n,$$

коэффициенты которой принадлежат K, и эта запись является единственно возможной.

Пример 2.1.2. Пусть $\mathbb{Z}$ — кольцо целых чисел. Любое ассоциативное кольцо с единицей R обладает однозначно определенной структурой $\mathbb{Z}$-алгебры. Структурный гомоморфизм $\varphi : \mathbb{Z} \to R$ определяется следующим образом:

$$\varphi(n) = \begin{cases} \overbrace{1_R + \cdots + 1_R}^{n}, & \text{при } n > 0 \\ 0_R & \text{при } n = 0 \\ \overbrace{-1_R - \cdots - 1_R}^{|n|}, & \text{при } n < 0 \end{cases}$$

Здесь 1_R и 0_R обозначают единицу и нуль кольца R. Нетрудное вычисление показывает, что эта формула действительно задает гомоморфизм колец, причем $\varphi(n)r = r\varphi(n)$ для всех $n \in \mathbb{Z}$ и $r \in R$. Вместо $\varphi(n)r$ в дальнейшем будем писать nr. Нетрудно также убедиться, что любой гомоморфизм ассоциативных колец является также и гомоморфизмоим $\mathbb{Z}$-алгебр. Это означает, что понятие алгебры над коммутативным кольцом является более содержательным, чем понятие ассоциативного кольца.

Пусть R есть K-алгебра, и $\varphi : K \to R$ — ее структурный гомоморфизм. Рассмотрим произвольный идеал I в кольце R. Как уже отмечено выше, он является подмодулем в K-модуле R. Это означает, что на факторкольце R/I определена дополнительная структура K-модуля, причем естественная проекция на факторкольцо $\pi : R \to R/I$ является не только гомоморфизмом колец, но и гомоморфизмом модулей. Напомним, что если $\lambda \in K$, $r \in R$, то $\lambda(r + I) = \lambda r + I$. С учетом того, что $\lambda r = \varphi(\lambda)r$, получаем следующее описание структуры K-модуля на R/I: $\lambda(r + I) = \varphi(\lambda)r + I$. С другой стороны, оперделим на R/I структуру K-алгебры, взяв в качестве структурного гомоморфизма суперпозицию гомоморфизмов $K \xrightarrow{\varphi} R \xrightarrow{\pi} R/I$. Так как $\pi(r) = r + I$, то легко убедиться, что структура K-модуля на R/I, опередляемая из структуры K-алгебры, совпадает с той, которая была определена выше. Гомоморфизм π является гомоморфизмом K-алгебр.

Пусть $f : R_1 \to R_2$ — гомоморфизм K-алгебр, $I = Ker(f)$. Известно, что существует инъективный гомоморфизм $\psi : R_1/I \to R_2$, такой, что $f = \psi\pi$, где $\pi : R_1 \to R_1/I$ — естественная проекция, $\pi(r) = r + I$. Явный вид ψ таков: $\psi(r+I) = f(r)$. Отсюда легко вывести, что ψ является гомоморфизмом K-алгебр.

Теорема 2.1.1. *Пусть R — некоторая K-алгебра (не обязательно коммутативная). Для каждого $r \in R$ существует, притом только один, гомоморфизм K-алгебр $h : K[x] \to R$, такой, что $h(x) = r$. При этом $h(\sum\limits_{i=0}^{n} a_i x^i) = \sum\limits_{i=0}^{n} a_i r^i$, где $a_0, a_1, \ldots, a_n \in K$.*

Если $g(x) = \sum\limits_{i=0}^{n} a_i x^i \in K[x]$, то элемент $\sum\limits_{i=0}^{n} a_i r^i \in R$ можно считать результатом подстановки в многочлен $g(x)$ элемента $r \in R$ вместо элемента x. Именно структура K-алгебры на R позволяет это сделать. Таким образом, $h(g(x)) = g(h(x)) = g(r)$.

Пусть K — поле, f — многочлен степени $n \geq 1$, $V_n = \langle 1, x, \ldots, x^{n-1} \rangle$ — подпространство векторного пространства $K[x]$, состоящее из всех многочленов, степени которых строго меньше n. Легко показать, что $K[x] = V_n \oplus (f)$.

Теорема 2.1.2. *Ограничение естественной проекции (гомоморфизма K-алгебр) $\pi : K[x] \to K[x]/(f)$ на подпространство V_n является изоморфизмом между векторными пространствами V_n и $K[x]/(f)$.*

Отсюда следует, что $\dim_K(K[x]/(f)) = deg(f)$, и что базисом $K[x]/(f)$ как векторного пространства над K являются смежные классы $\overline{1} = 1 + (f)$, $\overline{x} = x + (f)$, $\overline{x^2} = \overline{x}^2 = x^2 + (f)$, $\ldots$, $\overline{x}^{n-1} = x^{n-1} + (f)$.

Лемма 2.1.1. *Пусть R — некоторое ассоциативное кольцо с единицей, и пусть I — идеал кольца R. Имеется взаимно-однозначном соответствии между идеалами факторкольца R/I и идеалами R, содержащими идеал I. Соответствие задается следующим образом: пусть $\pi : R \to R/I$ — гомоморфизм проекции на факторкольцо, J — идеал кольца R/I, тогда идеалу J соответствует идеал $\pi^{-1}(J) = \{r \in R | \pi(r) \in J\}$.*

Теорема 2.1.3. *Если R — кольцо главных идеалов, I — идеал в R. Тогда R/I — также кольцо главных идеалов.*

Теорема 2.1.4. *Каждый идеал $K[x]$ — главный, т.е. имеет вид $(g) = K[x]g$ для некоторого $g \in K[x]$.*

Отсюда получаем описание идеалов факторкольца $K[x]/(f)$: это главные идеалы, порожденные образами многочленов $g(x)$, являющихся делителями многочлена $f(x)$. В случае, если многочлены $g(x)$ берутся приведенными (или нормированными; это означает, что старший

коэффициет равен единице), соответствие между идеалами $K[x]/(f)$ и приведенными делителями многочлена $f(x)$ взаимно-однозначно.

Отметим, что использовано следующее свойство: если a, b — элементы коммутативного кольца R, то $(a) \subseteq (b)$ тогда и только тогда, если $b|a$, то есть $a = bc$.

2.2. Конечные поля

Теорема 2.2.1. *Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ является полем тогда и только тогда, если n является простым числом.*

Теорема 2.2.2. *Пусть K — некоторое поле, $f(x) \in K[x]$ — многочлен. Факторкольцо (факторалгебра) $K[x]/(f)$ является полем тогда и только тогда тогда, если многочлен $f(x)$ неприводим над полем K.*

Поля $\mathbb{Z}/p\mathbb{Z}$ обозначаются через $\mathbb{F}_p$ или через $GF(p)$.

Пусть K — некоторое поле. Рассмотрим последовательность элементов этого поля: $1, 1+1, 1+1+1, \ldots, 1+\cdots+1, \ldots$. Возможен случай, когда все элементы в этой последовательности попарно различны. В этом случае говорят, что *характеристика* поля K равна нулю (обозначение: $char(K) = 0$). Поле нулевой характеристики бесконечно, и содержит подполе, изоморфное полю рациональных чисел $\mathbb{Q}$. если поле не является полем с нулевой характеристикой, то в последовательности $1, 1+1, 1+1+1, \ldots, 1+\cdots+1, \ldots$ должны встретиться равные элементы, то есть для некторых $n > m$ должно быть $\overbrace{1+\cdots+1}^{n} = \overbrace{1+\cdots+1}^{m}$. Отсюда следует $\overbrace{1+\cdots+1}^{n-m} = 0$, причем $n - m > 0$. Наименьшее целое положительное число p, обладающее тем свойством, что $\overbrace{1+\cdots+1}^{p} = 0$ в поле K, называется *характеристикой* поля K, обозначение $p = char(K)$.

Лемма 2.2.1. *Если характеристика поля не равна нулю, то она является простым числом.*

Пример 2.2.1. Примеры полей простой характеристики p: это $\mathbb{F}_p$ и $\mathbb{F}_p[x]/(f)$, где p — простое число, f — неприводимый многочлен.

Любое конечное поле является полем простой характеристики.

Лемма 2.2.2. *Пусть K — поле, $char(K) = p > 0$, R — коммутативное кольцо, такое, что $K \subseteq R$ (например, $R = K[x]$), и $a, b \in K$, то $pa = \overbrace{a + \cdots + a}^{p} = 0$, и $(a+b)^p = a^p + b^p$.*

Пусть K — некоторое поле. Рассмотрим на K структуру $\mathbb{Z}$-алгебры из примера 2.1.2, и пусть $\varphi : \mathbb{Z} \to K$ — соответствующий структурный гомоморфизм.

Лемма 2.2.3. *Поле K имеет нулевую характеристику тогда и только тогда, если гомоморфизм φ является инъективным, $Ker(\varphi) = \{0\}$.*

Поле K имеет характеристику $p > 0$ тогда и только тогда, когда ядро гомоморфизма $\varphi : \mathbb{Z} \to K$ является идеалом кольца $\mathbb{Z}$, порожденным простым числом p.

Отсюда (по теореме о гомоморфизме) следует, что если $char(K) = p > 0$, то существует инъективный гомоморфизм полей $\psi : \mathbb{Z}/p\mathbb{Z} \to K$, такой, что $\varphi = \psi\pi$, где $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ — естественная проекция. Явный вид ψ таков: $\psi(n + (p)) = \varphi(n) = \overbrace{1 + \cdots + 1}^{n}$ при $n > 0$, $\psi(n + (p)) = \varphi(n) = \overbrace{-1 - \cdots - 1}^{|n|}$ при $n < 0$, $\psi(0 + (p)) = \varphi(0) = 0$. Но так как все элементы $\mathbb{Z}/p\mathbb{Z}$ исчерпываются смежными классами (классами вычетов) $(p) = 0 + (p), 1 + (p), 2 + (p), \ldots, p - 1 + (p)$, то образ гомоморфизма ψ, который является подполем поля K, состоит только из элементов (все они попарно различны) $0, 1, 1 + 1, \ldots, \overbrace{1 + \cdots + 1}^{p-1}$. Это подполе называется *простым подполем* поля K, и будет иногда обозначаться через K_0. Из построения видно, что $K_0 \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Часто бывает удобно отождествлять простое подполе с полем $\mathbb{F}_p$. Поле K можно рассматривать как алгебру над соим простым подполем. Отсюда вытекает следующая теорема:

Теорема 2.2.3. *Количество элементов в конечном поле характеристики p равно p^n, где $n = \dim_{K_0}(K)$.*

Конечное поле из $q = p^n$ элементов обозначается через $\mathbb{F}_q$ или через $GF(q)$. GF означает Galois Field, т.е. поле Галуа. Далее будет показано, что любое конечное поле определяется количеством своих элементов однозначно с точностью до изоморфизма, и что для каждого простого числа p и натурального $n \geq 1$ существует поле из p^n элементов.

В общей теории полей часто рассматриваются пары полей $K \subseteq F$. Поле F называется *расширением* поля K. Обычно расширением называется вся пара полей. Поле F всегда можно рассматривать как K-алгебру, а значит — как векторное пространство над полем K. *Степенью расширения* называется число $[F : K] = dim_K(F)$ (если размерность конечна).

Напомним, что если $f(x) \in K[x]$, K — поле, $deg(f) = n > 0$, то f имеет в поле K не более n корней.

Теорема 2.2.4. *Все элементы конечного поля $K \subseteq F$, $|K| = q = p^n$, и только они, являются корнями многочлена $x^q - x$.*

Лемма 2.2.4. *Элемент α поля K принадлежит простому подполю тогда и только тогда, если $\alpha^p = \alpha$.*

Теорема 2.2.5. *Если $f(x)$ — многочлен с коэффициентами из простого подполя поля K характеристики p, и α — корень f, то корнями f являются также элементы α^p, α^{p^2}, ..., α^{p^k}, ...*

Лемма 2.2.5. (Первая лемма о делимости)

1. $(x^n - 1)|(x^m - 1) \Leftrightarrow n|m$;
2. $(q^n - 1)|(q^m - 1) \Leftrightarrow n|m$, *где* q — *натуральное число,* $q > 1$.

Теорема 2.2.6. *Пусть F — конечное поле, $char(F) = p$, $|F| = p^n$. Подполе $K \subseteq F$, такое, что $|K| = p^m$, существует тогда и только тогда, если $m|n$. При этом K однозначно определяется как множество корней многочлена $x^{p^m} - x$ в поле F.*

Пусть $\alpha \in F$, где F — расширение поля K. Тогда существует и однозначно определен гомоморфизм K-алгебр $h_\alpha : K[x] \to F$, такой, что $h_\alpha(x) = \alpha$. Если этот гомоморфизм инъективен, то α называется *трансцендентным* над K, если не инъективен, то α называется *алгебраическим* над K. Если поле F конечно, то каждый его элемент является алгебраическим над K.

Элемент α является алгебраическим над K тогда и только тогда, если существует многочлен $f(x) \in K[x]$, такой, что $f(\alpha) = 0$. Все такие многочлены f — это в точности ядро $Ker(h_\alpha)$, которое является идеалом $K[x]$.

Если $[F : K] < \infty$, то любой элемент $\alpha \in F$ является алгебраическим над K. В частности, это так, если поле F конечно.

Теорема 2.2.7. *Для каждого поля K и каждого многочлена $f(x) \in K[x]$ существует расширение полей $K \subseteq F$ такое, что $f(x)$ имеет корень в F. Это расширение можно выбрать конечным, т.е. $[F : K] < \infty$. В частности, если K конечно, то и F можно считать конечным.*

Если $f(x) = f_1(x)f_2(x)$, и $f_(x) \in K[x]$ — неприводимый многочлен, то можно взять $F = K[x]/(f_1)$, и $\alpha = x + (f_1)$ — корень $f(x)$ в F.

Из этой теоремы следует, что для любого многочлена $f(x) \in K[x]$ существует расширение поля K, в котором многочлен f раскладывается на линейные множители, причем если K конечно, то и F также можно считать конечным.

В доказательстве конечности расширния $K \subseteq F$ используется следующее утверждение:

Лемма 2.2.6. *Пусть даны три поля: $K \subseteq F \subseteq L$. Допустим, что $x_1, x_2, \ldots, x_n$ — базис K-алгебры F, а $y_1, y_2, \ldots, y_m$ — базис F-алгебры L. Тогда семейство $\{x_i y_j | 1 \leq i \leq n, 1 \leq j \leq m\}$ будет базисом K-алгебры L. В частности, $[L; K] = [L : F][F : K]$.*

Пусть $K \subseteq F$ — некоторое расширение полей, и пусть $\alpha \in F$ — алгебраический над K элемент. Тогда существует многочлен наименьшей степени $M_\alpha(x) \in K[x]$, такой, что $M_\alpha(\alpha) = 0$. Этот многочлен определен однозначно с точностью до скалярного ненулевого множителя, и называется *минимальным многочленом* элемента α (относительно подполя K).

Лемма 2.2.7. *Минимальный многочлен неприводим в $K[x]$, любой другой многочлен $f \in K[x]$ со свойством $f(\alpha) = 0$ делится на M_α.*

Лемма 2.2.8. *Пусть $g(x) \in K[x]$ — неприводимый многочлен, $F = K[x]/(g)$, $\alpha = x + (g)$ — элемент поля F. Тогда $g(x) = M_\alpha(x)$.*

Пусть дано расширение полей $K \subseteq F$, и $\alpha \in F$. Минимальное подполе поля F, содержащее K и α, которое обозначается через $K(\alpha)$, изоморфно $K[x]/(M_\alpha(x))$. При этом $[K(\alpha) : K] = deg(M_\alpha(x))$. Если $M_\alpha(x) = M_\beta(x)$, то $K(\alpha) \cong K(\beta)$ как K-алгебры.

Лемма 2.2.9. *Если $|F| = q$, $K \subseteq F$, $\alpha \in F$, и $M_\alpha(x) \in K[x]$ — минимальный многочлен элемента α (над K), то $M_\alpha(x)$ делит $x^q - x$, при этом у $x^q - x$ нет кратных корней ни в каком расширении поля K, а значит, то же самое верно и для $M_\alpha(x)$.*

2.3. Теорема о примитивном элементе и ее следствия

Пусть G — некоторая группа, $a \in G$. *Порядок* a (обозначение $\text{пор}(a)$) — это наименьшее положительное число k, обладающее свойством: $a^k = 1$. Если порядок конечен, то все элементы $1, a, \ldots, a^{k-1}$ попарно различны, и это множество есть подгруппа $\langle a \rangle$, порожденная элементом a. Так как $k = \text{пор}(a) = |\langle a \rangle|$, то по теореме Лагранжа порядок элемента группы делит порядок группы $|G|$ (если он конечен), и $a^{|G|} = 1$. Если $a^m = 1$, то m делится на порядок элемента a.

Лемма 2.3.1. *Если* $пор(a) = k$, *то* $пор(a^j) = \dfrac{k}{НОД(k, j)}$.

Лемма 2.3.2. *Пусть в группе* G *имеются два элемента* a *и* b, *такие, что* $ab = ba$, *причем* $пор(a) = n$, $пор(b) = m$. *Допустим, что* m *не делит* n (n *не делится на* m). *Тогда существует элемент* c, *порядок которого равен*

$$\frac{nm}{НОД(n, m)} > n.$$

На первом этапе доказательства показывается, что если $\text{НОД}(n, m) = 1$, то $\text{пор}(ab) = nm$.

Теорема 2.3.1. *Любая конечная подгруппа группы ненулевых элементов произвольного поля является циклической.*

В частности, группа обратимых элементов конечного поля циклична. Образующие элементы этой группы называются *примитивными элементами* поля. Таким образом, если $|K| = q$, и α — примитивный элемент поля K, то $K = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$, и $\alpha^{q-1} = 1$.

Теорема 2.3.2. *Любое конечное поле изоморфно полю вида* $\mathbb{F}_p[x]/(f(x))$, *где* $f(x)$ — *неприводимый многочлен из* $\mathbb{F}_p$.

2.4. Строение конечных полей

Лемма 2.4.1. (Вторая лемма о делимости)

1. *Пусть для многочлена $g(x)$ имеет место $g|(x^n-1)$, и n наименьшее с этим свойством. Тогда*

$$g(x)|(x^\ell-1) \Leftrightarrow n|\ell$$

Число n в этом случае называется показателем *многочлена $g(x)$.*

2. *Пусть для натурального a имеет место $a|(q^n-1)$, где $q>1$ — натуральное число, и n наименьшее с этим свойством. Тогда*

$$a|(q^\ell-1) \Leftrightarrow n|\ell$$

Число $n>1$ со свойством $a|(q^n-1)$ существует тогда и только тогда, если $\text{НОД}(a,q)=1$.

Лемма 2.4.2. *Пусть K — конечное поле, $q=|K|$, $g(x)\in K[x]$ — нормированный неприводимый многочлен. Тогда показатель $g(x)$ существует.*

Теорема 2.4.1. *Пусть $g(x)\in K[x]$ — неприводимый многочлен, $m=deg(g(x))$, и n — показатель $g(x)$. Тогда $n|(q^m-1)$, и если $n|(q^\ell-1)$ для некоторого ℓ, то $m\le\ell$.*

Теорема 2.4.2. *Пусть F — конечное поле, $K\subset F$, $\alpha\in F$, тогда показатель минимального многочлена $M_\alpha(x)\in K[x]$ совпадает с порядком элемента α.*

Элемент α примитивен тогда и только тогда, если показатель $M_\alpha(x)$ равен q^m-1.

Теорема 2.4.3. *Пусть $K\subset F$, $|K|=q$, $\alpha\in F$, $m=deg(M_\alpha(x))$. Тогда все корни $M_\alpha(x)$ — это $\alpha,\alpha^q,\alpha^{q^2},\dots,\alpha^{q^{m-1}}$. Если β — корень $M_\alpha(x)$, то $M_\beta(x)=M_\alpha(x)$. Все корни $M_\alpha(x)$ имеют один и тот же порядок.*

Теорема 2.4.4. *Пусть K — конечное поле, $q=|K|$, $g(x)\in K[x]$ — нормированный неприводимый многочлен, $m=deg(g(x))$. Тогда*

$$g(x)|(x^{q^\ell-1}-1) \Leftrightarrow m|\ell.$$

Теорема 2.4.5. *Пусть K — конечное поле, $q = |K|$. Тогда*

$$x^{q^\ell} - x = \prod_{deg(g)|\ell} g(x),$$

где произведение берется по всем неприводимым нормированным $g \in K[x]$, степени которых делят ℓ.

У этой теоремы есть несколько важных следствий.

Теорема 2.4.6. *Любые два конечных поля с одним и тем же количеством элементов изоморфны (как векторные пространства над простым подполем).*

Пусть $K = GF(q)$, N_j обозначает количество неприводимых многочленов из $K[x]$, имеющих степень j. Очевидно, что $N_1 = q$. Из $x^{q^\ell} - x = \prod_{deg(g)|\ell} g(x)$ следует, что

$$q^\ell = \sum_{j|\ell} jN_j.$$

Отсюда можно вывести следующее утверждение:

Теорема 2.4.7. *$N_j > 0$ для всех $j \geq 1$. В частности, это значит, что над любым конечным полем существуют неприводимые многочлены любых степеней.*

Отсюда следует утверждение, которым завершается описание структуры конечных полей:

Теорема 2.4.8. *Для любого простого числа p и произвольного целого $m \geq 0$ существует конечное поле из p^m элементов. Это поле определено однозначно с точностью до изоморфизма.*

2.5. Неприводимые многочлены над конечными полями

Опишем одну конструкцию, позволяющую строить неприводимые над полем K многочлены. Пусть даны натуральные числа q и n, НОД$(q, n) = 1$. Тогда $\overline{q} = q + n\mathbb{Z}$ — обратимый элемент в $\mathbb{Z}/n\mathbb{Z}$. Рассмотрим подгруппу G в группе всех обратимых элементов $\mathbb{Z}/n\mathbb{Z}$, порожденную элементом $\overline{q}$. Группа G действует на $\mathbb{Z}/n\mathbb{Z}$ по правилу

$(a,b) \mapsto ab$, и, таким образом, все множество $\mathbb{Z}/n\mathbb{Z}$ разбивается на непересекающиеся орбиты этого действия. Если отождествить $\mathbb{Z}/n\mathbb{Z}$ с множеством $0, 1, 2, \ldots, n-1$ (выбирая в каждом смежном классе минимальный неотрицательный представитель), то орбита, в которой содержится элемент j, описывается следующим образом. Это множество чисел

$$j, jq, jq^2, \ldots, jq^{m-1},$$

взятых по модулю n (т.е.фактически берутся остатки от деления этих чисел на n), причем m должно быть минимальным числом со свойством $jq^m \equiv j \pmod{n}$.

Описанные таким образом орбиты называются в литературе по теории кодирования $(q,n)-$циклами.

Теорема 2.5.1. *Пусть дано расширение полей $K \subseteq F$, $|K| = q$, $|F| = q^\ell$. Выберем примитивный элемент α поля F. Тогда существует взаимно-однозначное соответствие между неприводимыми многочленами из $K[x]$, степени которых делят ℓ (исключая многочлен x), и $(q, q^\ell - 1)-$циклами.*

Это соответствие строится по разложению

$$x^{q^\ell - 1} - 1 = \prod_{deg(g)=m, m|\ell} g(x)$$

где в произведении справа рассматриваются все неприводимые многочлены, степени которых делят ℓ, за вычетом многочлена x. Если взять один из таких многочленов $g(x)$, то в поле F он раскладывается в произведение линейных множителей:

$$g(x) = (x - \alpha^j)(x - \alpha^{jq})(x - \alpha^{jq^2}) \ldots (x - \alpha^{jq^{m-1}})$$

Тогда степени $j, jq, jq^2, \ldots, jq^{m-1}$, взятые по модулю $q^\ell - 1$ (это порядок элемента α) образуют $(q, q^\ell - 1)-$цикл, и проверяется, что так получаются все циклы.

Отсюда, в частности, следует, что если взять любой $(q, q^\ell - 1)-$цикл,

$$j, jq, jq^2, \ldots, jq^{m-1},$$

и примитивный элемент α в поле F, содержащем K и таком, что $|F| = q^\ell$, то многочлен

$$(x - \alpha^j)(x - \alpha^{jq})(x - \alpha^{jq^2}) \ldots (x - \alpha^{jq^{m-1}})$$

принадлежит кольцу $K[x]$ (после перемножения и выполнения всех операций с коэффициентами все коэффициенты окажутся в поле K), и является неприводимым.

ГЛАВА III. КОДЫ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА

3.1. Циклические коды и корни порождающих многочленов

Пусть $g(x) \in K[x]$ — порождающий многочлен $[n,k]-$кода, и предположим, что $g = g_1(x)g_2(x)\dots g_\ell(x)$, где все $g_i(x)$ — различные неприводимые многочлены из $K[x]$. Это условие равносильно тому, что в любом расширении $K \subseteq F$ поля K, в котором $g(x)$ раскладывается на линейные множители, у него нет кратных корней. В дальнейшем будут рассматриваться только такие порождающие многочлены.

Пусть $K \subseteq F$ — расширение поля K, в котором многочлен $g(x)$ раскладывается на линейные множители (такое расширение всегда существует). Выберем по одному корню для каждого множителя $g_i(x)$, например, пусть α_i есть корень $g_i(x)$ при $1 \le i \le \ell$.

Теорема 3.1.1. *$u(x) \in C$ тогда и только тогда, если $u(\alpha_1) = \dots = u(\alpha_\ell) = 0$.*

Если $u(x) = u_0 + u_1x + \dots + u_{n-1}x^{n-1}$, то это равносильно тому, что столбец $u = (u_0, u_1, \dots, u_{n-1})^T$ является решением системы $Hu = 0$, где H есть матрица

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_\ell & \alpha_\ell^2 & \cdots & \alpha_\ell^{n-1} \end{pmatrix}$$

Из этой матрицы можно построить обычную проверочную матрицу кода C, т.е. матрицу с компонентами из поля K размером $(n-k)\times n$, имеющую ранг $n-k$.

Циклическими кодами Хэмминга называются циклические коды над полем $\mathbb{F}_2$, порождающие многочлены которых являются минимальными многочленами примитивных элементов полей $\mathbb{F}_{2^m} = GF(2^m)$.

Теорема 3.1.2. 1) *Циклический код Хэмминга является $[2^m - 1.2^m - 1 - m]-$кодом, и его минимальное кодовое расстояние равно трем.*

2) *Не обязательно циклический $[2^m - 1, 2^m - m - 1]$-код Хэмминга $\mathcal{H}_m$ эквивалентен циклическому коду Хэмминга с порождающим многочленом — минимальным многочленом примитивного элемента поля $GF(2^m)$.*

3.2. Основные теоремы

Исходные данные: $K = GF(q)$, $\alpha \in GF(q^m)$ — элемент порядка n, где n делит $q^m - 1$, и дан код C длины n с порождающим многочленом $g(x)$. Пусть α^{e_1}, α^{e_2}, $\ldots$, $\alpha^{e_{n-k}}$ — все корни многочлена $g(x)$. Предположим, что кратных корней нет. Это означает, что в разложении $g(x)$ на неприводимые множители каждый неприводимый множитель имеет кратность единица, и поэтому применим способ построения проверочной матрицы, описанный в предыдущем параграфе.

Рассмотрим множество $e = \{e_1, \ldots, e_{n-k}\}$. В случае необходимости можно считать, что $0 \le e_i < n - 1$ для всех i, так как имеется возможность заменять e_i на остаток от деления e_i на n. Однако это не является обязательным требованием.

Теорема 3.2.1. *Минимальное расстояние кода C больше, чем наибольшее количество последовательных целых чисел в множестве e.*

Эта нижняя граница кодового расстояния (обозначим его через d_0) называется *нижней БЧХ-границей* минимального кодового расстояния (или *конструктивным кодовым расстоянием*) кода C.

В доказательстве теоремы 3.2.1 используется следующая лемма:

Лемма 3.2.1. *При сделанных выше предположениях $u(x) \in C$ тогда и только тогда, если $u(\alpha_1) = \cdots = u(\alpha_{n-k}) = 0$.*

Если $u(x) = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$, то это равносильно тому, что столбец $u = (u_0, u_1, \ldots, u_{n-1})^T$ является решением системы $Hu = 0$, где H есть матрица

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \cdots & \alpha_{n-k}^{n-1} \end{pmatrix}$$

Теорема 3.2.2. *При тех же условиях что и в теореме 3.2.1, пусть среди корней многочлена $g(x)$ есть подмножество вида α^e, α^{e+j}, $\ldots$, $\alpha^{e+j(d_0-2)}$, причем НОД$(j, n) = 1$. Тогда $d(C) > d_0$. В этой теореме e может быть любым целым числом, в том числе и отрицательным.*

Рассмотрим $\alpha \in \mathbb{F}_{q^m} = GF(q^m)$, причем порядок α равен n и n делит $q^m - 1$. Пусть $M_i(x) \in GF(q)[x]$ есть минимальный многочлен

элемента α^i. Зафиксируем m_0 и d_0 и рассмотрим циклический код с порождающим многочленом

$$g(x) = \text{НОК}(M_{m_0}(x), M_{m_0+1}(x), \ldots, M_{m_0+d_0-2}(x)).$$

Взятие НОК означает, что если в списке есть совпадающине многочлены, то в произведение должен войти только один из них. В результате $g(x)$ должен оказаться произведением различных неприводимых многочленов, $g(x) = g_1(x) \ldots g_l(x)$. При этом все корни многочленов $g_i(x)$, $1 \leq i \leq l$, будут степенями элемента α, а так как α есть корень многочлена $x^n - 1$, то каждый g_i должен делить $x^n - 1$. Так как многочлены $g_1, \ldots, g_l$ по построению попарно взаимно просты, то их произведение, то есть многочлен $g(x)$, также будет делителем $x^n - 1$. Таким образом, $g(x)$ будет порождающим многочленом некоторого циклического кода длины n с конструктивным кодовым расстоянием, равным d_0. Коды такого вида называются *кодами Боуза-Чоудхури-Хоквингема* (БЧХ-кодами). По теореме 3.2.2 минимальное расстояние такого кода больше числа d_0.

3.3. Коды Рида-Соломона и другие примеры

Лемма 3.3.1. *Циклический код Хэмминга является кодом БЧХ.*

Пусть α — примитивный элемент $GF(q)$. Тогда минимальный многочлен α^i над $GF(q)$ — это $x - \alpha^i$. *Коды Рида-Соломона* — это коды БЧХ с порождающими многочленами вида $g(x) = \prod_{i=1}^{r}(x - \alpha^i)$. Длина таких кодов равна $n = q - 1$, число информационных символов равно $n - r = q - 1 - r$. По теореме 3.2.2 минимальное расстояние кода Рида-Соломона больше или равно $r + 1$. Из неравенства Синглтона теперь следует, что что минимальное кодовое расстояние для кодов совпадает с нижней БЧХ-границей, и равно $r + 1$. Это значит, что коды Рида-Соломона являются кодами МДР. Код, двойственный к коду Рида-Соломона, также является кодом Рида-Соломона.

Рассмотрим еще один пример кодов БЧХ. Пусть α — элемент порядка $n = q + 1$ в поле $GF(q^2)$. Положим $d_0 = 2t + 1$, и рассмотрим многочлен $g(x) = (x - \alpha^{-t})(x - \alpha^{-t+1}) \ldots (x - \alpha^{t-1})(x - \alpha^t)$. Минимальные многочлены элементов α^i имеют степени либо 1 (и тогда это

$x - \alpha^i$), либо 2. В последнем случае корнем такого минимального многочлена, кроме α^i, является и элемент $(\alpha^i)^q$. Но так как $\alpha^q = \alpha^{-1}$, то $\alpha^{iq} = \alpha^{-i}$. Это значит, что коэффициенты $(x-\alpha^i)(x-\alpha^{-i})$ принадлежат полю $GF(q)$, а значит, и коэффициенты всего $g(x)$ принадлежат $GF(q)$, и $g(x)$ есть произведение различных минимальных многочленов элементов $1, \alpha^{\pm 1}, \alpha^{\pm 2}, \ldots, \alpha^{\pm t}$. Коэффициенты многочлена $g(x)$ принадлежат полю $GF(q)$, он удовлетворяет условиям теоремы 3.2.2 и порождает БЧХ-код, минимальное расстояние которого совпадает с нижней БЧХ-границей (и равно $2t+2$). Построенный код является кодом МДР.

Рассмотрим БЧХ-коды в случае $q = 2$. Пусть α — примитивный элемент поля $GF(2^m)$, и $M_i(x)$ — минимальный многочлен элемента α^i. Тогда каждый элемент вида α^{2r} есть корень некоторого $M_{2l+1}(x)$, где $2l+1 < 2r$. Следовательно, если взять $m_0 = 1$, $d_0 = 2t_0 + 1$, то соответствующий БЧХ-код имеет своим порождающим многочленом многочлен

$$g(x) = \text{НОК}(M_1(x), M_3(x), \ldots, M_{2t_0-1}(x)).$$

Степень каждого $M_i(x)$ не превосходит m. Отсюда выводится, что для любых целых m и $t_0 < n/2$ (где $n = 2^m - 1$) существует двоичный БЧХ-код длины n, исправляющий все комбинации из не более чем t_0 ошибок, и содержащий не более чем mt_0 проверочных символов (т.е. размерность кода $\leq mt_0$).

ГЛАВА IV. КОДЫ РИДА - МАЛЛЕРА

4.1. Пространства булевых функций

Пусть $K = \mathbb{F}_2 = GF(2) = \{0, 1\}$, и $m \geq 1$. Рассмотрим множество $\mathcal{B}_m$ всех функций от m переменных вида $f : K^m \to K$. Отображения такого вида принято называть *булевыми функциями*. Множество $\mathcal{B}_m$ булевых функций m от переменных является коммутативным ассоциативным кольцом, и даже алгеброй над полем $\mathbb{F}_2$. Это, в частности, означает, что для каждого $a \in \mathcal{B}_m$ выполняется равенство $2a = a + a = 0$. Особенностью колец $\mathcal{B}_m$ является также то, что в них для каждого элемента a имеет место равенство $a^2 = a$. Кольца с такими свойствами называются *булевыми*. Имеется тесная связь между булевыми кольцами и булевыми алгебрами, но нам она не потребуется.

В теории кодирования алгебры $\mathcal{B}_m$ используются как векторные пространства над полем $\mathbb{F}_2$, обладающие некоторыми специальными свойствами. Эти свойства позволяют строить важные классы кодов — подпространств простанств $\mathcal{B}_m$. Но прежде чем такое построение станет возможным, необходимо выяснить, как устроены алгебры $\mathcal{B}_m$.

Определим на $\mathcal{B}_m$ операции сложения, умножения, и умножения на элементы K. Пусть $\alpha = (\alpha_1, \ldots, \alpha_m)$ — произвольный элемент K^m, $f, g \in \mathcal{B}_m$, $\lambda \in K$. Положим

$$(f + g)(\alpha) = f(\alpha) + g(\alpha), \quad (fg)(\alpha) = f(\alpha)g(\alpha), \quad (\lambda f)(\alpha) = \lambda \cdot f(\alpha).$$

Определим также функцию $\mathbf{0} \in \mathcal{B}_m$, значение которой равно нулю для любых аргументов, и функцию $\mathbf{1} \in \mathcal{B}_m$, значение которой для любых аргументов равно единице.

Теорема 4.1.1. *Множество $\mathcal{B}_m$ с определенными выше операциями становится ассоциативным коммутативным кольцом с единицей $\mathbf{1}$ и нулем $\mathbf{0}$, а также векторным пространством над полем K, причем для любых $\lambda \in K$ и $f, g \in \mathcal{B}_m$ выполняются равенства:*

$$\lambda(fg) = (\lambda f)g = f(\lambda g).$$

Кроме того, для каждой функции $f \in B_m$ выполнны равенства:

$$f + f = 0, \quad ff = f^2 = f.$$

Мы будем рассмаривать некотороые коды над полем $K = \mathbb{F}_2 = GF(2)$ как подпространства векторного пространства $\mathcal{B}_m$, причем вес Хэмминга будет вычисляться относительно одного специального базиса, который строится следующим образом.

Для каждого $\alpha = (\alpha_1, \ldots, \alpha_m) \in K^m$ определим функцию e_α так, что

$$e_\alpha(\alpha) = 1 \quad \text{и} \quad e_\alpha(\beta) = 0$$

при $\beta \neq \alpha$, $\beta \in K^m$.

Теорема 4.1.2. *Множество функций e_α при всевозможных $\alpha \in K^m$ образует базис векторного пространства $\mathcal{B}_m$ над K. Для любой функции $f \in \mathcal{B}_m$ имеет место равенство:*

$$f = \sum_{\alpha \in K^m} f(\alpha) e_\alpha \tag{4.1.1}$$

Теорема 4.1.3. *Выполняются соотношения:*

$$e_\alpha^2 = e_\alpha, \quad e_\alpha e_\beta = \mathbf{0} \ \text{ при } \ \alpha \neq \beta, \quad \sum_{\alpha \in K^m} e_\alpha = \mathbf{1}.$$

Отсюда следует, что

$$\mathcal{B}_m = \bigoplus_{\alpha \in K^m} B_m e_\alpha \tag{4.1.2}$$

причем $\mathcal{B}_m e_\alpha = \{\mathbf{0}, e_\alpha\}$ — одномерное подпространство (и подкольцо, изоморфное полю K). Тем самым определено разложение $\mathcal{B}_m$ как ассоциативного кольца в прямое произведение 2^m экземпляров поля K.

Для каждого i, $1 \leq i \leq m$, обозначим через x_i функцию из K^m в K, отображающую $\alpha = (\alpha_1, \ldots, \alpha_i, \ldots, \alpha_m)$ в α_i. Для $\alpha_i \in K$ определим функцию $x_i^{(\alpha_i)}$, полагая ее равной x_i при $\alpha_i = 1$ и $\mathbf{1} + x_i$ при $\alpha_i = 0$.

Лемма 4.1.1. *Для любого α имеет место равенство:*

$$e_\alpha = x_1^{(\alpha_1)} x_2^{(\alpha_2)} \ldots x_m^{(\alpha_m)}.$$

Теорема 4.1.4. *Множество мономов*

$$\mathbf{1}, x_1, \ldots, x_m, x_1 x_2, \ldots, x_{i_1} x_{i_2}, \ldots, (x_{i_1} \ldots x_{i_s}), \ldots, (x_1 x_2 \ldots x_m)$$

образует базис векторного пространства $\mathcal{B}_m$. Здесь $1 \leq i_1 < i_2 < \cdots < x_{i_s} \leq m$ для всех возможных s, $0 \leq s \leq m$.

Таким образом, любая булева функция f обладает однозначно определенным представлением в виде:

$$f = \sum_{s=0}^{m} \sum_{i_1<\cdots<i_s} \xi_{i_1,\ldots,i_s}(x_{i_1} \ldots x_{i_s}) \tag{4.1.3}$$

Здесь $\xi_{i_1,\ldots,i_s} \in K$.

Таким образом, булевы функции можно записывать в виде, похожем на многочлены (полиномы). Особенностью является то, что все переменные входят только в первой степени (ибо $x_i^2 = x_i$). В частности, определена степень булевой функции. Полагая $deg(x_{i_1} \ldots x_{i_s}) = s$, определяем степень $deg(f)$ как максимальное s, для которого существует $\xi_{i_1,\ldots,i_s} \neq 0$.

4.2. Свойства кодов Рида-Маллера

Теорема 4.2.1. *Вес Хэмминга монома $x_{i_1} \ldots x_{i_r} \in \mathcal{B}_m$ равен 2^{m-r} ($r \geq 0$).*

Код Рида-Маллера $\mathcal{R}(r,m)$ степени r есть подпространство в векторном пространстве $\mathcal{B}_m$, состоящее из полиномов степеней, не превосходящих r. Это $[n,k]$-код, где $n = 2^m$, $k = C_n^0 + C_n^1 + \cdots + C_n^r$.

Лемма 4.2.1. *В коде $\mathcal{R}(1,m)$ каждое ненулевое кодовое слово имеет вес, равный либо 2^m, либо 2^{m-1}.*

Для вычисления кодового расстояния кодов Рида-Маллера нам потребуется один факт, относящийся к произвольным кодам над полем $\mathbb{F}_2$ Пусть C_1 есть некоторый $[n,k_1]$-код с минимальным расстоянием d_1, а C_2 есть $[n,k_2]$-код с минимальным расстоянием d_2. Оба кода рассматриваются над полем $\mathbb{F}_2 = GF(2)$. Полагаем

$$C = \left\{ \begin{pmatrix} u \\ u+v \end{pmatrix} \in K^{2n} | u \in C_1, v \in C_2 \right\}.$$

Обозначим этот код через $(C_1|C_1+C_2)$.

Теорема 4.2.2. *$(C_1|C_1+C_2)$ есть линейный $[2n, k_1+k_2]$-код с минимальным расстоянием, равным* $\min(2d_1, d_2)$.

Теорема 4.2.3. *Код $\mathcal{R}(r+1,m+1)$ эквивалентен коду $(\mathcal{R}(r+1,m)|\mathcal{R}(r+1,m)+\mathcal{R}(r,m))$.*

Теорема 4.2.4. $d(\mathcal{R}(r,m)) = 2^{m-r}$.

Теорема 4.2.5. $\mathcal{R}(r,m)^{\perp} = \mathcal{R}(m-r-1,m)$.

Список литературы

[1] Аршинов М.Н., Садовский Л.Е. Коды и математика. — М.:Наука. Гл. ред. физ.-мат. лит, 1983. — 143 с.

[2] Берлекэмп Э. Алгебраическая теория кодирования. — М.:“Мир”, 1971. — 478 с.

[3] Блейхут Р. Теория и практика кодов, контролирующих ошибки. — : “Мир”, 1986. — 576 с.

[4] Вернер М. Основы кодирования. — М.: Техносфера, 2004. — 288 с.

[5] Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. — М.: МЦНМО, 2003. — 504 с.

[6] Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под ред. чл.-кор. РАН Ю.Б.Зубарева. — М.: Горячая линия–Телеком, 2004. — 126 с.

[7] Касами Т., Токура Н., Ивадари Ё., Инагаки Я. Теория кодирования. — М.:“Мир”, 1978. — 576 с.

[8] Кострикин А.И. Введение в алгебру. Часть III. Основные структуры. — 2-е изд. — М.: Физико-математическая литература, 2001. — 272 с.

[9] Ленг С. Алгебра. — М.:“Мир”, 1968. — 564 с.

[10] Лидл Г., Нидеррайтер Г. Конечные поля. Том 1, Том 2. — М.:“Мир”, 1988. — 822 с.

[11] Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.

[12] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.— 744 с.

[13] Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. — М.: Техносфера, 2005. — 320 с.

[14] Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. — М.: “Мир”, 1976. — 594 с.