Министерство образования и науки Украины
Одесский национальный университет им. И.И. Мечникова

Теория кодирования

Варбанец С.П.

Одесса, 2013

Печатается по решению Ученого Совета ИМЭМ ОНУ
от 19 сентября 2013 года, протокол №1

составители: к. ф.-м. н. С.П. Варбанец

рецензенты: д. ф.-м. н. Ю.Г. Леонов,
к. ф.-м. н. С.М. Покась

Оглавление

Введение

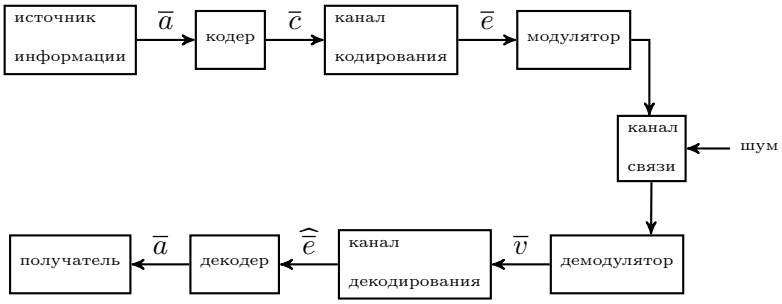
Одна из важнейших научно-технических проблем на современном этапе - создание автоматизированных систем управления и контроля для выполнения различных задач. В процессе автоматизированного управления и контроля происходит интенсивный обмен информацией между отдельными частями систем, причём объём информации, а также скорости обработки и передачи её постоянно растут. Всё более высокие требования предъявляются к достоверности передаваемых сообщений, что при водит к необходимости применять специальные меры, снижающие частость появления ошибок до некоторого допустимого уровня.

Одной из наиболее действенных мер является использование помехоустойчивого кодирования.

В предлагаемом курсе лекций по теории кодирования(часть первая) излагаются принципы построения различных кодов и методов их декодирования, анализы этих кодов и их классификации. Рассматриваются преимущественно двоичные коды. Рассмотрен ряд тестовых примеров по теории линейных кодов.

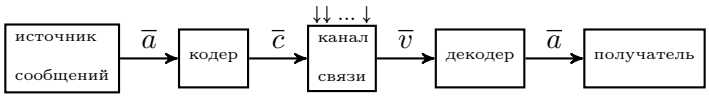
Блочные линейные коды

Начало математической теории кодирования восходит к основополагающей статье Клода Шеннона(1948г.) и изобретению кодов Хемминга(1950). Так началась история помехоустойчивого кодирования. Источник и получатель информации связаны между собой следующей схемой канонической цифровой системой связи.



В кодере входное входное сообщение записывается в цифровую последовательность $\overline{a}$ (информационное слово) в алфавите $\mathbb{F}_q$ (чаще всего в битах). В канале кодера информационное слово преобразуется (кодируется) в кодовое слово $\overline{c}$, записываемое в том же алфавите $\mathbb{F}_q$. Это наиболее важная часть кодирования. Поскольку дискретные символы не пригодны для передачи по физическим каналам связи, то используется модулятор (запись единиц алфавита), через который преобразованное сообщение поступает в канал связи, на который могут воздействовать шумы, а затем это физическое сообщение (вообще говоря, искаженное) поступает в демодулятор, где оно преобразуется в цифровую последовательность $\overline{v}$. В канале декодера исправляются ошибки (если это удаётся сделать) и получаем цифровую последовательность $\widehat{\overline{c}}$ (обычно $\widehat{\overline{c}} = \overline{c}$). В декодере $\widehat{\overline{c}}$ преобразуется в информационное слово $\widehat{\overline{a}}$ и направляется получателю. В идеале $\widehat{\overline{a}} = \overline{a}$, а иначе возникает ошибка декодирования.

В нашем курсе мы не будем рассматривать работу модулятора и демодулятора. Упрощённая схема имеет вид:



Данные, поступающие в систему связи от источника информации, прежде всего обрабатываются кодером источника, который представляет эти данные в некотором цифровом алфавите (например, в виде последовательности символов из конечного поля $\mathbb{F}_q$). Таким образом, входной сигнал от источника информации записывается в виде **информационного слова** $\overline{a}$ (это конеч-

ная последовательность символов в выбранном алфавите $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$). Кодер канала преобразует информационное слово $\overline{a}$ в более длинное слово $\overline{c}$ (обычно записываемое в том же алфавите $\mathbb{F}_q$), которое называется **кодовым словом**. Затем модулятор преобразует каждый символ кодового слова в соответствующий аналоговый символ из конечного множества допустимых аналоговых символов. Последовательность аналоговых символов передаётся по каналу, в котором могут возникать различные шумы, искажения и интерференция. Поэтому выход канала, вообще говоря, отличается от входа. Демодулятор преобразует каждый полученный на входе канала символ в последовательность символов выбранного цифрового алфавита. Демодулированная последовательность называется **принятым словом**, мы его будем обозначать символом $\overline{v}$. Из-за потенциальных ошибок, вообще говоря, $\overline{v} \neq \overline{c}$. Задача декодера, используя избыточную запись $\overline{v}$ для информационного слова $\overline{a}$, восстановить соответствующее кодовое слово $\overline{c}$, а затем и $\overline{a}$.

Пример 1. Пусть $\overline{a} = (110)$ в алфавите $\mathbb{F}_2 = \{0, 1\}$. Обозначим

$$\overline{c} = (111111111100000).$$

Слово $\overline{c}$ получено из $\overline{a}$ повторением каждого символа из $\overline{a}$ пять раз. В результате зашумления канала было принято слово $\overline{v} = (110110011100011)$. Мы видим, что в каждой последовательной пятерке символов

$$11011'00111'00011$$

чаще встречаются, соответственно, символы $1, 1, 0$, а потому заключаем, что кодовое слово

$$\overline{c} = (111111111100000).$$

Использованные код называется **кодом с повторением**. Он надежен, но очень медленный.

Пример 2. Каждому информационному слову $\overline{a}$ длины k, $\overline{a} = (a_1, \ldots, a_k)$ в алфавите $\mathbb{F}_2$ сопоставляем кодовое слово $\overline{c}$ длины $k+1$, $\overline{c} = (c_1, \ldots, c_k, c_{k+1})$,

где $c_i = a_i$, если $1 \le i \le k$, и $c_{k+1} = a_1 + \cdots + a_k$. Такой код называется **кодом с проверкой на четность**. Если при прохождении канала связи в кодовом слове допущено не более одной ошибки, то по принятому слову $\overline{v}$ можно это узнать, хотя искаженный символ определить не удастся.

Из приведённых примеров видно, что увеличение длины кодовых слов, вообще говоря, увеличивает способности кода к восстановлению кодового слова после искажения его символов в канале связи.

В дальнейшем мы будем изучать так называемые блочные коды. Это значит, что рассматриваем информационные слова в алфавите $\mathbb{F}_q$ одной и той же длины k. Ясно, что множество информационных слов есть пространство $\mathbb{F}_q^k = \{(a_1, \ldots, a_k) |\ a_i \in \mathbb{F}_q,\ i = 1, \ldots, k\}$. Мощность этого множества равна q^k. Каждому информационному слову $\overline{a}$ сопоставляем слово $\overline{c} \in \mathbb{F}_q^n$. Так как различным информационным словам должны соответствовать различные кодовые слова, то мощность множества C кодовых слов также равна q^k, а потому для $k < n$ имеем $|C| = q^k < q^n$, и значит, C - собственное подмножество в $\mathbb{F}_q^n$.

Таким образом, чтобы задать кодирование информационных слов длины k в кодовые слова длины n, достаточно указать взаимно-однозначное отображение $\mathbb{F}_q^k$ в $\mathbb{F}_q^n$. Так как наиболее естественными (и легко реализуемыми) отображениями линейного пространства $\mathbb{F}_q^k$ в $\mathbb{F}_q^n$ являются линейные отображения, то образы таких отображений называются **линейными кодами**. Следовательно, линейным кодом для информационных слов из $\mathbb{F}_q^k$ называется любое подпространство $C \subset \mathbb{F}_q^n$ размерности k. Линейный код длины n с длиной информационных слов k мы обозначаем $C(n, k)$-код.

Итак, чтобы построить линейный (n, k)-код в алфавите $\mathbb{F}_q$ и описать процедуру кодирования в этом коде, мы поступаем следующим образом:

Выбираем k линейно независимых векторов в пространстве $\mathbb{F}_q^n$: $\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_k$. Их линейная оболочка

$$L(\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_k) := \left\{ \sum_{i=1}^{k} \alpha_i \overline{g}_i \mid .\ \ \alpha_1 \ldots, \alpha_k \in \mathbb{F}_q \right\}$$

образует линейный (n, k)-код.

Теперь сам (n, k)-код как множество кодовых слов определен. Но процедура кодирования, то есть правило перехода информационных слов в кодовые, определяется конкретным изоморфным отображением

$$\mathbb{F}_q^k \stackrel{\varphi}{\to} L(\overline{g}_1, \ldots \overline{g}_k).$$

Поскольку изоморфизм линейных пространств вполне определяется правилом сопоставления базисных векторов этих пространств, то зафиксируем в пространстве информационных слов $\mathbb{F}_q^k$ стандартный базис

$$\overline{f}_1 = (1, 0, 0, \ldots, 0),$$
$$\overline{f}_2 = (0, 1, 0, \ldots, 0),$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\overline{f}_k = (0, 0, 0, \ldots, 1).$$

Векторы $\overline{g}_i$ запишем в координатной форме для стандартного базиса пространства $\mathbb{F}_q^n$:

$$\overline{g}_1 = (g_{11}, g_{12}, \ldots, g_{1n}),$$
$$\overline{g}_2 = (g_{11}, g_{12}, \ldots, g_{1n}),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\overline{g}_k = (g_{11}, g_{12}, \ldots, g_{1n})$$

Сопоставление $\overline{f}_j \rightleftharpoons \overline{g}_j$, $j = 1, \ldots, k$, даёт процедуру кодирования для линейного (n, k)-кода.

Выбирая в $L(\overline{g}_1, \ldots, \overline{g}_k)$ другой базис $\overline{g}'_1, \ldots, \overline{g}'_k$, мы получаем тот же код C, но с другим правилом преобразования информационных слов в кодовые.

Обозначим через G матрицу, составленную из координатных строк базисных векторов $\overline{g}_1, \ldots, \overline{g}_k$. Тогда сопоставление $\overline{a} \to \overline{c}$, задаваемое равенством

$$\overline{c} = \overline{a}G,$$

задаёт правило построения кодовых слов линейного
(n,k)-кода C. Матрица G называется **порождающей матрицей** линейного (n,k)-кода C.

Матрица G имеет ранг, равный k, а потому среди её столбцов имеется k линейно независимых.

Пусть для определённости это будут первые k столбцов. Из курса линейной алгебры следует, что элементарными преобразованиями над строками матрицу G можно привести к виду

$$G_0 = \begin{pmatrix} 1 & 0 & \cdots & 0 & \widetilde{g}_{1k+1} & \cdots & \widetilde{g}_{1,n} \\ 0 & 1 & \cdots & 0 & \widetilde{g}_{2k+1} & \cdots & \widetilde{g}_{2,n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & \widetilde{g}_{kk+1} & \cdots & \widetilde{g}_{k,n} \end{pmatrix},$$

а потому строки этой матрицы определяют координатные строки нового базиса подпространства того же самого кода C, а правило кодирования

$$\overline{a} \to \overline{c} = \overline{a}G_0$$

мы будем называть систематической (или канонической) формой кода C.

При систематическом кодировании первые k символов кодового слова $\overline{c}$, соответствующего информационному слову $\overline{a}$, совпадают с координатами вектора $\overline{a}$. Матрицу G_0 мы будем записывать в виде $G = (I_k A)$, где I_k - единичная матрица порядка k, а A - матрица размера $k \times (n-k)$, запись $(I_k A)$ означает конкатенацию матриц I_k и A.

Для линейного (n,k)-кода C с порождающей матрицей G обозначим через H матрицу, строки которой образуют базис пространства решений системы линейных однородных уравнений над полем $\mathbb{F}_q$ с матрицей G:

$$GX = 0, \;\; X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \;\; 0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Очевидно, что $GH^T = 0$, где знак "T"означает транспонирование соответ-

ствующей матрицы, 0 - есть нулевая матрица размера $k \times (n-k)$. Мы имеем: ранг$H = n-k$. Обозначим, $m = n-k$. Очевидно, что m характеризует количество избыточных (проверочных) символов кода C.

Из равенства $GH^T = 0$ следует $HG^T = 0$.

Матрицу H называют **проверочной матрицей** кода C.

Легко проверить, что, если $G = G_0 = (I_k A)$, то

$$H = \left((-A)^T I_{n-k}\right).$$

Из приведённых выше рассуждений видно, что с каждым линейным (n,k)-кодом C с порождающей матрицей G и проверочной матрицей H можно связать линейный (n,m)-код C_g с порождающей матрицей H и проверочной матрицей G. Коды C и C_g называются **двойственными** друг другу, причём любой кодовый вектор из C ортогонален (в смысле стандартного скалярного произведения) каждому вектору из C_g, и наоборот.

Пример 3. Построить линейный $(7,4)$-код C над $\mathbb{F}_2$. Выбираем матрицу размера 4×7 ранга 4:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Отображение $\overline{a} \to \overline{a}G = \overline{c}$ задаёт код

$$(0\,0\,0\,0) \longrightarrow (0\,0\,0\,0\,0\,0\,0)$$
$$(1\,0\,0\,0) \longrightarrow (1\,1\,0\,1\,0\,0\,0)$$
$$(0\,1\,0\,0) \longrightarrow (0\,1\,1\,0\,1\,0\,0)$$
$$(1\,1\,0\,0) \longrightarrow (1\,0\,1\,1\,1\,0\,0)$$
$$(0\,0\,1\,0) \longrightarrow (1\,1\,1\,0\,0\,1\,0)$$

$$(1\,0\,1\,0) \longrightarrow (0\,0\,1\,1\,0\,1\,0)$$

$$(0\,1\,1\,0) \longrightarrow (1\,0\,0\,0\,1\,1\,0)$$

$$(1\,1\,1\,0) \longrightarrow (0\,1\,0\,1\,1\,1\,0)$$

$$(0\,0\,0\,1) \longrightarrow (1\,0\,1\,0\,0\,0\,1)$$

$$(1\,0\,0\,1) \longrightarrow (0\,1\,1\,1\,0\,0\,1)$$

$$(0\,1\,0\,1) \longrightarrow (1\,1\,0\,0\,1\,0\,1)$$

$$(1\,1\,0\,1) \longrightarrow (0\,0\,0\,1\,1\,0\,1)$$

$$(0\,0\,1\,1) \longrightarrow (0\,1\,0\,0\,0\,1\,1)$$

$$(1\,0\,1\,1) \longrightarrow (1\,0\,0\,1\,0\,1\,1)$$

$$(0\,1\,1\,1) \longrightarrow (0\,0\,1\,0\,1\,1\,1)$$

$$(1\,1\,1\,1) \longrightarrow (1\,1\,1\,1\,1\,1\,1)$$

Находим проверочную матрицу H. Для этого рассмотрим систему линейных однородных уравнений с матрицей G:

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

Она имеет трапециидальный вид (см. матрицу G), поэтому x_5, x_6, x_7 её свободные неизвестные.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7
f_1	1	0	1	1	1	0	0
f_2	1	1	1	0	0	1	0
f_3	0	1	1	1	0	0	1

Следовательно,

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

Этот код не является систематическим. Однако, из матрицы G элементарными преобразованиями строк мы приходим к матрице

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}_{+C_4} \sim \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}_{+C_3} \sim$$

$$\sim \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}_{+C_2+C_4} \sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} =$$

$$= G_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 1 & 0 & A \\ 0 & 0 & 0 & 1 & \end{pmatrix}, \quad \text{где} \quad A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Поэтому

$$H_0 = \left((-A)^T I_{n-k}\right) = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Рассмотрим информационное слово $\overline{a} = (0\,1\,1\,0)$. При кодировании с помощью матрицы G имеем:

$$\overline{a} \longrightarrow \overline{c} = \overline{a}G = (0\,1\,0\,1\,1\,1\,0),$$

а при кодировании с матрицей G_0:

$$\overline{a} \longrightarrow \overline{c} = \overline{a}G_0 = (0\,1\,1\,0\,1\,0\,0).$$

Пример 4. Построить систематический $(7,3)$-код в алфавите $\mathbb{F}_3$.

Для решения задачи надо найти матрицу размера 3×7 и ранга 3 над полем $\mathbb{F}_3 = \{0,1,2\}$. Выберем два непропорциональных вектора длины 7:

$$\overline{g}_1 = (1\,0\,2\,1\,1\,0\,0), \overline{g}_2 = (2\,1\,1\,0\,2\,1\,0).$$

Ясно, что всякий вектор $\overline{g}_3$ с ненулевой последней координатой образует вместе с $\overline{g}_1$, $\overline{g}_2$ систему трёх линейно-независимых векторов.

Положим $\overline{g}_3 = (0\,1\,2\,1\,2\,0\,1)$. Тогда матрица

$$G = \begin{pmatrix} \overline{g}_1 \\ \overline{g}_2 \\ \overline{g}_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 1 \end{pmatrix}.$$

Поскольку над полем $\mathbb{F}_3$ определитель

$$\begin{vmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 0 & 1 & 2 \end{vmatrix} = 2 \neq 0,$$

то приведём матрицу G к систематической форме:

$$G = \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 0 \end{pmatrix}_{+C_1} \sim \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 & 0 & 1 \end{pmatrix}_{+2C_2} \sim \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 2 & 2 & 1 \end{pmatrix}_{+2C_3}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 2 & 2 & 1 \end{pmatrix}_{\cdot 2} = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 \end{pmatrix} = G_0 = \begin{pmatrix} I_3 & A \end{pmatrix},$$

где

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

Отсюда,

$$H_0 = \left((-A)^T I_4\right) = \begin{pmatrix} 2 & 2 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 1 & 0 & 0 \\ 2 & 2 & 2 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Теперь мы в состоянии закодировать информационное слово $\overline{a} = (2\,1\,0)$ в систематической форме кода. Имеем

$$\overline{a} \longrightarrow \overline{a}G_0 = (2\,1\,0\,0\,1\,0\,1).$$

В рассмотренных примерах мы использовали некоторые свойства конечных полей. Поэтому в следующем параграфе мы приведём некоторые полезные сведения о конечных полях.

Арифметика конечного поля

Зафиксируем натуральное число $m > 1$ и разобьём множество целых чисел на классы, относя в один и тот же класс все числа, которые при делении на m имеют один и тот же остаток. Так, для $m = 7$ числа 16 и -40 попадут в один и тот же класс: $16 = 7\cdot 2 + 2$ и $-40 = 7\cdot(-6) + 2$. Различных классов будет столько, сколько имеется различных остатков (это числа $0, 1, 2, \ldots, m-1$). Таким образом, мы имеем m классов $K_0, K_1, \ldots, K_{m-1}$ (здесь класс K_i состоит из чисел, которые при делении на m дают в остатке i, где $0 \le i \le m-1$). На множестве классов введём две алгебраические операции: сложение$(+)$ и умножение$(\cdot)$. Результаты выполнения этих операций обычно записывают с помощью таблиц сложения и умножения. Суммой двух классов $K_i + K_j$ будет класс K' , в котором содержится число $i + j$; а произведением $K_i \cdot K_j$ будет класс K'', в котором содержится число $i \cdot j$. Относительно этих операций множество клас-

сов для выбранного m (его мы обозначаем через $\mathbb{Z}_m$) образует коммутативное кольцо, которое, в случае m = p-простое число, является полем. Итак, если m есть простое число p, то $\mathbb{Z}_p$-поле. Для таких полей результаты сложения и умножения классов записывают с помощью таблиц. Ради удобства, классы K_i будем обозначать через $\overline{i}$. Так, например, поле $\mathbb{Z}_7$ состоит из элементов $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$. Соответствующие таблицы сложения и умножения имеют вид:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{6}$	$\overline{6}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$

·	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Заметим, что в таблице умножения отсутствует умножение на $\overline{0}$, так как результатом умножения на $\overline{0}$ всегда будет $\overline{0}$.

Поля типа $\mathbb{Z}_p$ называются **простыми полями** и в дальнейшем мы будем писать $\mathbb{F}_p$ вместо $\mathbb{Z}_p$. Это объясняется тем, что мы будем использовать и другие конечные поля, которые не порождаются классами вычетов K_j, рассмотренными выше.

Определение 1. Конечным полем $\mathbb{F}_q$ называется множество из q элементов, на котором определены две алгебраические операции: сложение $(+)$ и умножение $(\cdot)$, относительно которых выполняются следующие требования:

1. Сложение ассоциативно, коммутативно, и существует элемент $\overline{0} \in \mathbb{F}_q$ такой, что $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$ $\forall \overline{a} \in \mathbb{F}_q$; каждый элемент $\overline{a} \in \mathbb{F}_q$ обратим по сложению (т.е. для $\overline{a} \in \mathbb{F}_q$ найдётся элемент $\overline{b} \in \mathbb{F}_q$ так, что $\overline{a}+\overline{b} = \overline{b}+\overline{a} = \overline{0}$).

2. Умножение ассоциативно, коммутативно и существует элемент $\overline{1} \in \mathbb{F}_q$ такой, что $\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}$; каждый элемент $\overline{a} \in \mathbb{F}_q$, $\overline{a} \neq 0$, обратим по умножению (т.е., $\exists \overline{b} \in \mathbb{F}_q \Rightarrow \overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1}$).

3. Умножение дистрибутивно относительно слодения, т.е. $(\overline{a}+\overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$ для любых $\overline{a}, \overline{b}, \overline{c} \in \mathbb{F}_q$.

В дальнейшем мы часто будем использовать обозначение $k \cdot \overline{a}$ для суммы $\underbrace{\overline{a} + \overline{a} + \cdots + \overline{a}}_{k\text{-раз}}$, $\overline{a} \in \mathbb{F}_q$, и обозначение $\overline{a}^k = \underbrace{\overline{a} \cdot \overline{a} \cdots \overline{a}}_{k\text{-раз}}$, где k натуральное число. Кроме того, условимся, что $0 \cdot \overline{a} = \overline{0}$ и $\overline{a}^0 = \overline{1}$.

Определение 2. Характеристикой конечного поля $\mathbb{F}_q$ называется наименьшее натуральное число ℓ такое, что $\ell \overline{a} = \overline{0}$ для каждого $\overline{a} \in \mathbb{F}_q$.

Следующие факты мы примем к сведению (их доказательства можно найти в любой книге, посвящённой конечным полям. Например, Лидл, Нидерайтер...).

Лемма 1. *Характеристика конечного поля $\mathbb{F}_q$ есть простое число.*

Лемма 2. *Пусть $\mathbb{F}_q$-конечное поле характеристики p. Тогда $q = p^m$ для некоторого натурального m.*

Лемма 3. *Совокупность ненулевых элементов конечного поля $\mathbb{F}_q$ образует группу по умножению, число элементов этой группы равно $q-1$ и эта группа циклическая (т.е. существует элемент $\overline{h} \in \mathbb{F}_q$, $\overline{h} \neq \overline{0}$ такой, что для любого $\overline{a} \in \mathbb{F}_q$, $\overline{a} \neq \overline{0}$ имеем $\overline{a} = \overline{h}^k$ с некоторым целым k, $0 \leq k < q-1$).*

Элемент $\overline{h}$ называется порождающим элементом мультипликативной группы поля (её мы обозначаем $\mathbb{F}_q^*$, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{\overline{0}\}$).

Пусть $\overline{a} \in \mathbb{F}_q^*$. Наименьшее натуральное значение ℓ, для которого $\overline{a}^\ell = \overline{1}$, называется порядком элемента $\overline{a}$ в группе $\mathbb{F}_q^*$. Ясно, что порядок порождающего элемента группы $\mathbb{F}_q^*$ равен $q-1$. В дальнейшем, порождающий элемент группы $\mathbb{F}_q^*$ мы также будем называть первообразным корнем по модулю p, если $q = p$, а в случае $q = p^m$, $m > 1$, порождающий элемент $\mathbb{F}_q^*$ будем называть примитивной величиной поля $\mathbb{F}_q$.

Лемма 4. *Пусть $\overline{h}$-порождающий элемент мультипликативной группы $\mathbb{F}_q^*$. Тогда $\overline{a} = \overline{h}^k$ будет порождающим элементом в $\mathbb{F}_q^*$ тогда и только тогда, когда $(k, q-1) = 1$. Более того, $\overline{a} = \overline{h}^k$ имеет порядок, равный $\frac{q}{НОД(k,q-1)}$.*

Доказательство. Пусть НОД$(k, q-1) = d$. Тогда $k = dk_1$, $(q-1) = dr$, НОД$(k_1, r) = 1$. И мы имеем

$$\overline{a}^{\frac{q-1}{\text{НОД}(k,q-1)}} = (\overline{h}^{dk_1})^{\frac{q-1}{\text{НОД}(k,q-1)}} = (\overline{h}^{k_1})^{q-1} = 1.$$

Далее, пусть $0 < \ell < \frac{q-1}{\text{НОД}(k,q-1)}$. Тогда $\overline{a}^\ell = (\overline{h}^{\ell k})$, число ℓk не делится на $(q-1)$, а потому $\ell k = (q-1)t + r$, $0 < r < q-1$. Значит, из $\overline{a}^\ell \equiv 1$ следует, что $\overline{h}^r = 1$, что невозможно. □

Следствие 1. *Каждое $\overline{a} \in \mathbb{F}_q^*$ имеет порядок, делящий $(q-1)$.*

Из определения порядка элемента в группе $\mathbb{F}_q^*$ следует, что для каждого $\overline{a} \in \mathbb{F}_q^*$ обратным к $\overline{a}$ будет $\overline{a}^{\ell-1}$, где ℓ-порядок элемента $\overline{a}$.В частности, если $\overline{a} = \overline{h}^r$, то $\overline{a}^{-1} = \overline{h}^{(q-1-r)}$. Это показывает, что деление в конечном поле проще, чем в поле рациональных чисел. Пока мы пользовались только простыми полями $\mathbb{F}_p$, где p-простое число. Для построения поля $\mathbb{F}_q$, $q = p^m$, $m > 1$, нам понадобятся специальные многочлены с коэффициентами из поля $\mathbb{F}_p$.

Напомним, что степенью ненулевого многочлена $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ называется наибольшее значение $k \in \{0, 1, \ldots, n\}$, для которого $a_k \neq 0$.

Определение 3. Многочлен $f(x)$ из кольца многочленов $\mathbb{F}_p[x]$ называется неприводимым над $\mathbb{F}_p$, если степень $f(x) \geq 1$ и его нельзя представить в виде произведения многочленов меньших степеней.

Известно, что для каждого $n = 1, 2, \ldots$, существуют многочлены степени n, неприводимые над $\mathbb{F}_p$ (доказательство см. в [?]). Поскольку для нас особый интерес представляют неприводимые многочлены над $\mathbb{F}_2$, то постоим такие многочлены.

Имеется два многочлена $I^{\underline{\text{ой}}}$ степени над $\mathbb{F}_2$:

$$x \text{ и } x+1,$$

и оба они неприводимы над $\mathbb{F}_2$. Можно указать все 4 многочлена второй степени над $\mathbb{F}_2$:

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

но только x^2+x+1 неприводим над $\mathbb{F}_2$, так как остальные многочлены имеют корни $\overline{0}$ или $\overline{1}$ в $\mathbb{F}_2$, а потому делятся на линейные многочлены x или $x+1$. Аналогично можно убедиться, что x^3+x+1 и x^4+x+1 являются неприводимыми многочленами над $\mathbb{F}_2$, соответственно степеней 3 и 4. В различных книгах даны полные списки неприводимых над $\mathbb{F}_2$ многочленов соответственно степеней $1, 1, 3, \ldots, N$. Мы приведём некоторые такие многочлены, которые содержат наименьшее возможное число ненулевых слагаемых:

$$x^5+x^2+1,\ x^6+x+1,\ x^7+x^3+1,\ x^8+x^4+x^3+x^2+1,$$

$$x^9+x^4+1,\ x^{10}+x^3+1,\ x^{11}+x^2+1,\ x^{12}+x^6+x^4+x+1.$$

Обращаем внимание на то, что неприводимые над $\mathbb{F}_2$ многочлены содержат обязательно нечетное число слагаемых. Заметим также, что неприводимых многочленов над $\mathbb{F}_2$ одной и той же степени n достаточно много. Имеется формула для подсчёта количества неприводимых многочленов степени n над произвольным конечным полем $\mathbb{F}_p$. Но мы её не приводим, так как она нам не понадобится. И ещё: всё сказанное о неприводимых многочленах над $\mathbb{F}_p$

остаётся справедливым и для многочленов над произвольным конечным полем $\mathbb{F}_q$.

Как же построить поле из $q = p^m$ элементов, если $m > 1$? Воспользуемся следующей процедурой.

Пусть $P(x)$-неприводимый над $\mathbb{F}_p$ многочлен степени m. Все многочлены из кольца многочленов $\mathbb{F}_p[x]$ разобьём на классы, относя к одному и тому же классу все многочлены, имеющие одинаковые остатки от деления на $P(x)$. Так возникает конечное число классов, характеризующихся одним и тем же остатком $r(x)$, где ст$r(x) <$ ст$P(x)$, если $r(x) = 0$. Пусть степень $P(x) = m$. Тогда каждый многочлен $r(x) \neq 0$ можно записать в виде

$$r(x) = r_0 + z_1 x + \cdots + r_{m-1}x^{m-1},\ r_i \in \mathbb{F}_p,\ i = 0, 1, \ldots, m-1.$$

Всех таких многочленов вместе с нулевым многочленом будет ровно p^m. Отсюда заключаем, что всего имеется точно p^m классов $K_{r(x)}$.

Вводим операции сложения и умножения классов:

$$K_{r_1(x)} + K_{r_2(x)} = K_{r(x)},$$

где $r(x) = r_1(x) + r_2(x)$,

$$K_{r_1(x)} \cdot K_{r_2(x)} = K_{\widetilde{r}(x)},$$

где $r(x)$-остаток от деления $r_1(x) \cdot r_2(x)$ на $P(x)$.

Проиллюстрируем это на примере поля $\mathbb{F}_2$ с неприводимым многочленом $P(x) = x^3 + x + 1$.

Пусть

$$r_1(x) = x^2 + x,\ \ r_2(x) = x + 1.$$

Имеем,

$$K_{r_1(x)} + K_{r_2(x)} = K_{x^2+1},$$

ибо $x^2 + x + x + 1 = x^2 + 1$.

Далее,

$$K_{r_1(x)} \cdot K_{r_2(x)} = K_1,$$

ибо

$$(x^2+x)\cdot(x+1) = x^3+x = x^3+x+1+1 = P(x)+1,$$

$\Rightarrow$ остаток от деления x^3+x на $P(x)$ равен 1.

Покажем, что множество классов образует поле из 2^3 элементов. Действительно, всего имеется 2^3 многочленов степени < 3 (вместе с нулевым). Необходимо только проверить, что каждый ненулевой класс (как элемент поля, которое мы строим) обратим. Пусть $r(x) \neq 0$, степень $r(x) < 3$. Многочлены $r(x)$ и $P(x)$ взаимно просты, так как $P(x)$ делится только на себя и 1, а потому НОД$(r(x), P(x)) = 1$. Используя линейное представление НОД двух многочленов, получаем

$$r(x)u(x) + P(x)v(x) = 1,$$

где $u(x)$-многочлен степени < 3.

Отсюда следует, что $K_{z(x)} \cdot K_{u(x)} = K_1$, т.е. $K_{u(x)}$ является обратным к $K_{z(x)}$.

Итак, мы построили поле поле $\mathbb{F}_{2^3}$.

Обозначим класс K_x через α. Тогда класс $K_{r(x)}$, где $r(x) = a_0 + a_1x + a_2x^2$, $a_i \in \mathbb{F}_2$, можно записать как

$$a_0K_x^0 + a_1K_x + a_2K_x^2 = a_0 + a_1\alpha + a_2\alpha^2.$$

Заметим ещё, что

$$K_0 = K_{P(x)} = K_{x^3+x+1} = K_{x^3} + K_x + K_1 =$$

$$= (K_x)^3 + K_x + 1 = \alpha^3 + \alpha + 1,$$

а потому $\alpha^3 = \alpha + 1$.

Пользуясь последним равенством, вычислим все степени α^i, $i = 0, 1, \ldots, 7, \ldots$. Имеем

$$\alpha^0 = 1,\ \alpha^1 = \alpha,\ \alpha^2 = \alpha^2,\ \alpha^3 = \alpha + 1,\ \alpha^4 = \alpha^2 + \alpha,$$

$$\alpha^5 = \alpha^3 + \alpha^3 = \alpha^2 + \alpha + 1,\ \alpha^6 = \alpha = \alpha^3 + \alpha^2 + \alpha = \alpha^+1,$$

$$\alpha^7 = \alpha^3 + \alpha = 1,\ \alpha^8 = \alpha,\ \alpha^9 = \alpha^2, \ldots.$$

Поэтому последовательные степени α от 0 до 6 порождают все ненулевые элементы построенного поля $\mathbb{F}_{2^3} = \mathbb{F}_8$.

Построение поля $\mathbb{F}_{p^m}$ для произвольного простого p и натурального $m > 1$ проходит аналогично.

Процедура построения поля $\mathbb{F}^{p^m}$ показывает, что
$\mathbb{F}_{p^m} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}$ и в то же время $\mathbb{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} | \ a_i \in \mathbb{F}_p\}$, ибо каждая степень α однозначно представляется в виде многочлена от α степени $\leq m-1$ с коэффициентами из $\mathbb{F}_p$, и наоборот. Степенное представление ненулевых элементов поля $\mathbb{F}_{p^m}$ удобно для выполнения операции умножения (например, в поле $\mathbb{F}_{2^3}$ имеем $\alpha^5 \cdot \alpha^4 = \alpha^9 = \alpha^7 \cdot \alpha = \alpha^{2^3-1} \cdot \alpha = \alpha$), а представление многочленами степени $\leq m-1$ удобно при выполнении операции сложения в $\mathbb{F}_{p^m}$ (например, $\alpha^5 + \alpha^4 = (\alpha^2 + \alpha + 1) + (\alpha^2 + \alpha) = 1$).

Пример 5. Рассмотрим поле $\mathbb{F}_{3^2} = \mathbb{F}_9$. Для построения поля из 9 элементов найдём неприводимый многочлен второй степени над $\mathbb{F}_3$. Непосредственной проверкой убеждаемся, что многочлен $P(x) = x^2 + 1$ неприводим над $\mathbb{F}_3$. Как и выше убеждаемся, что класс $K_x = \alpha$ порождает поле из 9 элементов:

$$0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2,$$

причём

$$\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = 2, \alpha^3 = 2\alpha, \alpha^4 = 2\alpha^2 = 1,$$

и значит α не является примитивным элементом поля $\mathbb{F}_{3^2}$. Но для элемента $\beta = \alpha + 1 \in \mathbb{F}_{3^2}$ имеем

$$\beta^0 = 1, \ \ \beta^1 = \beta, \ \ \beta^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = 2\beta + 1,$$

$$\beta^3 = 2\beta^2 + \beta = 2\beta + 2, \ \ \beta^4 = 2\beta^2 + 2\beta = 2, \ \ \beta^5 = 2\beta,$$

$$\beta^6 = \beta + 2, \ \ \beta^7 = \beta + 1, \ \ \beta^8 = 1,$$

и значит, $\beta = \alpha + 1$ имеет порядок $3^2 - 1 = 8$, а потому является примитивным элементом поля $\mathbb{F}_{3^2}$.

Этот пример показывает, что не всякий неприводимый многочлен $P(x)$ на $\mathbb{F}_p$ имеет своим корнем примитивный элемент поля $\mathbb{F}_{p^m}$, хотя $P(x)$порождает

поле $\mathbb{F}_{p^m}$. Интересующий нас неприводимый многочлен $Q(x)$ степени 2, корнем которого является β, порождающий поле $\mathbb{F}_{3^2}$ (так, что β становится примитивным элементом поля $\mathbb{F}_{3^2}$) будет построен позже.

Пример 6. Построим поле $\mathbb{F}_{2^4}$. Мы имеем три неприводимых многочлена четвёртой степени над $\mathbb{F}_2$:

$$P_1(x) = x^4 + x + 1,\ P_2(x) = x^4 + x^3 + 1,\ P_3(x) = x^4 + x^3 + x^2 + x + 1.$$

По аналогии с построением поля $\mathbb{F}_{2^3}$ обозначим через α, β, γ корни многочленов $P_i(x)$, $i = 1, 2, 3$, соответственно.

Используя равенства

$$\alpha^4 = \alpha + 1,\ \beta^4 = \alpha^3 + 1,\ \gamma^4 = \gamma^3 + \gamma^2 + \gamma + 1,$$

мы получим следующие таблицы степеней α^j, β^j, γ^j

Таблица 1: Представление степеней α через базис 1, α, α^2, α^3

Степень α^j	Представление α^j полиномом $r(\alpha)$	Степень α^j	Представление α^j полиномом $r(\alpha)$
1	$1\cdot1+0\cdot\alpha+0\cdot\alpha^2+0\cdot\alpha^3$	α^8	$1\cdot1+0\cdot\alpha+1\cdot\alpha^2+0\cdot\alpha^3$
α	$0\cdot1+1\cdot\alpha+0\cdot\alpha^2+0\cdot\alpha^3$	α^9	$0\cdot1+1\cdot\alpha+0\cdot\alpha^2+1\cdot\alpha^3$
α^2	$0\cdot1+0\cdot\alpha+1\cdot\alpha^2+0\cdot\alpha^3$	α^{10}	$1\cdot1+1\cdot\alpha+1\cdot\alpha^2+0\cdot\alpha^3$
α^3	$0\cdot1+0\cdot\alpha+0\cdot\alpha^2+1\cdot\alpha^3$	α^{11}	$0\cdot1+1\cdot\alpha+1\cdot\alpha^2+1\cdot\alpha^3$
α^4	$1\cdot1+1\cdot\alpha+0\cdot\alpha^2+0\cdot\alpha^3$	α^{12}	$1\cdot1+1\cdot\alpha+1\cdot\alpha^2+1\cdot\alpha^3$
α^5	$0\cdot1+1\cdot\alpha+1\cdot\alpha^2+0\cdot\alpha^3$	α^{13}	$1\cdot1+0\cdot\alpha+1\cdot\alpha^2+1\cdot\alpha^3$
α^6	$0\cdot1+0\cdot\alpha+1\cdot\alpha^2+1\cdot\alpha^3$	α^{14}	$1\cdot1+0\cdot\alpha+0\cdot\alpha^2+1\cdot\alpha^3$
α^7	$1\cdot1+1\cdot\alpha+0\cdot\alpha^2+1\cdot\alpha^3$	α^{15}	$1\cdot1+0\cdot\alpha+0\cdot\alpha^2+0\cdot\alpha^3$

Таблица 2: Представление степеней β через базис 1, β, β^2, β^3

Степень β^j	Представление β^j полиномом $r(\beta)$	Степень β^j	Представление β^j полиномом $r(\beta)$
1	$1{\cdot}1+0{\cdot}\beta+0{\cdot}\beta^2+0{\cdot}\beta^3$	β^8	$0{\cdot}1+1{\cdot}\beta+1{\cdot}\beta^2+1{\cdot}\beta^3$
β	$0{\cdot}1+1{\cdot}\beta+0{\cdot}\beta^2+0{\cdot}\beta^3$	β^9	$1{\cdot}1+0{\cdot}\beta+1{\cdot}\beta^2+0{\cdot}\beta^3$
β^2	$0{\cdot}1+0{\cdot}\beta+1{\cdot}\beta^2+0{\cdot}\beta^3$	β^{10}	$0{\cdot}1+1{\cdot}\beta+0{\cdot}\beta^2+1{\cdot}\beta^3$
β^3	$0{\cdot}1+0{\cdot}\beta+0{\cdot}\beta^2+1{\cdot}\beta^3$	β^{11}	$1{\cdot}1+0{\cdot}\beta+1{\cdot}\beta^2+1{\cdot}\beta^3$
β^4	$1{\cdot}1+0{\cdot}\beta+0{\cdot}\beta^2+1{\cdot}\beta^3$	β^{12}	$1{\cdot}1+1{\cdot}\beta+0{\cdot}\beta^2+0{\cdot}\beta^3$
β^5	$1{\cdot}1+1{\cdot}\beta+0{\cdot}\beta^2+1{\cdot}\beta^3$	β^{13}	$0{\cdot}1+1{\cdot}\beta+1{\cdot}\beta^2+0{\cdot}\beta^3$
β^6	$1{\cdot}1+1{\cdot}\beta+1{\cdot}\beta^2+1{\cdot}\beta^3$	β^{14}	$0{\cdot}1+0{\cdot}\beta+1{\cdot}\beta^2+1{\cdot}\beta^3$
β^7	$1{\cdot}1+1{\cdot}\beta+1{\cdot}\beta^2+0{\cdot}\beta^3$	β^{15}	1

Таблица 3: Представление степеней γ через базис 1, γ, γ^2, γ^3

Степень γ^j	Представление γ^j полиномом $r(\gamma)$	Степень γ^j	Представление γ^j полиномом $r(\gamma)$
1	$1{\cdot}1+0{\cdot}\gamma+0{\cdot}\gamma^2+0{\cdot}\gamma^3$	γ^8	$1{\cdot}1+0{\cdot}\gamma+1{\cdot}\gamma^2+0{\cdot}\gamma^3$
γ	$0{\cdot}1+1{\cdot}\gamma+0{\cdot}\gamma^2+0{\cdot}\gamma^3$	γ^9	$0{\cdot}1+1{\cdot}\gamma+0{\cdot}\gamma^2+1{\cdot}\gamma^3$
γ^2	$0{\cdot}1+0{\cdot}\gamma+1{\cdot}\gamma^2+0{\cdot}\gamma^3$	γ^{10}	$1{\cdot}1+1{\cdot}\gamma+1{\cdot}\gamma^2+0{\cdot}\gamma^3$
γ^3	$0{\cdot}1+0{\cdot}\gamma+0{\cdot}\gamma^2+1{\cdot}\gamma^3$	γ^{11}	$0{\cdot}1+1{\cdot}\gamma+1{\cdot}\gamma^2+1{\cdot}\gamma^3$
γ^4	$1{\cdot}1+1{\cdot}\gamma+0{\cdot}\gamma^2+0{\cdot}\gamma^3$	γ^{12}	$1{\cdot}1+1{\cdot}\gamma+1{\cdot}\gamma^2+1{\cdot}\gamma^3$
γ^5	$0{\cdot}1+1{\cdot}\gamma+1{\cdot}\gamma^2+0{\cdot}\gamma^3$	γ^{13}	$1{\cdot}1+0{\cdot}\gamma+1{\cdot}\gamma^2+1{\cdot}\gamma^3$
γ^6	$0{\cdot}1+0{\cdot}\gamma+1{\cdot}\gamma^2+1{\cdot}\gamma^3$	γ^{14}	$1{\cdot}1+0{\cdot}\gamma+0{\cdot}\gamma^2+1{\cdot}\gamma^3$
γ^7	$1{\cdot}1+1{\cdot}\gamma+0{\cdot}\gamma^2+1{\cdot}\gamma^3$	γ^{15}	$1{\cdot}1+0{\cdot}\gamma+0{\cdot}\gamma^2+0{\cdot}\gamma^3$

Из таблиц 1 и 2 следует, что α и β являются примитивными элементами поля $\mathbb{F}_{2^4}$, а таблица 3 показывает, что γ в группе $\mathbb{F}^*_{2^4}$ имеет порядок 5, а потому не является примитивным элементом поля $\mathbb{F}_{2^3}$, хотя элементы 1, γ,

γ^2, γ^3 порождают поле $\mathbb{F}_{2^3}$, т.е. $\mathbb{F}_{2^3} = \{a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 \,:\, a_i \in \mathbb{F}_2\}$.

Определение 4. Пусть $\beta \in \mathbb{F}_{p^m}$. Минимальным многочленом для β над $\mathbb{F}_p$ называется ненулевой многочлен $\psi(x)$ над $\mathbb{F}_p$ наименьшей степени, корнем которого является β (т.е. $\psi(\beta) = 0$).

Ясно, что минимальный многочлен любого элемента поля $\mathbb{F}_{p^m}$ является неприводимым над $\mathbb{F}_p$. Кроме того,каждый ненулевой многочлен из $\mathbb{F}_p[x]$, корнем которого является β, делится на минимальный многочлен для β. Действительно, пусть $\psi(x)$-минимальный многочлен для β, и пусть $F(x) \neq 0$, но $F(\beta) = 0$. Тогда из теоремы о делении с остатком имеем

$$F(x) = \psi(x)g(x) + r(x),\ \text{ст}r(x) < \text{ст}\psi(x),$$

И, так как

$$0 = F(\beta) = \psi(\beta)g(\beta) + r(\beta),$$

то заключаем, что $r(\beta) = 0$, что возможно только в случае $r(x)$-нулевой многочлен.

Значит, $F(x)$ делится на $\psi(x)$.

Изучим ещё некоторые основные свойства поля $\mathbb{F}_{p^m}$. Мы видели, что поле $\mathbb{F}_{p^m}$ может быть получено из простого поля $\mathbb{F}_p$ (иногда мы будем называть $\mathbb{F}_p$ основным полем характеристики p), присоединением к $\mathbb{F}_p$ корня неприводимого над $\mathbb{F}_p$ многочлена $P(x)$ степени m, т.е. $\mathbb{F}_{p^m} = \mathbb{F}_p(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \,|\, a_i \in \mathbb{F}_p,\ P(\alpha) = 0\}$. Отсюда видно, что конструкция поля $\mathbb{F}_p(\alpha)$ напоминает конструкцию поля комплексных чисел $\mathbb{C} = \mathbb{R}(i) = \{a + bi \,|\, a, b \in \mathbb{R},\ i^2 + 1 = 0\}$.

Поле $\mathbb{F}_{p^m}$ называется расширением поля $\mathbb{F}_p$, а многочлен $P(x)$ имеет, вообще говоря, m различных корней, каждый из которых порождает поле $\mathbb{F}_{p^m}$. Эти поля $\mathbb{F}_{p^m}$ идентичны, как это видно из построения поля $\mathbb{F}_{p^m}$ с помощью

классов $K_{r(x)}$ (ибо остатки $r(x)$ не зависят от корня α). Возникает вопрос: как связаны между собой различные корни многочлена $P(x)$? Из элементарной теории чисел известно, что каждое $a \in \mathbb{F}_p$ удовлетворяет уравнению $x^p - x = 0$ над полем $\mathbb{F}_p$, т.е. мы имеем все p различных корней многочлена $x^p - x$, и других корней нет ни в каком алгебраическом расширении поля $\mathbb{F}_p$. А потому справедлива

Лемма 5. *Элемент $\alpha \in \mathbb{F}_{p^m}$ удовлетворяет равенству $\alpha^p = \alpha$ тогда и только тогда, когда $\alpha \in \mathbb{F}_p$.*

Лемма 6. *Пусть $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_{p^m}$. Тогда*

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_k)^p = \alpha_1^p + \alpha_2^p + \cdots + \alpha_k^p.$$

(Это следует из того, что при формальном возведении суммы $\alpha_1 + \cdots + \alpha_p$ в степень p все остальные слагаемые имеют коэффициенты, кратные p, а поле $\mathbb{F}_{p^m}$ имеет характеристику p).

Лемма 7. *Пусть $f(x) \in \mathbb{F}_p[x]$ и пусть $\alpha \in \mathbb{F}_{p^m}$. Тогда, если α корень $f(x)$, то и α^{p^ℓ}, $\ell = 0, 1, 2, \ldots$, также корень $f(x)$.*

Доказательство. Пусть $f(x) = a_0 + a_1 x + \cdots + a_k x^k$. Тогда $a_0 + a_1 x + \cdots + a_k x^k = 0$. Возводя в степень p полученное равенство и применяя леммы 5 и 6, находим

$$\begin{aligned} 0 &= (a_0 + a_1\alpha + \cdots + a_k\alpha^k)^p = \\ &= a_0^p + (a_1\alpha)^p + \cdots + (a_k\alpha^k)^p = \\ &= a_0 + a_1\alpha^p + \cdots + a_k(\alpha^p)^k, \end{aligned}$$

т.е. α^p-также корень $f(x)$.

Теперь по индукции сразу следует утверждение леммы. □

Лемма 8. *Пусть $f(x) \in \mathbb{F}_p[x]$-неприводимый многочлен степени k и пусть $\alpha \in \mathbb{F}_{p^m}$-корень $f(x)$. Тогда $\alpha, \alpha^p, \ldots, \alpha^{p^{k-1}}$ суть все различные корни $f(x)$.*

Доказательство. То, что α^{p^j}, $j = 0, 1, \ldots, k-1$-корни $f(x)$ следует из леммы 7. Все эти корни различные (ибо неприводимый многочлен не имеет кратных корней). □

Следствие 2. *Пусть $\beta \in \mathbb{F}_{p^m}$, $\beta \neq 0$. Тогда неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$, корнем которого является β, имеет степень $\leq m$ И $f(x)$ делит $x^{p^m-1} - 1$.*

Действительно, поскольку $\beta \in \mathbb{F}_{p^m}$, $\beta \neq 0$, то порядок β является делителем порядка мультипликативной группы $\mathbb{F}^*_{p^m}$, т.е. порядок β делит $p^m - 1$, а потому $\beta^{p^m-1} = 1$. Значит, β является корнем $x^{p^m-1} - 1$. Но тогда $f(x)$ делит $x^{p^m-1} - 1$. Далее, все корни $f(x)$ образуют множество $\{\beta, \beta^p, \ldots, \beta^{p^{\ell-1}}\}$, $\ell \leq m$. Значит, степень $f(x)$ равна ℓ.

Определение 5. Неприводимый над $\mathbb{F}_p$ многочлен, корнем которого является $\beta \in \mathbb{F}_{p^m}$ (для некоторого $m \geq 1$), будем называть **минимальным многочленом для β**. Часто минимальный многочлен для β мы будем обозначать $f_\beta(x)$.

Следствие 3. *Пусть $\beta \in \mathbb{F}_{p^m}$, $\beta \neq 0$. Тогда минимальный многочлен для β над $\mathbb{F}_p$ равен*

$$f(x)(x - \beta)(x - \beta^p)\cdots(x - \beta^{p^{k-1}}),$$

где k-наименьшее натуральное, для которого $\beta^{p^k} = \beta$.

Пример 7. Рассмотрим поле $\mathbb{F}_{2^4}$, порождённое корнем δ многочлена $p(x) = x^4 + x^3 + 1 \in \mathbb{F}_2[x]$. Пусть $\beta = \alpha^{11}$. Построим минимальный многочлен для β над $\mathbb{F}_p$. Имеем

$$\beta = \alpha^1 1,\ \beta^2 = \alpha^{22} = \alpha^7,\ \beta^4 = \alpha^{14},\ \beta^8 = \alpha^{13},\ \beta^{16} = \beta = \alpha^{11}.$$

Значит, α^{11}, α^7, α^{13}, α^{14} - суть все различные корни $f(x)$, а потому

$$f(x) = (x + \alpha^{11})(x + \alpha^7)(x + \alpha^{13})(x + \alpha^{14}).$$

Теперь, раскрывая скобки и используя таблицу 2 (см. выше), получим

$$f(x) = x^4 + x^3 + 1.$$

Определение 6. Пусть $\beta \in \mathbb{F}_{p^m}$, $\beta = neq0$, и пусть степень минимального многочлена $f_\beta(x) \in \mathbb{F}_p[x]$ равна k. Тогда $\{\beta, \beta^p, \ldots, \beta^{p^{k-1}}\}$ называется множеством сопряжённых с β элементов, т.е. каждое β^{p^ℓ}, $0 \le \ell \le k-1$, называется сопряжённым с β.

Пример 8. Пусть α-порождающий элемент поля $\mathbb{F}_{2^4}$, и пусть x^4+x+1-его минимальный над $\mathbb{F}_2$ многочлен. Чтобы построить минимальный многочлен для $\beta = \alpha^9$, рассмотрим 2^j, $j = 0, 1, \ldots$ степеней β:

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

и определим наименьшее $j \ge 1$, для которого $\beta^{2^j} = \beta$. Используя таблицу 1, находим

$$\beta = \alpha^9,\ \beta^2 = \alpha^{18} = \alpha^3,\ \beta^4 = \alpha^6,\ \beta^8 = \alpha^{12},$$

$$\beta^{16} = \alpha^{24} = \alpha^9 = \beta.$$

Значит, $j = 4$, и поэтому

$$\begin{aligned}
f_\beta(x) &= (x+\alpha^9)(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12}) = \\
&= (x^2 + (\alpha^9+\alpha^3)x + \alpha^{12})\times \\
&\quad \times (x^2 + (\alpha^6+\alpha^{12})x + \alpha^{18}) = \\
&= x^4 + (\alpha^3+\alpha^9+\alpha^6+\alpha^{12})x^3 + \\
&\quad + (\alpha^{18}+\alpha^{12}+\alpha^{15}+\alpha^9+\alpha^{21}+\alpha^{15})x^2 + \\
&\quad + (\alpha^{27}+\alpha^{21}+\alpha^{18}+\alpha^{24})x + \alpha^{30} = \\
&= x^4 + x^3 + x^2 + x + 1.
\end{aligned}$$

Имеется и другой метод нахождения коэффициентов минимального многочлена. Пусть $\gamma \in \mathbb{F}_{p^m}$ и пусть γ, γ^p, γ^{p^2},...,$\gamma^{p^{k-1}}$- все сопряжённые над $\mathbb{F}_p$

элементы. Обозначим $f_\gamma(x) = a_0 + a_1 x + \cdots + a_k x^k$. Отсюда

$$a_0 + a_1\gamma + \cdots + a_k\gamma^k = 0.$$

Пользуясь представлением γ через полином от примитивного элемента α поля $\mathbb{F}_{p^m}$, получаем

$$a_0 + a_1 \underbrace{(b_{10} + b_{11}\alpha + \cdots + b_{1m\text{-}1}\alpha^{m\text{-}1})}_{\gamma} +$$

$$+ a_2 \underbrace{(b_{20} + b_{21}\alpha + \cdots + b_{2m\text{-}1}\alpha^{m\text{-}1})}_{\gamma^2} + \cdots = 0.$$

Теперь левая часть последнего равенства есть многочлен $F(\alpha)$ относительно α, причём степень этого многочлена $\leq m-1$. Учитывая, что степень минимального многочлена для α равна m, заключаем, что все коэффициенты $F(\alpha)$ должны быть равны нулю, а потому мы получаем систему линейных однородных уравнений относительно неизвестных коэффициентов a_j, которая легко решается над конечным полем $\mathbb{F}_p$.

Пример 9. Построим минимальный многочлен для $\beta = \alpha^9$, где α-примитивный элемент поля $\mathbb{F}_{2^4}$ и $f_\alpha(x) = x^4 + x + 1$.

Мы уже определили, что $f_\beta(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$. Поэтому, используя таблицу 1, находим

$$\beta = \alpha^9 = \alpha + \alpha^3, \quad \beta^2 = \alpha^3, \quad \beta^3 = \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3, \quad \beta^4 = \alpha^6 = \alpha^2 + \alpha^3.$$

Следовательно,

$$0 = f_\beta(\beta) = a_0 + a_1(\alpha + \alpha^3) + a_2\alpha^3 + a_3(1 + \alpha + \alpha^2 + \alpha^3) + a_4(\alpha^2 + \alpha^3) =$$

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

Поэтому имеем следующую систему

$$a_0 + a_3 = 0$$

$$a_1 + a_3 = 0$$

$$a_3 + a_4 = 0$$

$$a_1 + a_2 + a_3 + a_4 = 0$$

Откуда следует $a_0 = a_1 = a_2 = a_3 = a_4 = 1$, так как $f_\beta(x) \neq 0$. Поэтому

$$f_\beta(x) = x^4 + x^3 + x^2 + x + 1.$$

Из метода построения поля $\mathbb{F}_{p^m}$ следует, что, если α-примитивный элемент этого поля, то и все сопряжённые с ним являются примитивными элементами.

Лемма 9. *Если $\beta \in \mathbb{F}_{p^m}^*$ и имеет порядок n, то и все сопряжённые с β имею тот же порядок n.*
Доказательство. Прежде всего заметим, что $n | p^m - 1$. Далее, если $\beta^n = 1$, то $(\beta^n)^{p^j} = 1$, $j = 0, 1, \ldots$, так что порядок β^{p^j} делит число n. Но порядок β^{p^j} равен $\frac{n}{\text{НОД}(p^j, n)}$, и так как $(p^j, p^m - 1) = 1$, заключаем, что $\frac{n}{\text{НОД}(p^j, n)} = n$. □

Лемма 10. *Минимальный многочлен любого элемента $\beta \in \mathbb{F}_{p^m}$ делит многочлен $x^{p^m-1} - 1$.*
Доказательство. Это следует из того, что порядок β делит $p^m - 1$, т.е. $\beta^{p^m-1} - 1 = 0$, а значит, $f_\beta(x)$ и $x^{p^m-1} - 1$ имеют общий корень и, в силу неприводимости $f_\beta(x)$, следует, что $f_\beta(x)$ делит $x^{p^m-1} - 1$. □

Лемма 11. *Пусть $\beta \in \mathbb{F}_{p^m}$ и $f_\beta(x)$-минимальный многочлен для β степени k. Тогда k делит m.*

Доказательство. Действительно, мы имеем

$$\beta,\ \beta^p, \ldots, \beta^{p^{k-1}},\ \beta^{p^k} = \beta, \ldots, \beta^{2k} = \beta, \ldots, \beta^{p^m} = \beta. \qquad (*)$$

(ибо $\beta^{p^m-1} = 1$, $\beta^{p^m} = \beta$).

Следовательно, в ряде $(*)$ без последнего элемента укладывается целое число раз совокупность

$$\{\beta, \beta^p, \ldots, \beta^{p^{k-1}}\},$$

откуда и заключаем, что m кратно k. □

В заключение этого параграфа рассмотрим примеры решения систем линейный уравнений над $\mathbb{F}_p$ и примеры нахождения корней многочленов над $\mathbb{F}_{p^m}$ в поле $\mathbb{F}_{p^m}$.

Пример 10. Над полем $\mathbb{F}_2$ решить систему

$$\begin{cases} x_1 + x_2 + x_4 + x_5 &= 1, \\ x_1 + x_3 + x_5 &= 0, \\ x_2 + x_3 + x_4 + x_5 &= 1, \\ x_1 + x_2 &= 0, \\ x_2 + x_3 + x_4 &= 1. \end{cases}$$

Такие системы удобно решать методом Гаусса, приводя систему к трапециидальному виду. Процедуру приведения проводим в матричном виде

$$G = \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \begin{matrix} \\ +C_1 \\ \\ +C_1 \\ \end{matrix} \sim \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right) \begin{matrix} \\ \\ +C_2 \\ \\ +C_2 \end{matrix} \sim$$

$$\sim \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \begin{matrix} \\ \\ \\ \curvearrowright \\ \\ \end{matrix} \sim \left(\begin{array}{ccccc|c} 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

Свободной неизвестной является x_3, ранг системы =3. Частное решение неоднородной системы (при $x_3 = 1$):

$$(1, 1, 1, 1, 0).$$

Общее решение соответствующей однородной системы (с одной свободной неизвестной):

$$(\lambda, \lambda, \lambda, 0, 0), \lambda \in \mathbb{F}_2.$$

Поэтому общее решение данной системы имеет вид:

$$(\lambda, \lambda, \lambda, 0, 0) + (1, 1, 1, 1, 0) = (\lambda + 1, \lambda + 1, \lambda + 1, 1, 0).$$

Пример 11. Над полем $\mathbb{F}_3$ решить систему линейных уравнений

$$\begin{cases} 2x_1 & +x_2 & & +x_4 & = 2, \\ 2x_1 & +2x_2 & +x_3 & +2x_4 & = 1, \\ x_1 & +x_2 & +2x_3 & +x_4 & = 1, \\ x_1 & +2x_2 & +2x_3 & +x_4 & = 2. \end{cases}$$

Имеем,

$$G = \left(\begin{array}{cccc|c} 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 2 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 2 & 2 & 1 & 2 \end{array}\right) \begin{array}{l} \\ +2C_1 \\ +C_1 \\ +C_1 \end{array} \sim \left(\begin{array}{cccc|c} 2 & 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 2 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 & 1 \end{array}\right) \begin{array}{l} \\ \\ \\ +C_2 \end{array} \sim \left(\begin{array}{cccc|c} 2 & 1 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 2 & 1 \end{array}\right)$$

Система несовместна.

Пример 12. Над $\mathbb{F}_5$ решить систему линейных уравнений

$$\begin{cases} 2x_1 & +x_2 & +x_3 & +2x_4 & = 1, \\ 3x_1 & +4x_2 & +2x_3 & +x_4 & = 0, \\ x_1 & +2x_2 & +3x_3 & +x_4 & = 2, \\ 2x_1 & +3x_2 & +x_3 & +x_4 & = 2. \end{cases}$$

Имеем,

$$G = \left(\begin{array}{cccc|c} 2 & 1 & 1 & 2 & 1 \\ 3 & 4 & 2 & 1 & 0 \\ 1 & 2 & 3 & 1 & 2 \\ 2 & 3 & 1 & 1 & 2 \end{array}\right) \begin{array}{l} \\ +C_2 \\ +2C_2 \\ +4C_2 \end{array} \sim \left(\begin{array}{cccc|c} 2 & 1 & 1 & 2 & 1 \\ 0 & 0 & 3 & 3 & 1 \\ 0 & 4 & 0 & 0 & 4 \\ 0 & 2 & 0 & 4 & 1 \end{array}\right) \begin{array}{l} \\ \\ \\ +2C_3 \end{array} \sim \left(\begin{array}{cccc|c} 2 & 1 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 3 & 3 & 1 \\ 0 & 0 & 0 & 4 & 4 \end{array}\right)$$

Система приведена к треугольному виду, а потому имеет единственное решение

$$(1, 1, 1, 1)$$

Пример 13. Над полем $\mathbb{F}_{2^4}$ решить уравнение

$$x^2 + \alpha^2 x + \alpha^9 = 0,$$

если α-корень примитивного многочлена $x^4 + x + 1$.

Поскольку характеристика поля $\mathbb{F}_{2^4}$ равна 2, то привычная формула корней квадратного уравнения здесь не применима (нельзя делить на 2). Для решения этого уравнения применим процедуру Ченя, последовательно подставляя в данное уравнение элементы поля $\mathbb{F}_2$. Пусть $g(x) = x^2 + \alpha^2 x + \alpha^9$. Имеем

$$g(\alpha) = \alpha^2 + \alpha^3 + \alpha^9 = \alpha + \alpha^2 \neq 0,\ g(\alpha^2) = \alpha^4 + \alpha^4 + \alpha^9 = \neq 0,$$

$$g(\alpha^3) = \alpha^6 + \alpha^5 + \alpha^9 = 0,\ g(\alpha^4) = \alpha^8 + \alpha^6 + \alpha^5 = 1 + \alpha \neq 0,$$

$$g(\alpha^5) = \alpha^{10} + \alpha^7 + \alpha^9 = \alpha + \alpha^2 \neq 0,\ g(\alpha^6) = \alpha^{12} + \alpha^8 + \alpha^9 = 0.$$

Мы нашли два корня уравнения $x_1 = \alpha^3$, $x_2 = \alpha^6$, других корней искать не нужно.

Пример 14. Задана квадратная матрица A над полем $\mathbb{F}_{p^m}$. Узнать обратима ли эта матрица и построить обратную, если она существует.

Для того, чтобы квадратная матрица была обратима, необходимо и достаточно, чтобы её определитель был отличен от нуля в поле $\mathbb{F}_{p^m}$. И, если $\det A \neq 0$, то обратная матрица может быть построена по формулам элементов обратной матрицы (как отношение алгебраических дополнений транспонированной матрицы к её ненулевому определителю).

Пусть гад полем $\mathbb{F}_{2^4}$ задана матрица

$$A = \begin{pmatrix} \alpha & \alpha^2 & \alpha^9 \\ \alpha^8 & \alpha & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix}$$

Вычисляем $\det A$:

$$\det A = \alpha^6 + \alpha^5 + \alpha^{19} + \alpha^{10} + \alpha^6 + \alpha^{14} = \cancel{\alpha^3} + \cancel{\alpha^2} + \cancel{\alpha^2} + \cancel{\alpha} + \cancel{\alpha} + \cancel{1} + \cancel{\alpha^2} + \alpha + \cancel{1} +$$

$$+ \cancel{\alpha^3} + \cancel{\alpha^2} + \alpha^3 + 1 = \alpha^3 + \alpha^2 + 1 = \alpha^{13} \neq 0$$

$$\Rightarrow (\det A)^{-1} = \alpha^2$$

Вычисляем алгебраические дополнения для элементов матрицы A:

$$A_{11} = \alpha^5 + \alpha^5 = 0, \quad A_{12} = \alpha^{12} + \alpha^3 = \alpha^2 + \alpha + 1 = \alpha^{10},$$

$$A_{13} = \alpha^{10} + \alpha = \alpha^8;$$

$$A_{21} = \alpha^6 + \alpha^{11} = \alpha, \quad A_{22} = \alpha^5 + \alpha^9 = \alpha^3 + \alpha^2 = \alpha^6,$$

$$A_{23} = \alpha^3 + \alpha^2 = \alpha^6;$$

$$A_{31} = \alpha^5 + \alpha^{10} = 1, \quad A_{32} = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1 = \alpha^{10},$$

$$A_{33} = \alpha^2 + \alpha^{10} = \alpha + 1 = \alpha^4.$$

Поэтому

$$A^{-1} = \begin{pmatrix} 0 & \alpha^3 & \alpha^2 \\ \alpha^{12} & \alpha^8 & \alpha^{12} \\ \alpha^{10} & \alpha^8 & \alpha^6 \end{pmatrix}.$$

Найдём ещё обратную к $A = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ над полем $\mathbb{F}_5$.

Имеем, $\det A = 4$, $(\det A)^{-1} = 4$. Поэтому

$$A^{-1} = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}.$$

Блочные линейные коды (продолжение)

Рассмотрим блочный линейный (n, k)-код C в алфавите $\mathbb{F}_q$. Пусть G-порождающая матрица этого кода. Зафиксируем проверочную матрицу H этого кода. Тогда $H \cdot G^T = 0$, где $k \times n$, $(m \times n)$, $(m \times k)$-соответственно размеры матриц G, H, O.

Фиксирование матрицы H означает, что только кодовые слова $\overline{c}$ (т.е. векторы из пространства C кодовых слов) удовлетворяют равенству $H\overline{c}^T = \overline{0}$. Поэтому, если для принятого слова $\overline{v}$ имеем $H\overline{v}^T \neq \overline{0}$, мы делаем заключение, что в канале произошло искажение кодового слова $\overline{c}$, а потому $\overline{v} = \overline{c} + \overline{e}$. По-

скольку $H\overline{v}^T = H\overline{c}^T + H\overline{e}^T = H\overline{e}^T$, то вектор $H\overline{e}^T$ свидетельствует о наличии ошибок в полученном сообщении и его называют **синдромом** сектора ошибок. Однако, если вектор ошибок совпадает с каким-либо кодовым вектором, то мы получим, что $H\overline{e}^T = \overline{O}$, и значит мы не узнаем об ошибках в канале связи, а потому произведём неправильное декодирование.

Определение 7. Синдромом произвольного вектора $\overline{y} \in \mathbb{F}^{q^n}$ относительно линейного (n,k)-кода C (или его проверочной матрицы H) называется вектор $H\overline{y}^T \in \mathbb{F}_q^m$. Обозначается $S(\overline{y}) = (s_0, s_1, \ldots, s_{m-1})$.

Предполагая, что канал связи достаточно "хорош т.е. количество искажений в одном кодовом слове "мало мы можем исключить ситуацию $S(\overline{e}) = 0$, если кодовые выбирать заведомо отличные от возможных векторов ошибок.

Определение 8. Пусть $\overline{y} = (y_0, y_1, \ldots, y_{n-1})$-произвольный вектор из $\mathbb{F}_q^m$. **Весом Хэмминга** вектора $\overline{y}$ называется число ненулевых координат этого вектора.

Определение 9. Расстоянием Хэмминга между векторами $\overline{x}$ и $\overline{y} \in \mathbb{F}_q^m$ называется число ненулевых координат вектора $\overline{x} - \overline{y}$.

Если $w(\overline{x})$ означает вес Хэмминга для $\overline{x}$, а $d(\overline{x}, \overline{y})$-расстояние Хэмминга между $\overline{x}$ и $\overline{y}$, то имеем

$$d(\overline{x}, \overline{y}) = w(\overline{x} - \overline{y}).$$

Легко проверить, что расстояние Хэмминга на $\mathbb{F}_q^n$ определяет матрицу на пространстве $\mathbb{F}_q^n$, и при этом выполняется неравенство треугольника

$$d(\overline{x}, \overline{z}) + d(\overline{y}, \overline{z}) \geq d(\overline{x}, \overline{y})$$

для любых $\overline{x}, \overline{y}, \overline{z} \in \mathbb{F}_q^n$.

Определение 10. Пусть дан линейный (n,k)-код над $\mathbb{F}_q$. Минимальным

кодовым расстоянием для C (обозначается d_C) называется минимальный вес ненулевых кодовых слов; $d_C = \min\limits_{0 \neq c \in C} w(c)$.

Поскольку разность кодовых слов есть кодовое слово (так как C-подпространство над $\mathbb{F}_q$), то имеем

$$d_C = \min_{\substack{c_1, c_2 \in C \\ c_1 \neq c_2}} (d(c_1, c_2)).$$

Например, пусть $\overline{c}_1 = (101011)$, $\overline{c}_1 = (111001) \in \mathbb{F}_2^6$. Тогда $w(\overline{c}_1) = 4$, $w(\overline{c}_1) = 4$, $d(\overline{c}_1, \overline{c}_2) = w(\overline{c}_1 - \overline{c}_2) = 2$. Отсюда видно, что, если $d_C \geq 5$, а канал связи таков, что в каждом проходящем по каналу слове может быть допущено не более 3^x ошибок, то для принятого слова $\overline{v}$ его синдром (а значит, и синдром вектора ошибок) будет отличен от нулевого вектора.

В теории кодирования исповедуется следующий принцип декодирования в каналах с шумами: "принятое слово $\overline{v}$ декодируется в ближайшее (в смысле расстояния Хэмминга) кодовое слово. Если для данного $\overline{v}$ имеется по крайней мере два кодовых слова, для которых $d(\overline{v}, \overline{c}_1) = d(\overline{v}, \overline{c}_2) \geq d(\overline{v}, \overline{c})$ для всех кодовых слов $\overline{c} \in C$, $\overline{c} \neq \overline{c}_1$, $\overline{c} \neq \overline{c}_2$, то возникает коллизия, приводящая к отказу от декодирования".

Определение 11. Сферой радиуса t, $t \in \mathbb{N}$ с центром в точке $\overline{y}_0 \in \mathbb{F}_q^n$ называется множество векторов $\overline{y} \in \mathbb{F}_q^n$, для которых $d(\overline{y}_0, \overline{y}) \leq t$. (Обозначение: $B_t(y_0)$).

Определение 12. Говорят, что код C исправляет t ошибок и менее, если для каждого $\overline{y} \in \mathbb{F}_q^n$ сфера $B_t(y)$ сожержит не более одного кодового слова.

Теорема 1. *Линейный (n, k)-код C исправляет t ошибок и менее тогда и только тогда, когда $d_C \geq 2t + 1$.*

Доказательство. Если код C исправляет t ошибок, то для любых кодовых слов $\overline{c}_1$, $\overline{c}_2$, $\overline{c}_1 \neq \overline{c}_2$ из предположения $d(\overline{c}_1, \overline{c}_2) \leq 2t$ следует $w(\overline{c}_2 - \overline{c}_1) \leq 2t$.

Возьмём в качестве $\overline{y}$ вектор, у которого первые из t ненулевых координат такие же, что и у вектора $\overline{c}_2 - \overline{c}_1$, а остальные координаты равны 0. Для такого вектора $\overline{y}$ имеем $d(\overline{y}, \overline{c}_2 - \overline{c}_1) = t$, $d(\overline{y}, 0) \le t$, а потому сфера радиуса t с центром в точке $\overline{y}$ содержит два кодовых слова $\overline{0}$ и $\overline{c}_2 - \overline{c}_1$, что противоречиво.

И наоборот, если $d_C \ge 2t + 1$, то для каждого $\overline{y} \in \mathbb{F}_q^*$ имеем

$$d(\overline{y}, \overline{c}_1) + d(\overline{y}, \overline{c}_2) \ge d(\overline{c}_1, \overline{c}_2) \ge 2t + 1$$

для любых $\overline{c}_1, \overline{c}_2 \in C$, $\overline{c}_1 \ne \overline{c}_2$, а значит, хотя бы одно из неравенств

$$d(\overline{y}, \overline{c}_1) > t, \quad d(\overline{y}, \overline{c}_2) > t$$

выполняется, т.е. сфера $B_t(\overline{y})$ содержит не более одного вектора $\overline{c}_1, \overline{c}_2 \in C$, $\overline{c}_1 \ne \overline{c}_2$. □

Теорема 2. *Пусть C-линейный (n, k)-код над $\mathbb{F}_q$. Для каждого кодового слова $\overline{c}$ с весом Хэмминга ℓ, $\ell \ne 0$, существует ℓ столбцов проверочной матрицы H этого кода, такие, что линейная комбинация этих столбцов, коэффициентами которых служат ненулевые координаты вектора $\overline{c}$, равна нулю. И наоборот, если существует ℓ столбцов матрицы H и ℓ ненулевых элементов $a_1, \ldots, a_\ell$ поля $\mathbb{F}_q$ так, что линейная комбинация этих столбцов с коэффициентами a_1,...,a_ℓ равна нулю, то существует кодовый вектор, ненулевые компоненты которого равны $a_1, \ldots, a_\ell$ и расположены на номерах выделенных столбцов матрицы H.*

Доказательство. Действительно, для любого вектора $\overline{v} = (v_1, \ldots, v_n)$ произведение $\overline{v}H^T = v_1\overline{h}_1 + \cdots + v_n\overline{h}_n$, где $\overline{h}_i$ - i-тый столбец матрицы H. Отсюда без труда проверяется справедливость теоремы в обе стороны. □

Следствие 4. *Если проверочная матрица H линейного (n, k)-кода такова, что любые её s столбцов линейно независимы над $\mathbb{F}_q$, то (n, k)-код C в алфавите $\mathbb{F}_q$ имеет минимальное кодовое расстояние $\ge s + 1$.*

Следствие 5. *Пусть C-линейный (n,k)-код над $\mathbb{F}_2$. Тогда d_C равно наименьшему числу столбцов проверочной матрицы H, сумма которых равна $\overline{O}$.*

Пример 15. Пусть C-(7,4)-код над $\mathbb{F}_2$ с проверочной матрицей

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Матрица H не имеет пропорциональных столбцов (значит, любые два столбца линейно независимы). Но сумма второго, третьего и четвёртого столбцов равна нулю. Следовательно, $d_C = 3$, и, в силу теоремы 1, этот код исправляет одиночные ошибки.

Теперь и до конца параграфа мы будем рассматривать линейные (n,k)-коды в алфавите $\mathbb{F}_2$, хотя излагаемая теория верна и над произвольным алфавитом $\mathbb{F}_q$.

Если по каналу связи был послан кодовый вектор $\overline{c}$ И в канале произошло ℓ искажений символов, то для принятого слова $\overline{v}$ имеем $d(\overline{c},\overline{v}) = \ell$, и значит, при $\ell < d_C$ слово $\overline{v}$ не совпадёт ни с каким кодовым словом. Для такого кода искажение в $d_C - 1$ или меньше символах не приведёт к кодовому слову. Значит, линейный (n,k)-код C с минимальным кодовым расстоянием d_C способен обнаружить появление ошибок в количестве $d_C - 1$ и менее (но не обязательно их исправить).

Мы будем считать, что количество искажений в кодовых словах после прохождения канала с шумами меньше, чем d_C, т.е. вероятность противоположного события достаточно малая. Только в этих предположениях имеет смысл пользоваться данным кодом.

Пусть C-данный линейный (n,k)-код в алфавите $\mathbb{F}_2$. Код C содержит 2^k слов, а в пространстве $\mathbb{F}_2^n$ имеется 2^n векторов. Разобьём множество векторов

из $\mathbb{F}_2^n$ на классы следующим образом:

класс K_1 состоит из 2^k кодовых слов;

класс K_2 состоит из векторов вида $\overline{e}_2 + \overline{c}$, где $\overline{c}$ пробегает всё множество C, а вектор $\overline{e}_2$ имеет наименьший вес среди векторов из $\mathbb{F}_q \setminus C$;

класс K_3 состоит из векторов вида $\overline{e}_3 + \overline{c}$, $\overline{c} \in C$, $\overline{e}_3$ вектор наименьшего веса Хэмминга из $\mathbb{F}_q \setminus (C \bigcup K_2)$,

и так далее.

Каждый класс K_i содержит точно 2^k векторов, эти векторы различны, а классы K_i и K_j не пересекаются при $i \neq j$ (Действительно, из $K_i \bigcap K_j \neq \varnothing$ следует, что найдутся векторы $\overline{c}_\ell$ и $\overline{c}_m$ из C такие, что

$$\overline{e}_i + \overline{c}_\ell = \overline{e}_j + \overline{c}_m.$$

Пусть для определённости $j > i$. Тогда имеем

$$\overline{e}_j = \overline{e}_i + (\overline{c}_\ell + \overline{c}_m) = \overline{e}_i + \overline{c}, \text{ где } \overline{c} \in C,$$

но это противоречит выбору $\overline{e}_j$ как вектора с наименьшим весом и не лежащем ни в каком из предыдущих классах).

Классы K_i будем называть смежными классами пространства $\mathbb{F}_2$ по коду C. Ясно, что всего будем иметь $2^{n-k} = 2^m$ классов. Выделенные векторы $\overline{e}_i \in K_i$, $(\overline{e}_0 = \overline{0})$, имеют наименьший вес Хэмминга в классе K_i, но в этом классе кроме вектора $\overline{e}_i$ могут находиться и другие векторы с весом, равным весу $\overline{e}_i$.

Результаты разбиения множества векторов пространства $\mathbb{F}_2^n$ на классы удобно записывать с помощью таблицы

Выделенные векторы $\overline{e}_i$, $i = 2, 3, \ldots, 2^m$, называются лидерами классов K_i. Лидером класса $K_1 = C$ является нулевой вектор $\overline{e}_1 = (0, \ldots, 0)$.

Лидер	Элементы класса $K_j \setminus \{\overline{e}_j\}$					Синдром лидера
$\overline{c}_1=\overline{0}$	$\overline{c}_2$	$\cdots$	$\overline{c}_j$	$\cdots$	$\overline{c}_{2^k}$	$S(\overline{0})=0$
$\overline{e}_2$	$\overline{c}_2+\overline{e}_2$	$\cdots$	$\overline{c}_j+\overline{e}_2$	$\cdots$	$\overline{c}_{2^k}+\overline{e}_2$	$S(\overline{e}_2)$
$\overline{e}_3$	$\overline{c}_2+\overline{e}_3$	$\cdots$	$\overline{c}_j+\overline{e}_3$	$\cdots$	$\overline{c}_{2^k}+\overline{e}_3$	$S(\overline{e}_3)$
$\cdots\cdots$	$\cdots\cdots$	$\cdots$	$\cdots\cdots$	$\cdots$	$\cdots\cdots$	$\cdots\cdots\cdots\cdots$
$\overline{e}_{2^m}$	$\overline{c}_2+\overline{e}_{2^m}$	$\cdots$	$\overline{c}_j+\overline{e}_{2^m}$	$\cdots$	$\overline{c}_{2^k}+\overline{e}_{2^m}$	$S(\overline{e}_{2^m})$

Пример 16. Пусть C-линейный $(6,3)$-код с порождающей матрицей

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Порождающая матрица позволяет записать все кодовые слова как всевозможные линейные комбинации строк матрицы G с коэффициентами из $\mathbb{F}_2$. Имеем

$$\overline{c}_1 = (000000),\ \overline{c}_2 = (101010),\ \overline{c}_3 = (010110),\ \overline{c}_4 = (110001)$$

$$\overline{c}_5 = (111100),\ \overline{c}_6 = (011011),\ \overline{c}_7 = (100111),\ \overline{c}_8 = (001101).$$

Поэтому имеем такую таблицу классов

(000000)	(101010)	(010110)	(110001)	(111100)	(011011)	(100111)	(001101)
(100000)	(001010)	(110110)	(010001)	(011100)	(111001)	(000111)	(101101)
(010000)	(111010)	(000110)	(100001)	(101100)	(001011)	(110111)	(011101)
(001000)	(100010)	(011110)	(111001)	(110100)	(010011)	(101111)	(000101)
(000100)	(101110)	(010010)	(110101)	(111000)	(011111)	(100011)	(001001)
(000010)	(101000)	(010100)	(110011)	(111110)	(011001)	(100101)	(001111)
(000001)	(101011)	(010111)	(110000)	(111101)	(011010)	(100110)	(001100)
(100100)	(001110)	(110010)	(010101)	(011000)	(111111)	(000011)	(101001)

Рассмотрим произвольный класс

$$K_j = \{\overline{e}_j + \overline{c}_i \,|\, \overline{c}_i \in C,\ i = 1, 1, \ldots, 2^k\}.$$

Тогда имеем

$$S(\overline{e}_j + \overline{c}_i) = S(\overline{e}_j) + S(\overline{c}_i) = S(\overline{e}_j),\ \ i = 1, \ldots, 2^k.$$

Это означает, что элементы одного и того же класса имеют равные синдромы. Используя принцип выбора лидера смежного класса, мы, в силу метода де-

кодирования в ближайшее кодовое число, получаем алгоритм декодирования по лидеру смежного класса:

I шагВычисляем синдром принятого вектора $\overline{v}$: $S(\overline{v}) = H\overline{v}^T$.

II шагВ таблице синдромов находим строку, для которой $S(\overline{v}) = S(\overline{e}_j)$.

III шагДекодируем принятое слово $\overline{v}$ в слово $\overline{c} = \overline{v} + \overline{e}_j$.

Такой метод декодирования минимизирует ошибку декодирования, так как по принятому нами соглашению вероятность появления на входе канала слова $\overline{v}$ уменьшается с увеличением количества искаженных символов. В поддержку указанного метода кодирования указывает и такой факт, что расстояние Хэмминга между принятым словом $\overline{v}$ и кодовым словом $\overline{c}$ (смотри III шаг) не больше, чем расстояние между $\overline{v}$ и другим (отличным от $\overline{c}$) кодовым словом. Действительно,

$$d(\overline{v}, \overline{c}') = w(\overline{v} + \overline{c}') = w(\overline{e}_j + \overline{c} + \overline{c}') = w(\overline{e}_j + \overline{c}''),\ \overline{c}'' = \overline{c} + \overline{c}'.$$

А поскольку лидер $\overline{e}_j$ и вектор $\overline{e}_j + \overline{c}''$ находятся в одном и том же смежном классе, то в силу выбора лидера в смежном классе, заключаем $w(\overline{e}_j) \leq w(\overline{e}_j + \overline{c}'')$, а потому $d(\overline{v}, \overline{c}) \leq d(\overline{v}, \overline{c}')$.

Приведённые рассуждения также показывают, что в случаях, когда лидер смежного класса может быть выбран единственным образом, то декодирование по лидеру смежного класса имеет минимальную ошибку декодирования. |indent Обозначим через A число лидеров классов смежности, имеющих вес j. Числа $A_0, A_1, \ldots, A_n$ будем называть **весовым распределением лидеров**. В некоторых случаях весовое распределение позволяет оценить вероятность ошибки декодирования. Рассмотрим двоичный симметричный канал (ДСК) с вероятностью p искажения одного символа, т.е.

$$P(0|1) = P(1|0) = p$$

(здесь $P(0|1)$ означает вероятность того, что посланный символ 1 перейдет в символ 0).

Поскольку ошибка декодирования появляется тогда и только тогда, когда вектор ошибок не является лидером смежного класса, получаем, что вероятность неправильного декодирования в таком канале равна

$$P(E) = 1 - \sum_{i=0}^{n} A_i p^i (1-p)^{n-i}.$$

В рассмотренном выше примере 15 для линейного $(6,3)$-кода с порождающей матрицей G имеем следующее распределение весов:

$$A_0 = 1,\ A_1 = 6,\ A_2 = 1,\ A_3 = A_4 = A_5 = A_6 = 1.$$

Поэтому

$$P(E) = 1 - (1-p)^6 - 6p(1-p)^5 - p^2(1-p)^4.$$

Для $p = 10^{-2}$ получаем $P(E) \approx 1.4 \cdot 10^{-3}$.

Теорема 3. *Пусть C-линейный (n,k)-код с минимальным кодовым расстоянием d_C. Тогда все векторы веса $t = \left[\frac{d_C - 1}{2}\right]$ и меньше могут быть исследованы как лидеры смежных классов, но хотя бы один вектор веса $t+1$ не может быть лидером смежного класса.*

Утверждение теоремы следует из определения кода, исправляющего t ошибок, а рассмотренный пример 16 иллюстрирует сказанное для $t = 1$. (Например, вектор (010001) не может быть лидером).

Пример 17. Рассмотрим $(7,4)$-код с порождающей матрицей

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Проверочная матрица H имеет размер $(7,3)$, так что число смежных классов

равно $2^3 = 8$ и она имеет вид

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

У матрицы H любые два столбца не равны, но первый столбец равен сумме двух последних. Следовательно, $d_C = 3$. Поэтому код C исправляет одиночные ошибки. Об этом также свидетельствует тот факт, что любые два вектора с весом 1 не могут находиться в одном и том же смежном классе. Таких векторов всего 7, которые, вместе с нулевым, строкой дают восемь различных лидеров, т.е. каждый смежный класс имеет в качестве лидера вектор веса ≤ 1, что позволяет однозначно исправить одиночные ошибки.

Например, если принято сообщение $\overline{v} = (0010010)$, мы вычисляем $S(\overline{v}) = H\overline{v}^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ и сравниваем с синдромами векторов веса 1:

$$S(1000000) = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},\ S(0100000) = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix},$$

$$S(0010000) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},\ S(0001000) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix},$$

$$S(0000100) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ S(0000010) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ S(0000001) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Откуда заключаем, что ошибка в четвертой позиции, а потому $\overline{c} = (0011010)$. Если бы произошла двойная ошибка, например, $\overline{e} = (0010010)$, а мы получи-

ли $\overline{v} = (1001110)$, то вычисления дают $S(\overline{v} = S(\overline{e})) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$. Теперь при декодировании по методу смежных классов мы имели бы ошибочный результат $\overline{e} = (0000001)$, $\overline{c} = (1001111)$ вместо отправленного сообщения $\overline{c}_0 = (1011100)$.

Таким образом, преувеличивая возможности декодирования по методу смежных классов, мы можем прийти к ошибочному результату.

Коды Хэмминга

Код Хэмминга был первым примером линейного (n, k)-кода, позволяющим обнаружить и исправить одиночные ошибки. Зафиксируем натуральное $m \geq 3$ и рассмотрим матрицу, столбцами которой является m-значная запись чисел от 1 до 2^{m-1}. Мы получим матрицу H размера $2^{m-1} \times m$, которую будем рассматривать как проверочную матрицу линейного (n, k)-кода, где $n = 2^m - 1$, $k = n - m = 2^m - m - 1$. Этот код называется кодом Хэмминга. Очевидно, что столбцы матрицы H различны, но имеется столбец, равный сумме двух других. Поэтому этот код исправляет одиночные ошибки. Имеется $2^{n-k} = 2^m$ смежных классов, а векторы

$$(000\cdots00),\ (100\cdots00),\ (010\cdots00),\ \ldots,\ (000\cdots10),\ (000\cdots01)$$

принадлежат различным смежным классам.

Каждая сфера радиуса 1 содержит $n+1$ точку из $\mathbb{F}_2^n$, а потому непересекающиеся сферы с центрами в кодовых словах содержат $(n+1)2^k = 2^m \cdot 2^k = 2^n$ точек из $\mathbb{F}_2^n$, т.е. эти сферы покрывают без пересечений всё пространство $\mathbb{F}_2^n$.

Определение 13. Код, исправляющий t-ошибок и менее называется **совершенным кодом, если**, если все векторы с весом Хэмминга $\leq t$ являются

лидерами смежных классов и других лидеров не имеется.

Поэтому код Хэмминга является совершенным кодом, исправляющим одиночные ошибки. Кроме кода Хэмминга существует ещё один бинарный совершенный (23,12)-код Галея. Рассмотренный в примере 17 (7,4)-код является бинарным кодом Хэмминга. В алфавите $\mathbb{F}_q$ также существуют совершенные коды.

Построим обобщённый код Хэмминга. Пусть $m \geq 3$. Положим $n = \frac{q^m-1}{q-1}$ и обозначим через α примитивный элемент поля $\mathbb{F}_{q^m}$. Тогда порядок α в группе $\mathbb{F}_{q^m}^*$ равен $q^m - 1$. Напомним, что каждый элемент поля $\mathbb{F}_{q^m}$ однозначно представляется линейной комбинацией элементов 1, α,...,α^{m-1} с коэффициентами из $\mathbb{F}_q$:

$$\alpha^j = \sum_{i=0}^{m-1} a_{ij}\alpha^i,\ j = 0, 1, \ldots, n-1.$$

Образуем матрицу H, столбцами которой являются $\overline{h}_j = \begin{pmatrix} a_{0j} \\ \vdots \\ a_{m-1,j} \end{pmatrix}$, т.е.

$$H = \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0,n-1} \\ a_{10} & a_{11} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{pmatrix}$$

Обобщённым кодом Хэмминга называется линейный (n, k)-код в алфавите $\mathbb{F}_q$, проверочная матрица которого равна H (здесь $k = n - m$).

Теорема 4. *Обобщённый код Хэмминга является совершенным кодом, исправляющим одиночные ошибки.*

Доказательство. Различные столбцы матрицы представляют различные степени α, а потому из их пропорциональности следует, что $\alpha^i = a\alpha^j$, $a \in \mathbb{F}_q$,

$0 \le j < i \le n-1$. Но тогда $a = \alpha^{i-j}$, а потому $1 = a^{q-1} = \alpha^{(i-j)(q-1)}$, что невозможно, так как $0 < (i-j)(q-1) < n(q-1) = q^m - 1$, а порядок α равен $q^m - 1$. Таким образом, для рассматриваемого кода: $d_C \ge 3$, т.е. код исправляет одиночные ошибки. Каждая сфера $B_1(\overline{y})$, $\overline{y} \in \mathbb{F}_q$ содержит точку $\overline{y}$ и ещё $n(q-1)$ точек, отстоящих от $\overline{y}$ на расстоянии 1, т.е. $|B_1(\overline{y})| = 1 + n(q-1) = q^m$. Когда $\overline{y}$ пробегает множество всех q^k кодовых слов, то множество $\bigcup\limits_{\overline{c} \in C} B_1(\overline{c})$ будет содержать $q^k \cdot |B_1(\overline{y})| = q^{k+m} = q^n$ векторов. Значит, эти сферы покрывают все пространство $\mathbb{F}_q^n$. Следовательно, обобщённый код Хэмминга является совершенным кодом. $\square$

Список литературы

[1] Shu Lin, Daniel J. Costello, Jr., Error control coding. Fundamentals and Applications. - Prentice-Hall, Inc. Englewood Cliffs, New Jersey. - 1983. - 603 pp.

[2] Березюк Н. Т., Андрущенко А. Г., Мощицкий С. С. и др., Кодирование информации (двоичные коды. - Харьков, издательское объединение "Вища школа". - 1978. - 252 с.

[3] Блейхут Р. Теория и практика кодов, контролирующих ошибки, Перевод с англ.: И.И. Грушко, В.М. Блиновский. Под редакцией: К.Ш. Зигангирова. — М.: Мир. - 1986. — 576 с.

[4] Р. Морелос-Сарагоса, Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. - Москва: Техносфера. - 2005. - 320с.