БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра дифференциальных уравнений

В. А. Липницкий, Н. В. Чесалин

ЛИНЕЙНЫЕ КОДЫ И КОДОВЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

Учебно-методическое пособие для студентов механико-математического факультета БГУ

Минск
2008

УДК 519.711.4 (075.8)
ББК 22.18я73
Л61

Рекомендовано
Ученым советом механико-математического факультета
9 декабря 2008 г., протокол № 4

Рецензент
доктор технических наук,
профессор *А. Н. Курбацкий*

Липницкий, В. А.

Л 61 Линейные коды и кодовые последовательности: учеб.-метод. пособие для студентов мех.-мат. фак. БГУ / В. А. Липницкий, Н. В. Чесалин. — Минск: БГУ, 2008. — 41 с.

Учебно-методическое пособие “Линейные коды и кодовые последовательности” является введением в теорию помехоустойчивых кодов.

Предназначено для студентов механико-математического факультета.

УДК 517.711.4 (075.8)
ББК 22.18я73

Предисловие

Учебно-методическое пособие написано в соответствии с действующей программой специального курса «Теория помехоустойчивых кодов» и предназначено для студентов высших учебных заведений, изучающих теорию кодирования и криптографию. Его основная цель — познакомить студентов с основными понятиями теории линейных кодов и кодовых последовательностей, некоторыми основными методами кодирования и декодирования, а также с проблемами данной теории.

Учебно-методическое пособие состоит из введения, двух глав и списка литературы.

Введение

Теория и практика помехоустойчивого кодирования, в отличие от многих иных разделов научного знания, имеет точную дату своего рождения. Это 1948 год. Именно в этом году американский инженер-исследователь Клод Шеннон получил ряд результатов, на основе которых сделал, знаменитый впоследствии, секретный доклад Сенату США. Всё это легло в основу его монографии [1].

До Шеннона было широко распространено мнение, что для достижения сколь угодно малой вероятности ошибки в каналах связи скорость передачи сообщений должна стремиться к нулю [17]. Созданная теория информации характеризовала канал связи единственным параметром — пропускной способностью. Используя вероятностные методы, Шеннон доказал, что возможно передавать информацию со скоростью, сколь угодно близкой снизу к пропускной способности канала связи и со сколь угодно малой вероятностью ошибки. За прошедшие 60 лет появилось большее количество исследований, связанных с построением эффективных методов кодирования информации для передачи по реальным каналам связи с шумами, но пионерская работа Клода Шеннона до сих пор остается основной для различных исследований по защите информации от помех и несанкционированного доступа.

Эффективные методы кодирования и декодирования информации с привлечением теории конечных полей были изложены в основополагающих работах Рида и Соломона (1960 г.), Хоквингема (1959 г.), Боуза и Чоудхури (1960 г.), Горнстейна и Цирлера (1961 г.) и Питерсона (1961 г.).

Выбрав в качестве алфавита кода поле Галуа, удалось свести задачу к решению соответствующих алгебраических уравнений. Причем вычислительная сложность таких алгоритмов оказалась на порядок ниже пол-

ного перебора. Построенная в последнее десятилетие теория помехоустойчивого кодирования нашла широкое применение в различных областях информатики и радиоэлектроники. Особую роль играют низкоскоростные коды максимальной длины, которые применяются в радиолокационных и навигационных системах связи. Отдельные кодовые слова данного кода называют M –последовательностями. Такие последовательности можно задавать с помощью специального устройства, называемого регистром сдвига с обратной связью.

В последней четверти XX века вышел ряд монографий по теории кодирования, в частности, [2-6] Среди них выделяется своей фундаментальностью и полнотой информации на момент издания монография [2].

В данной работе излагаются основные сведения о помехоустойчивых кодах и кодовых последовательностях. Для усвоения излагаемого материала необходимо свободное владение знаниями из линейной алгебры на уровне первого курса вуза, а также теории конечных полей.

Следует отметить, что существуют различные подходы к описанию помехоустойчивых кодов. В отдельных случаях удобен полиномиальный подход, доведенный на практике до реализации в технических устройствах. Математическую основу этого подхода составляют фактор-кольца колец полиномов по своим идеалам, как максимальным, так и не максимальным.

Нам представляется более естественным и более простым матричный подход – задание кодов с помощью порождающих или проверочных матриц.

Как уже отмечалось, периодические кодовые последовательности, являясь тесно связанными с заданным кодом, имеют большое самостоятельное прикладное значение. Они имеют широкое применение в радиолокационных и навигационных системах, системах связи и др.

Изучению свойств подобных периодических последовательностей посвящены некоторые известные работы С. Голомба [12-13]. Им была предложена классификация $T = q^n - 1$ периодических последовательностей по некоторым выделенным свойствам. До сих пор остается нерешенной проблема С. Голомба для двоичных последовательностей о совпадении класса M-последовательностей с классом периодических последовательностей сдвигового регистра линейной сложности n, обладающих идеальной автокорреляционной функцией. Для $n \le 10$ контрпримеров не существует, а для $n > 10$ само утверждение не доказано, но и контрпримеров не найдено.

В этой связи интерес представляют любые новые характеристики и свойства кодовых последовательностей и способы их задания.

1. Основы теории линейных кодов

Equation Chapter 1 Section 1

1.1. Понятие линейного кода

Понятие линейного кода — одно из первичных, базовых понятий теории и практики помехоустойчивого кодирования. Сформировалось в теории информации к середине XX века. Аккумулирует в себе достаточно широкую научно-философскую концепцию.

Предполагается, что исходная информация записывается в виде блоков — конечных последовательностей фиксированной длины k символов из данного поля P. Другими словами, всякое информационное слово представляет собой k – разрядный вектор — произвольный вектор из линейного пространства $P_k = \{(x_1, x_2, ..., x_k) | x_i \in P\}$. Такая форма представления информации кодированием не считается. Главная цель кодирования — обеспечить надежную передачу информации в каналах с шумами, то есть помехами. В линейных кодах цель эта достигается введением покоординатных проверок. С математической точки зрения — это линейное отображение линейного пространства P_k в пространство большей размерности P_n, $n > k$. Все мы привыкли к матричному заданию линейных отображений векторных пространств. Следовательно, кодирование есть, по сути дела, умножение информационных слов-векторов на некоторую матрицу G порядка $k \times n$ с коэффициентами из поля P.

Поясним этот момент сведениями из линейной алгебры. Если оговорено или из контекста ясно, с какими базисами этих пространств мы имеем дело, то линейный оператор $\varphi : P_k \to P_n$ однозначно определяется матрицей A_φ этого оператора в данных базисах. Пусть $\overline{u}_1, \overline{u}_2, ..., \overline{u}_k$ — базис пространства P_k, а $\overline{v}_1, \overline{v}_2, ..., \overline{v}_n$ — базис пространства P_n. Векторы $\varphi(\overline{u}_1), \varphi(\overline{u}_2), \ldots, \varphi(\overline{u}_k)$ разложим по базису пространства P_n. Полученные координаты векторов $\varphi(\overline{u}_1), \varphi(\overline{u}_2), \ldots, \varphi(\overline{u}_k)$ составляют столбцы матрицы A_φ. Как известно, для всякого вектора $\overline{x} = (x_1, x_2, ..., x_k) \in P_k$ вектор-столбец $A_\varphi(x) = (y)$, где (x) — столбец из координат вектора $\overline{x}$, состоит из координат вектора $\varphi(\overline{x})$ в базисе $\overline{v}_1, \overline{v}_2, ..., \overline{v}_n$ пространства P_n. Протранспонировав равенство $A_\varphi(x) = (y)$, получим соотношение: $\varphi(\overline{x}) = \overline{x} \cdot A_\varphi^T$. Таким образом, из сказанного выше следует, что матрица $G = A_\varphi^T$.

Получаемые в результате умножения векторов пространства P_k на матрицу G $n-$разрядные векторы — векторы из пространства P_n — называются кодовыми словами. В совокупности они образуют $k-$мерное подпространство L в линейном пространстве P_n. Таким образом, получен линейный (n,k)–код L над полем P. Здесь n — длина, а k — размерность кода L. Изложенную концепцию неявно и предполагает следующее формально-математическое

Определение 1.1. *Линейным $(n,k)-$кодом над полем P называется произвольное $k-$мерное подпространство линейного пространства P_n. Параметр n называется длиной кода, а $k-$размерностью кода.*

Линейный $(n,k)-$код называется высокоскоростным, если отношение k/n близко к 1, и низкоскоростным, если отношение $k/n<<1-$близко к нулю.

Пример 1.1. С середины XX века долгое время в американских системах цифровой связи передача данных осуществлялась в так называемом ASCII-формате. Этот формат требовал передавать данные блоками по 8 двоичных бит, 7 из них были информационными, а 8-й – был проверочным, в нём записывался 0 или 1 так, чтобы во всём байте, то есть во всём блоке сохранялось чётное число единиц. Таким образом, восьмой бит осуществлял проверку на чётность во всём байте — все восемь координат x_i, $1\le i\le 8$, байта в совокупности удовлетворяли линейному однородному уравнению:

$$x_1+x_2+\ldots+x_8=0.$$

Согласно одному из фундаментальных результатов линейной алгебры, множество решений любой однородной системы уравнений от n неизвестных с коэффициентами из поля P образует подпространство в пространстве P_n, причём размерность подпространства решений равна $k=n-r$, где r — ранг матрицы H коэффициентов системы. Часто в линейной алгебре данное подпространство называют ядром матрицы H и потому обозначают через $KerH$.

Множество решений данного однородного уравнения представляют весь спектр векторов-слов ASCII-формата. В соответствии с отмеченным выше результатом, эти решения – двоичные векторы 8-мерного пространства P_8 над полем Галуа $P=GF(2)$ из двух элементов — образуют в P_8 7-мерное подпространство $L-(8,7)$ — линейный код над полем из двух элементов. Легко видеть, что Ф.С.Р. — базис пространства L решений данного уравнения – образуют следующие 7 векторов:

$\overline{e}_1 = (1000\,0001)$, $\overline{e}_2 = (0100\,0001),...,$ $\overline{e}_7 = (0000\,0011)$. Пусть G — $(7\times 8)-$матрица, строки которой состоят из координат векторов $\overline{e}_1, \overline{e}_2, ..., \overline{e}_7$. Умножением произвольных 7-мерных информационных двоичных векторов на матрицу G мы преобразуем их в ASCII-формат.

Пример 1.2. Очевидно, пример 1.1 допускает обобщение на коды любой длины. Это двоичные, как и в примере 1.1, коды. Каждое кодовое слово получается добавлением к информационным блокам длиной k единственного $k+1-$ого проверочного разряда, в нём записывается 0 или 1 так, чтобы во всём блоке сохранялось чётное число единиц. Здесь, $n = k+1$. Такие коды называют кодами с проверкой на чётность. Будем их в дальнейшем обозначать символом C_+.

Замечание. Глубокое осмысление данного примера Клодом Шенноном привело к формулировке его знаменитой теоремы [1], выражающей главную цель и назначение помехоустойчивых кодов.

Теорема 1.1 (Шеннон К.,1948 год). *Введением избыточности в передаваемую в зашумлённом канале связи информацию можно добиться исправления возникающих в процессе передачи этой информации сколь угодно сложных ошибок.*

Этот же пример привел Роберта Хемминга — современника и соотечественника К. Шеннона — к созданию конкретных основ помехоустойчивого кодирования. Первым шагом в этом направлении было развитие примера 1.2, которым является

Пример 1.3. Пусть $P = GF(2)$ — поле Галуа из двух элементов; $k = 4$, то есть передаваемая информация состоит из 4-мерных векторов $\overline{x} = (x_1, x_2, x_3, x_4)$ с координатами x_i, $1 \le i \le 4$, со значениями $0,1 \in GF(2)$. Каждый вектор $\overline{x}$ кодируем, присоединив к нему координаты x_5, x_6, x_7, вычисленные по правилам: $x_5 = x_1 + x_2 + x_4$, $x_6 = x_1 + x_3 + x_4$, $x_7 = x_2 + x_3 + x_4$. Тем самым получим линейный код C, состоящий из векторов $\overline{z} = (x_1, x_2, \ldots, x_7) \in P_7$, удовлетворяющих проверочным соотношениям:

$$\begin{cases} x_1 + x_2 + x_4 + x_5 = 0, \\ x_1 + x_3 + x_4 + x_6 = 0, \\ x_2 + x_3 + x_4 + x_7 = 0. \end{cases} \qquad (1.1)$$

Это известный совершенный систематический линейный $(7,4)$ — код, принадлежащий семейству кодов Хэмминга.

1.2. Порождающая и проверочная матрицы линейного кода

Пусть C — линейный (n,k) – код над полем P. Пусть $\overline{g}_1,\overline{g}_2,\ldots,\overline{g}_k$ — базис кода C.

Определение 1.2. *Порождающей матрицей кода* C *называется* (k,n) – *матрица* G, *строки которой состоят из координат векторов* $\overline{g}_1,\overline{g}_2,\ldots,\overline{g}_k$ *в каком-нибудь заданном базисе пространства* P_n.

Приведенная выше в примере 1.1 матрица G является, очевидно, матрицей, порождающей ASCII-формат. Название порождающей матрицы объясняется тем, что любое кодовое слово кода C является линейной комбинацией строк матрицы G, порождается строками матрицы G. Из определения непосредственно следует, что ранг матрицы G равен k.

Здесь следует вспомнить, что базисов в любом нетривиальном пространстве достаточно много. Поэтому из определения 1.2 так же вытекает, что порождающая матрица кода определена неоднозначно.

Определение 1.3. *Матрица* H *порядка* $m\times n$, $m=n-k$, *называется проверочной матрицей кода* C, *если* $KerH=C$.

Из этого определения следует, что код C состоит из решений однородной системы линейных уравнений $H\cdot\overline{x}^T=\overline{0}^T$, то есть H – матрица коэффициентов системы из m проверочных линейных соотношений, определяющих код C.

Пример 1.4. Код C_+ с проверкой на чётность из примера 1.2 состоит из векторов-решений единственного уравнения $x_1+x_2+\ldots+x_n=0$ над полем $P=GF(2)$. Следовательно, проверочная матрица кода C_+ есть $(1\times n)$ — матрица, имеющая вид: $H=(11\ldots1)$.

Пример 1.5. Согласно определению 1.3 матрица коэффициентов приведенной выше системы линейных уравнений (1)

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

есть проверочная матрица $(7,4)$ — кода Хэмминга, определенного в примере 1.3. Так как базисный минор матрицы H расположен в последних трех столбцах, то x_1,x_2,x_3,x_4 — свободные переменные системы линейных уравнений (1.1). Отсюда легко получаем порождающую матрицу кода Хэмминга:

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

Координаты базиса ядра матрицы G составляют проверочную $(n-k)\times n$ – матрицу H кода L: только для векторов $\overline{c} \in L \quad H \cdot \overline{c}^T = \overline{0}$ и только для них. Каждая из матриц G или H однозначно определяет код L.

Предложение 1.1. *Пусть H — проверочная матрица кода C. Тогда для всякой невырожденной квадратной матрицы A порядка $m = n - k$ матрица $A \cdot H$ также является проверочной для кода C.*

Доказательство. Ранг матрицы AH равен m. Следовательно, $\dim\ker(AH) = n - m = k$. Для каждого вектора $\overline{c} \in C$ произведение $H\overline{c}^T = \overline{0}^T$ по определению проверочной матрицы кода. В силу ассоциативности векторно-матричных произведений $(AH)(\overline{c}^T) = A(H\overline{c}^T) = A\overline{0}^T = \overline{0}^T$. Это означает, что $\ker(AH) \supseteq \ker H = C$. Поскольку $\dim\ker(AH) = \dim\ker H$, то отсюда следует, что $\ker(AH) = C$, то есть AH — проверочная матрица кода C, что и требовалось доказать.

Предложение 1.2. *Пусть H и H_1 — две проверочные матрицы линейного (n, k)-кода C. Тогда существует квадратная $m \times m$ - матрица A для $m = n - k$, такая, что $AH = H_1$.*

Доказательство. Согласно предложению 1.1 матрицы H и H_1 состоят из координат базисов пространства решений системы уравнений (3.2). Пусть $[\overline{h}] = [\overline{h}_1, \overline{h}_2, ..., \overline{h}_m]$ и $[\overline{h}'] = [\overline{h}'_1, \overline{h}'_2, ..., \overline{h}'_m]$ — строки из векторов этих базисов. Пусть T — матрица перехода от базиса

$$\overline{h}_1, \overline{h}_2, ..., \overline{h}_m \tag{1.2}$$

к базису

$$\overline{h}'_1, \overline{h}'_2, ..., \overline{h}'_m \tag{1.3}$$

Тогда $[\overline{h}'] = [\overline{h}]T$. Оба базиса заданы своими координатами в некотором базисе

$$\overline{e}_1, \overline{e}_2, ..., \overline{e}_m \tag{1.4}$$

пространства P_m. Пусть A и B — матрицы со столбцами — координатами векторов систем (1.2) и (1.3) соответственно в базисе (1.4). Тогда $\left[\overline{h}\right]=\left[\overline{e}\right]A=\left[\overline{e}_1,\overline{e}_2,...,\overline{e}_m\right]Aq$; $A=H^{\mathrm{T}}$; $B=H_1^{\mathrm{T}}$. $[\overline{h}']=[\overline{e}]B=[\overline{h}]T=[\overline{e}]AT$. Следовательно, $B=A\cdot T$ или $T^{\mathrm{T}}A^T=B^T$, то есть $H_1=A\cdot T$ для невырожденной квадратной $m\times m-$матрицы $A=T^{\mathrm{T}}$. Предложение доказано.

Из предложений 1.1 и 1.2 следует критерий того, что две матрицы являются проверочными матрицами одного и того же линейного кода.

Теорема 1.2. *Пусть H — проверочная $m\times n$ — матрица линейного $(n,k)-$ кода C. Матрица H^* порядка $m\times n$ является проверочной матрицей этого же кода тогда и только тогда, когда найдется такая невырожденная $m\times m$ - матрица A, что $H^*=AH$.*

Следствие 1. *Если у проверочной матрицы H кода C столбцы $h_{i1},h_{i2},\ldots,h_{im}$ образуют ненулевой (нулевой) минор, то и все остальные проверочные матрицы кода C обладают тем же свойством.*

Следствие 2. *Количество различных проверочных матриц линейного $(n,k)-$ кода над конечным полем P совпадает с количеством различных невырожденных квадратных матриц порядка m в поле P, то есть с порядком группы $GL_m(P)$ невырожденных квадратных матриц порядка m над полем P.*

Следствие 2 позволяет определить количество проверочных матриц у данного линейного кода над конечным полем P. Так над полем $GF(2)$ из двух элементов, по теореме 4.11 [11], группа матриц $GL_m(GF(2))$ имеет порядок

$$\left|GL_m(GF(2))\right|=(2^m-1)(2^m-2)\cdot\ldots\cdot(2^m-2^{m-1})=$$
$$=2^{0,5m(m-1)}\left(2^m-1\right)\left(2^{m-1}-1\right)\cdot\ldots\cdot\left(2^2-1\right).$$

В частности, при $m=5$ этот порядок равен

$$2^{10}\left(2^5-1\right)\left(2^{4-1}-1\right)\left(2^3-1\right)\left(2^2-1\right)=9999360.$$

Это означает, в частности, что у $(31,26)-$кода Хемминга над полем $GF(2)$ имеется 9999360 различных проверочных матриц. При $m=3$ искомый порядок равен $2^3\left(2^3-1\right)\left(2^{2-1}-1\right)=168$. Это означает, что у $(7,4)-$кода Хемминга над полем $GF(2)$ имеется 168 различных проверочных матриц.

1.3. Эквивалентные коды

Определение 1.4. *Коды, отличающиеся перестановкой отсчетов, то есть координат, называются эквивалентными.*

Из определения следует существование перестановочной матрицы $П$, такой, что для каждого кодового слова $\overline{c}$ кода C, вектор $\overline{c} \cdot П = \overline{c}'$ есть кодовое слово эквивалентного (коду C) кода C'.

Из этого замечания следует

Предложение 1.3. *Пусть $П$ – перестановочная матрица, преобразующая код C в код C'. Если H_C — проверочная матрица кода C, то $H_{C'} = H_C П^{-1}$ – проверочная матрица кода C'.*

Теорема 1.3. *Матрицы H и H' являются проверочными матрицами эквивалентных линейных (n,k)-кодов C и C' соответственно тогда и только тогда, когда существуют невырожденная квадратная матрица A порядка $m = n - k$ и перестановочная матрица $П$ такие, что* $\mathrm{H}' = \mathrm{A} \cdot \mathrm{H} \cdot \mathrm{П}$.

Доказательство следует из теоремы 1.2 и предложения 1.3.

Пример 1.6. Для кода Хэмминга используют различные задания. Одни из наиболее известных является лексикографическое — когда $i-$й столбец проверочной матрицы есть двоичная запись числа i. Значит, лексикографически заданный $(7,4)$-код Хэмминга имеет проверочную матрицу

$$\mathrm{H}_{лекс} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Общепринятым является интерпретация столбцов проверочной матрицы как элементов поля $GF(2^m)$, являющихся векторами из P_n в базисе $1, \alpha, \alpha^2, \ldots, \alpha^n$ для примитивного элемента α поля $GF(2^m)$. Если в качестве α взять корень неприводимого полинома $x^3 + x + 1$, то матрица

$$\tilde{H} = \left[1, \alpha, \alpha^2, ..., \alpha^{2^m - 2}\right] = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

есть матрица линейного $(7,4)$ - кода. Непосредственными вычислениями можно убедиться, что $A \cdot H_{лекс} \cdot B = H$ и $C \cdot \tilde{H} \cdot D = H$ для $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$; $C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$; H - проверочной матрицы из примера 1.3 кода Хэмминга и перестановочных матриц порядка 7

$$B = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Таким образом, H, $\tilde{H}$ и $H_{лекс}$ являются проверочными матрицами различных эквивалентных друг другу $(7,4)$- кодов Хэмминга.

1.4. Систематические коды

Определение 1.5. *Линейный (n,k) – код называется систематическим, если он задается проверочной матрицей вида $H = (H' \mid E)$, где E — единичная $m \times m$ - матрица для $m = n - k$.*

Пример 1.7. Сопоставляя определение 1.5 и матрицу H из примера 1.5, убеждаемся, что ранее рассмотренный в вышеназванном примере $(7,4)$ — код Хэмминга действительно является систематическим двоичным линейным кодом.

Теорема 1.4 (Критерий систематичности линейного кода). *Линейный $(n,\ k)$ - код C является систематическим тогда и только тогда, когда у любой его проверочной $m \times k$ - матрицы последние m столбцов образуют невырожденную подматрицу.*

Доказательство. Необходимость утверждения очевидна, так как единичная матрица не вырожденна.

Достаточность. Пусть $H=\left(K\middle|L\right)$, где L — квадратная $m\times m$ – подматрица, невырожденная по условию. Тогда для матрицы $A=L^{-1}$ матрица $\mathrm{H}'=\mathrm{AH}=\left(\mathrm{K}'|\mathrm{E}\right)$, где $\mathrm{K}'=\mathrm{A}\cdot\mathrm{K}$, является проверочной матрицей кода C согласно предложению 1.3. С другой стороны, из вида матрицы H' следует, что код C – систематический. Теорема доказана.

Из теоремы 1.4 с учетом теоремы 1.3 получаем

Следствие. Всякий линейный код эквивалентен систематическому.

Теорема 1.5. Матрица $H=(K\middle|E_m)$ порядка $m\times n$ для $m=n-k$ является проверочной матрицей систематического $(n,k)-$кода тогда и только тогда, когда $\left(k\times n\right)-$матрица $G=\left(E_k\middle|K^T\right)$ является порождающей матрицей этого кода.

Доказательство проводится непосредственным перемножением матриц G и H.

1.5. Метрика Хэмминга

Определение 1.6. *Метрикой или расстоянием на множестве X называется определённая на декартовом произведении $X\times X$ функция ρ с неотрицательными действительными значениями, удовлетворяющая при любых $x, y\in X$ условиям:*

1) $\rho\left(x,y\right)=0$ тогда и только тогда, когда $x=y$ (аксиома тождества);

2) $\rho\left(x,y\right)\le\rho\left(x,z\right)+\rho\left(y,z\right)$ (аксиома треугольника);

3) $\rho\left(x,y\right)=\rho\left(y,x\right)$ (аксиома симметрии).

Замечание. Часто в данное определение добавляют ещё аксиому неотрицательности. Но она является следствиями перечисленных аксиом. Действительно, при $x=y=z$ аксиома треугольника приобретает вид: $\rho\left(x,x\right)\le\rho\left(x,x\right)+\rho\left(x,x\right)$, что в силу отсутствия делителей нуля в поле вещественных чисел означает неравенство $\rho\left(x,x\right)\ge 0$. Далее, полагая $x=y$ в неравенстве треугольника, получаем неравенство $\rho\left(x,z\right)\ge 0$.

Мы привыкли к евклидовой метрике в пространстве $\mathbb{R}^n$, задаваемой формулой $\rho\left(x,y\right)=\sqrt{\sum_{i=1}^{n}\left(x_i-y_i\right)^2}$. Но на этом пространстве возможны и

другие метрики, например, задаваемые формулами: $\sigma(x, y) = \sum_{i=1}^{n} |x_i - y_i|$ или $\mu(x, y) = \max_{1 \le i \le n} |x_i - y_i|$.

Хэмминг весьма удачно предложил свою метрику на векторных пространствах с координатами в полях Галуа. В дальнейшем в этом параграфе будем предполагать, что $P = GF(q)$ — конечное поле из q элементов, P_n – векторное n – мерное пространство над полем P, содержащее линейный (n, k)–код C.

Определение 1.7. *Расстоянием Хэмминга между векторами* $\overline{x}, \overline{y} \in P_n$ *называется количество* $\mathrm{dist}(\overline{x}, \overline{y})$ *несовпадающих координат этих векторов.*

Весом $w(\overline{x})$ *вектора* $\overline{x} \in P_n$ *называется количество ненулевых координат этого вектора.*

Несложно видеть, что расстояние Хэмминга между векторами $\overline{x}, \overline{y} \in P_n$ равно весу вектора $\overline{x} - \overline{y}$. Очевидно, $wt(\overline{x} + \overline{y}) \le wt(\overline{x}) + wt(\overline{y})$.

Лемма 1.1. *Расстояние Хэмминга обладает всеми свойствами обычного расстояния (из определения 1.6):*

1) $dist(\overline{x}, \overline{y}) = 0$ *тогда и только тогда, когда* $\overline{x} = \overline{y}$*;*

2) $dist(\overline{x}, \overline{z}) + dist(\overline{z}, \overline{y}) \ge dist(\overline{x}, \overline{y})$ *– неравенство треугольника;*

3) $dist(\overline{y}, \overline{x}) = dist(\overline{x}, \overline{y})$ *– свойство симметричности.*

Доказательство. Первое и третье свойства непосредственно следуют из отмеченного выше соотношения: $\mathrm{dist}(\overline{x}, \overline{y}) = wt(\overline{x} - \overline{y}) = wt(\overline{y} - \overline{x})$. Аналогично

$$\mathrm{dist}(\overline{x}, \overline{z}) + \mathrm{dist}(\overline{z}, \overline{y}) =$$

$$= wt(\overline{x} - \overline{z}) + wt(\overline{z} - \overline{y}) \ge wt\big((\overline{x} - \overline{z}) + (\overline{z} - \overline{y})\big) =$$

$$= wt(\overline{x} - \overline{y}) = \mathrm{dist}(\overline{x}, \overline{y}).$$

Таким образом, доказано и второе свойство расстояния.

Определение 1.8. t *– окрестностью вектора* $\overline{x} \in P_n$ *назовём совокупность всех векторов* $\overline{y} \in P_n$*, для которых* $dist(\overline{x}, \overline{y}) \le t$.

t – окрестности обладают обычным свойством отделимости.

Лемма 1.2. *Если* $\mathrm{dist}(\overline{x}, \overline{z}) > 2t$*, то* t *– окрестности векторов* $\overline{x}, \overline{z} \in P_n$ *не пересекаются.*

Доказательство методом от противного. Предположим, что в пространстве P_n найдутся векторы $\bar{x}, \bar{z}$ на расстоянии $\mathrm{dist}(\bar{x}, \bar{z}) \geq 2t+1$ друг от друга и с вектором $\bar{y} \in P_n$, одновременно принадлежащим обеим $t-$окрестностям векторов $\bar{x}, \bar{z} \in P_n$. Тогда по аксиоме треугольника $\mathrm{dist}(\bar{x}, \bar{z}) \leq \mathrm{dist}(\bar{x}, \bar{y}) + \mathrm{dist}(\bar{y}, \bar{z}) \leq t + t = 2t < 2t+1$, что противоречит условию: $\mathrm{dist}(\bar{x}, \bar{z}) \geq 2t+1$. Следовательно, предположение о пересекаемости окрестностей невозможно и лемма доказана.

1.6. Минимальное расстояние кода

Определение 1.9. *Минимальным или кодовым расстоянием кода C называется наименьшее из расстояний между попарно различными векторами кода C.*

Из равенства $\mathrm{dist}(\bar{x}, \bar{y}) = wt(\bar{x} - \bar{y})$ следует, что минимальное расстояние линейного кода равно наименьшему из весов ненулевых векторов этого кода.

Значение кодового расстояния определяет следующая — фундаментальная в помехоустойчивом кодировании

Теорема 1.6. *Если минимальное расстояние кода C равно $d = 2t+1$ или $d = 2t+2$, то код C может обнаружить до $d-1$ ошибок и исправить до t ошибок в каждом принятом векторе-слове длиной n.*

Доказательство. Возможность обнаружения до $d-1$ ошибок. Если к кодовому слову $\bar{c} \in C$ прибавить любой вектор $\bar{e} \in P_n$, у которого менее d ненулевых координат, то полученный вектор $\bar{x} = \bar{c} + \bar{e}$ не принадлежит, очевидно, подпространству C (в противном случае $\bar{x} - \bar{c} = \bar{e} \in C$, что противоречит минимальности d). Как мы уже знаем, принадлежность и не принадлежность данного вектора коду C определяется результатом умножения на проверочную матрицу H_C этого кода. Результат $\bar{x} \cdot H_C^T \neq \bar{0}$ означает, что принятое сообщение $\bar{x} \notin C$ и, следовательно, в отличие от переданного слова $\bar{c}$, содержит ошибки.

О возможности декодирования до t ошибок. Если к кодовому слову $\bar{c} \in C$ прибавить любой вектор $\bar{e} \in P_n$, у которого $\tau \leq t$ ненулевых координат, то полученный вектор $\bar{x} = \bar{c} + \bar{e}$ находится на расстоянии τ от вектора $\bar{c} \in C$. Если $\bar{c}_i$ – другой вектор подпространства C, то в силу леммы 1.2 $dist(\bar{x}, \bar{c}_i) > t$. Предположение о противоположном неравенстве приводит к противоречию: если предположить, что найдётся вектор

$\overline{c}_j \in C$, для которого $dist(\overline{x}, \overline{c}_j) \le t$, то в силу неравенства треугольника $d \le \mathrm{dist}\left(\overline{c}, \overline{c}_j\right) \le \mathrm{dist}\left(\overline{c}, \overline{x}\right) + \mathrm{dist}\left(\overline{x}, \overline{c}_j\right) \le 2t < d$.

Таким образом, существует единственный вектор $\overline{c} \in C$, находящийся на расстоянии $\rho \le t$ от принятого вектора-сообщения $\overline{x}$. Этот однозначно определённый вектор $\overline{c}$ естественно взять в качестве правильного, не искажённого переданного сообщения. Теорема полностью доказана.

Замечание 1. Если вектор ошибок $\overline{e}$ содержит $\tau \ge d$ ненулевых координат, то он может оказаться кодовым словом, то есть принадлежать подпространству C. Тогда в силу замкнутости C относительно операции сложения вектор $\overline{x} = \overline{c} + \overline{e} \in C$. В таком случае мы не сможем заметить ошибки в принятом сообщении $\overline{x} = \overline{c} + \overline{e}$.

Замечание 2. Предложенный в доказательстве теоремы метод декодирования носит название «декодирования в ближайшее кодовое слово» или «декодирование по максимуму правдоподобия» (см. [6], стр. 26).

При достаточно общем определении 1.1 далеко не каждое $k-$мерное подпространство линейного пространства P_n относят к реальным линейным кодам. На практике применяются коды с попарно удалёнными друг от друга кодовыми словами в смысле метрики Хемминга — с достаточно большим кодовым расстоянием d. Ведь согласно фундаментальной в помехоустойчивом кодировании теореме 1.6 только такие коды могут исправлять возникающие в процессе передачи информации ошибки. Со схемотехнической точки зрения полезны в практическом применении и иные свойства линейных кодов — систематичность, цикличность, реверсивность и так далее. Все эти свойства определяются соответствующими свойствами проверочной матрицы H.

Следующая теорема служит критерием для определения минимального расстояния кода.

Теорема 1.7. *Пусть H — проверочная матрица двоичного кода C. Минимальное расстояние этого кода равно d тогда и только тогда, когда любые $d-1$ столбцов матрицы H линейно независимы, но найдутся d линейно зависимых столбцов.*

Доказательство теоремы вытекает из следующей леммы.

Лемма 1.3. *Пусть $[i] - i-$й столбец проверочной матрицы H линейного кода C над полем P. Вектор $\overline{c} \in P_n$ весом ϖ с ненулевыми координатами на позициях $i_1, i_2, ..., i_\varpi$ принадлежит коду C тогда и только тогда, когда система столбцов $[i_1], [i_2], ..., [i_\varpi]$ линейно зависима.*

Доказательство.

По условию $\overline{c} = \left(0,\ldots,0,c_{i_1},0,\ldots,0,c_{i_2},0,\ldots,0,c_{i_\varpi},0,\ldots,0\right)$ с единственными ненулевыми координатами $c_{i_j} \in P$, $1 \le j \le \varpi$. Вектор $\overline{c}$ принадлежит коду C тогда и только тогда, когда $H \cdot \overline{c}^T = \overline{0}$. По свойствам матричного умножения $H \cdot \overline{c}^T = c_{i_1}[i_1] + c_{i_2}[i_2] + \ldots + c_{i_\varpi}[i_\varpi]$. Равенство $c_{i_1}\left[i_1\right] + c_{i_2}\left[i_2\right] + \ldots + c_{i_\varpi}\left[i_\varpi\right] = \overline{0} = \left[0\right]$ означает линейную зависимость столбцов $[i_1],[i_2],...,[i_\varpi]$. Лемма полностью доказана.

1.7. Коды Хэмминга

Определение 1.10. *Кодом Хемминга называется линейный код* C_χ *с проверочной матрицей* $H_\chi = \left(1,\alpha,\ldots,\alpha^{2m-2}\right)$. *Здесь* α^i *- двоичный вектор-столбец над полем* $GF(2)$ *в базисе* $1,\alpha,\ldots,\alpha^{m-1}$ *для примитивного элемента* α *поля* $GF\left(2^m\right)$.

Из определения следует, что столбцами матрицы H_χ являются все возможные ненулевые векторы двоичного пространства P_n. Поэтому произвольный код Хэмминга имеет параметры $n = 2^m - 1$, $k = n - m$: $(7, 4); (15, 11); (31, 26); (63, 57); (127, 120); (255, 247); (511, 502); (1023, 1013)$ и так далее.

Теорема 1.8. *У кода Хэмминга минимальное расстояние* $d = 3$.

Доказательство. Из задания проверочной матрицы $H_\chi = \left(1,\alpha,\ldots,\alpha^{2m-2}\right)$ непосредственно видно, что в ней любые два столбца попарно различны и, следовательно, линейно независимы. Однако в этой матрице обязательно найдется тройка линейно зависимых столбцов, например, столбцы $1, \alpha, \alpha + 1$.

Следствие. *Код Хэмминга исправляет одиночные ошибки.*

Следует отметить, что коды Хемминга — это исторически первый и удачный класс линейных помехоустойчивых кодов, нашедших приложения и в теории и на практике.

Отметим, что все коды, эквивалентные коду C_χ, также называются кодами Хэмминга. Все они имеют то же кодовое расстояние и так же исправляют одиночные ошибки.

Почти одновременно с кодами Хемминга был открыт код C_{ASC} на основе ASCII-формата, также исправляющий одиночные ошибки. Это двоичный $\left(64, 49\right)$ – код. Его кодовые слова лучше представлять в виде дво-

ичных квадратных матриц порядка 8. В этих матрицах координаты c_{ij}, $1 \le i, j \le 7$, являются информационными, а остальные — проверочными. Восьмой элемент каждой строки – проверочный. Как и в ASCII-формате, $c_{i8} = 1$ или $c_{i8} = 0$, причём выбирается такое значение, чтобы сумма всех элементов $i-$й строки равнялась нулю. Аналогичным рассуждением со столбцами определяются элементы c_{8j} восьмой строки матрицы с тем, чтобы сумма единиц в каждом столбце была чётной. 64-й разряд каждого кодового слова – элемент c_{88} — проверяет на чётность суммарное количество единиц в проверочных разрядах строк.

Если при передаче кодового слова произошла одиночная ошибка в информационном поле, то нарушение чётности в конкретных проверочных разрядах строк и столбцов однозначно укажет на ошибочную позицию. Если же возникает нарушение чётности в 64-ом разряде, то этот факт можно проигнорировать, поскольку ошибка произошла в каком-то из проверочных разрядов и не затронула информационные разряды.

Сравнивая данный код с кодом Хемминга, можно утверждать, что код Хемминга — лучше, поскольку при примерно равных длинах (63 и 64) имеет почти на порядок меньше проверочных разрядов (6 и 15 соответственно).

Тем не менее код C_{ASC} послужил прообразом целого направления в помехоустойчивом кодировании — разработки так называемых кодов-произведений, кодов-перемежений, каскадных кодов.

1.8. Декодирование по таблицам смежных классов

Пусть $C-$линейный $(n, k)-$код над конечным полем $P = GF(q)$ из q элементов. Векторное пространство P_n состоит из q^n элементов, а его подпространство $C-$из $\tau = q^k$ векторов. Для каждого $\overline{a} \in P_n$, $\overline{a} \notin C$, множество $\overline{a} + C = \left\{ \overline{a} + \overline{c}_i \middle| \overline{c}_i \in C \right\}$ в теории групп называется смежным классом аддитивной группы P_n по подгруппе C. Видимый приоритет вектора $\overline{a}$ в смежном классе иллюзорен — этот вектор можно заменить любым другим вектором этого же смежного класса ввиду легко проверяемого равенства: $\overline{b} + C = \overline{a} + C$ для каждого вектора $\overline{b} \in \overline{a} + C$ и наоборот.

Как аддитивная группа, P_n распадается в объединение $s = q^{n-k}$ непересекающихся смежных классов по своей подгруппе C, также содержащих

по q^k векторов: $P_n = \left(\overline{0} + C\right) \cup \left(\overline{a}_1 + C\right) \cup \ldots \cup \left(\overline{a}_{s-1} + C\right)$ для подходящих векторов $\overline{a}_i \in P_n$, $1 \le i \le s-1$.

Если в результате передачи неизвестного на приёмном конце кодового слова $\overline{c} \in C$ получен вектор $\overline{y} \ne \overline{c}$, то все возможные значения вектора ошибок $\overline{e} = \overline{y} - \overline{c}$ лежат в одном смежном классе с вектором $\overline{y}$. Наиболее вероятным вектором ошибок из них является, очевидно, тот вектор смежного класса, который в этом классе имеет наименьший вес. Определив такой вектор $\overline{e}$, мы декодируем $\overline{y}$, заменяя его кодовым словом $\overline{c} = \overline{y} - \overline{e}$.

Определение 1.11. *Лидером смежного класса* $U = \overline{a}_i + C$ *называется вектор* $\overline{e}_i$ *наименьшего веса в этом смежном классе.*

В силу отмеченных свойств смежных классов $U = \overline{a}_i + C = \overline{e}_i + C$. Предложенный выше метод коррекции ошибок кодом C называется *методом декодирования по лидерам смежных классов.* Реализуется он выписыванием таблицы смежных классов:

$\overline{0}$	$\overline{c}_1$	...	$\overline{c}_{\tau-1}$	- строка кодовых слов
$\overline{e}_1$	$\overline{e}_1 + \overline{c}_1$	...	$\overline{e}_1 + \overline{c}_{\tau-1}$	- остальные
...	...	...	...	смежные
$\overline{e}_{s-1}$	$\overline{e}_{s-1} + \overline{c}_1$	...	$\overline{e}_{s-1} + \overline{c}_{\tau-1}$	классы

Первый столбец этой таблицы состоит из лидеров смежных классов. Если $\overline{y} = \overline{e}_i + \overline{c}_j$ — элемент $i-$ой строки и $j-$ого столбца выписанной таблицы смежных классов, то лидер этой строки $\overline{e}_i$ есть вектор-ошибка в принятом сообщении $\overline{y}$, а истинное передаваемое сообщение есть вектор $\overline{c}_j$ – первый элемент $j-$ого столбца.

Пример 1.8. Рассмотрим линейный $(6,3)-$код C с порождающей матрицей $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} = \left(E_3 \middle| K^T\right)$ над полем Галуа из двух элементов. Легко видеть, что определитель матрицы $K^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ не равен нулю. Поэтому, согласно теореме 1.4 данный код является систематическим, а по теореме 1.5 его проверочная матрица

$H = \left(K \middle| E_3\right) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$. Так же легко видно, что любые два столбца матрицы H образуют линейно независимую систему. Тогда в силу теоремы 1.7 минимальное расстояние кода есть величина $d = 3$. Следовательно, этот код способен корректировать одиночные ошибки. Ясно, что $\left|P_6\right| = 2^6 = 64$, а $\left|C\right| = 8$. Код C, как известно, составляют нулевой вектор, векторы-строки матрицы G, суммы этих строк по две – векторы (110101), (101001), (011100), а также сумма всех трёх сток – вектор (111010). Выпишем таблицу смежных классов с лидерами векторного пространства P_6 над полем $P = GF(2)$ по коду C:

000000	100110	010011	110101	001111	101001	011100	111010
100000	000110	110011	010101	101111	001001	111100	011010
010000	110110	000011	001100	011111	111001	100101	101010
001000	101110	011011	010100	000111	100001	111101	110010
000100	100010	010111	011000	001011	101101	110001	111110
000010	100100	010001	011110	001101	111011	110110	111000
000001	100111	010010	011101	001110	101000	110100	111011
000101	100011	010110	011001	001010	101100	110000	111111

Первая строка этой таблицы — строка всех кодовых слов из кода C, а первый столбец состоит из лидеров строк — смежных классов. Если принято слово 110011, которое находится во второй строке и третьем столбце таблицы, то истинным передаваемым сообщением следует считать кодовое слово 010011; Если принято слово 100101, которое находится в третьей строке и седьмом столбце таблицы, то истинным передаваемым сообщением следует считать кодовое слово 110101.

Данный метод позволяет в рассмотренном примере корректировать все одиночные ошибки и даже одну двойную ошибку — лидера восьмого смежного класса.

1.9. Весовой спектр кода

Метод декодирования по таблицам смежных классов хорош и удобен, но применим лишь для кодов с не очень большими по размерам таблицами этих классов. Во многих важных для практики случаях такой метод не приемлем, не всегда известен или практически не обозрим список кодовых слов. В таких случаях ценную информацию о коде может дать ве-

совой спектр кода — таблица или гистограмма значений веса кодовых слов.

В любом коде в точности один вектор – нулевой – имеет вес 0, определённое количество кодовых слов имеют минимальный вес d. Весовые значения остальных кодовых слов находятся в диапазоне от $d+1$ до n. Однако распределение весов в этом диапазоне имеет определённые закономерности и достаточно причудливую специфику.

Лемма 1.4. *В любом двоичном линейном коде C либо все кодовые слова имеют чётный вес, либо ровно половина кодовых слов имеет чётный вес, а половина – нечётный вес.*

Доказательство. Любой двоичный линейный код C является группой относительно операции сложения. Нетрудно видеть, что кодовые слова чётного веса образуют подгруппу D в группе C. Если в коде C имеются и кодовые слова нечётного веса, то они образуют отдельный смежный класс по подгруппе D. Мощность смежного класса совпадает с мощностью подгруппы D. Поскольку любое кодовое слово либо принадлежит D, либо указанному смежному классу, то тем самым лемма полностью доказана.

Без труда строится таблица весов кода C из предыдущего параграфа. Наглядной иллюстрацией к доказанному утверждению является

Пример 1.9. Код Хэмминга над полем $GF\left(2^{11}\right)$ имеет параметры $\left(n,k,d\right)=\left(2047,2036,3\right)$. Следовательно, проверочная матрица этого кода есть $\left(11\times 2047\right)-$матрица $H_{\chi}=\left(1,\alpha,\alpha^{2},\ldots,\alpha^{2046}\right)$ для примитивного элемента α поля $GF\left(2^{11}\right)$ — корня неприводимого и примитивного полинома 11-ой степени над полем из двух элементов, например, полинома $x^{11}+x^{2}+1-$одного из 176 двоичных примитивных полиномов 11-ой степени. Отметим, что длина этого кода $n=2047=23\cdot 89-$составная. Пусть $\beta=\alpha^{89}$. Выделим в матрице H_{χ} подматрицу $H_{\Gamma}=\left(1,\beta,\beta^{2},\ldots,\beta^{22}\right)$. Это $\left(11\times 23\right)-$матрица. Векторы ядра матрицы H_{Γ} образуют линейный $\left(23,12\right)-$код Γ. На рис. 1 представлена диаграмма весов кода Γ, данные для которой получены компьютерными расчётами – решением системы линейных уравнений $H_{\Gamma}\cdot\overline{x}^{T}=\overline{0}$ и анализом весов полученных векторов-решений.

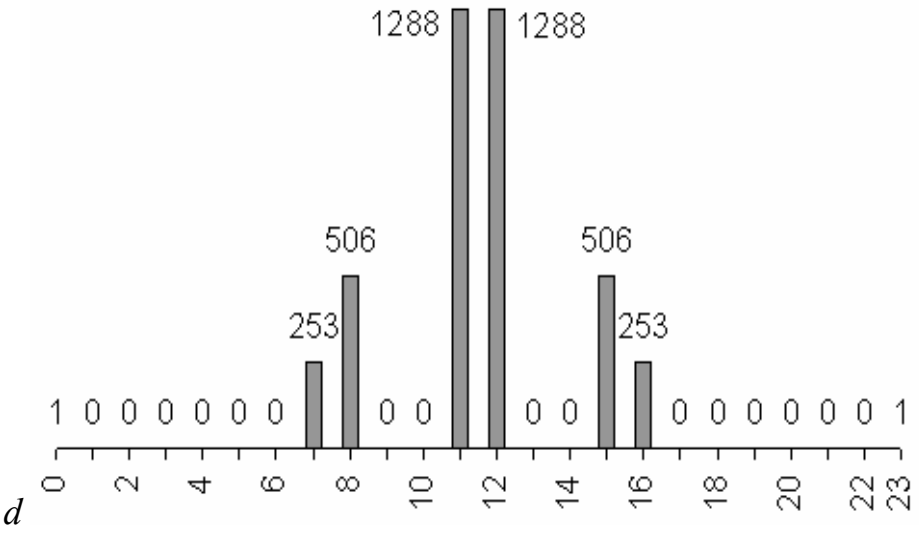

Рис. 1. Диаграмма весов кодовых слов $(23,12)-$*кода* Γ.

Из приведенной на рис.1 диаграммы видим, что полностью подтверждается вторая часть альтернативы доказанной леммы 1.4. Также видим, что минимальное расстояние данного кода равно 7. Следовательно, код Γ способен корректировать векторы-ошибки весом 1 – 3.

Оказалось, что найденный спектр весов полностью совпадает с весовым спектром $(23,12,7)-$кода Голея — знаменитого своими уникальными свойствами кода, тщательного изученного в [2]. Иных кодов с такими параметрами не существует. Об этом свидетельствуют многочисленные аналитические и компьютерные исследования, проведенные в различных уголках земного шара. Поэтому можно с уверенностью утверждать, что линейный код с проверочной матрицей $H_{\Gamma}=\left(1,\beta,\beta^2,...,\beta^{22}\right)$ есть код Голея, во всяком случае, эквивалентен коду Голея.

Подобная выше рассмотренной процедура получения нового кода называется укорочением. Как видим, она позволяет в отдельных случаях добиться существенного увеличения кодового расстояния, несмотря на уменьшение длины и размерности кода.

1.10. Синдромы ошибок

Одним из важнейших понятий теории помехоустойчивых кодов является синдром ошибок. В процессе передачи информации на кодовое слово $\overline{c}$ может наложиться «шум» — вектор-ошибок $\overline{e}$. В результате приемное устройство получает слово $\overline{y}=\overline{c}+\overline{e}$.

Определении 1.12. *Синдромом ошибок принятого слова* $\overline{y}$ *в коде* C *с проверочной матрицей* H *называется вектор* $S=H\cdot\overline{y}^T$.

Если $S=\overline{0}$, то $\overline{y}-$кодовое слово. Следовательно, условие $S\neq\overline{0}$ служит признаком наличия ошибочных символов в принятом слове $\overline{y}$. В силу ассоциативности операций сложения и умножения матриц синдром $S=\mathrm{H}\cdot\overline{y}^T=\mathrm{H}\cdot\left(\overline{c}^T+\overline{e}^T\right)=\mathrm{H}\cdot\overline{c}^T+\mathrm{H}\cdot\overline{e}^T=\mathrm{H}\cdot\overline{e}^T$. Это означает, что S зависит только от вектора ошибок $\overline{e}$ и не зависит от кодовых слов.

Предложение 1.4. *Пусть* H *и* H_1 *проверочные матрицы кода* C. *Пусть* $\overline{e}_1$ *и* $\overline{e}_2$ *- различные векторы-ошибки, синдромы которых относительно матрицы* H *совпадают (различны). Тогда и относительно матрицы* H_1 *их синдромы также совпадают (различны).*

Доказательство. Пусть по условию $H\cdot\overline{e}_1^T=H\cdot\overline{e}_2^T=S$. Докажем, что $H_1\cdot\overline{e}_1^T=H_2\cdot\overline{e}_2^T$. Согласно теореме 1.2, $H_1=A\cdot H$ для подходящей невырожденной матрицы A порядка m. Тогда синдромы векторов ошибок $\overline{e}_1$ и $\overline{e}_2$ относительно матрицы H_1 соответственно равны $H_1\cdot\overline{e}_1^T=A\cdot H\cdot\overline{e}_1^T=A\cdot S$; $H_1\left(\overline{e}_2^T\right)=A\cdot H\left(\overline{e}_2^T\right)=A\cdot S$. Названные синдромы совпадают. Предложение доказано.

Пусть H — фиксированная проверочная матрица данного линейного $(n,k)-$кода L над полем P. Пусть $E_n=P_n-$пространство всех векторов размерности n над полем P — пространство возможных ошибок кода L, содержащее L в качестве своего подпространства.

Предложение 1.5. *Если* $\overline{e}$ *пробегает все векторы пространства* E_n, *то* S *пробегает все векторы пространства* E_{n-k}.

Доказательство. Отображение φ_H, ставящее каждому вектору $\overline{e}\in E_n$ в соответствие его синдром $S=S\left(\overline{e}\right)$, есть линейный оператор из пространства E_n в пространство E_{n-k}. Образ пространства E_n при этом отображении (множество всех синдромов) есть подпространство в E_{n-k} размерности $n-\dim KerH=n-k$ и, следовательно, совпадает с E_{n-k}. Таким образом вектор S может быть любым вектором. Предложение доказано.

Следствие. *Пусть* C *– линейный* $\left(n,k\right)-$ *код над конечным полем из* q *элементов. Тогда каждое значение синдрома* $S=S\left(\overline{e}\right)$ *принимают в точности* q^k *различных векторов-ошибок, а именно, векторы* $\overline{a}+\overline{e}$ *для всех* $\overline{a}\in C$ *и только они.*

Доказательство. Пусть S — синдром вектора-ошибки $\overline{e}$ в коде C. Тогда для каждого вектора $\overline{a}\in C$ в силу линейности оператора

$\varphi_H : \overline{e} \to S(\overline{e})$ синдром $S(\overline{a}+\overline{e}) = S(\overline{a}) + S(\overline{e}) = \overline{0} + S(\overline{e}) = S(\overline{e})$. Следовательно, не менее q^k векторов-ошибок имеет синдром $\overline{e}$.

С другой стороны, если для векторов-ошибок $\overline{f}$ и $\overline{e}$ $S(\overline{f}) = S(\overline{e})$, то $S(\overline{f}-\overline{e}) = 0$. Следовательно, $\overline{f}-\overline{e} = \overline{a} \in C$. Таким образом, $\overline{f} = \overline{a}+\overline{e}$, что и требовалось доказать.

Пусть d – минимальное расстояние кода C. Пусть $t = [d/2]$, если d нечетно, и $t = (d/2)-1$, если d четно. Пусть $K_{od\ldots t}$ – множество всех векторов весом $1, 2, \ldots, t$ в пространстве E_n.

Предложение 1.6. *Если* $\overline{x} \neq \overline{e}$ *для* $\overline{e} \in K_{od\ldots t}$, *но* $S(\overline{e}) = S(\overline{x})$, *то* $w(\overline{x}) \geq d$. *Следовательно, для произвольных* $\overline{e}_1, \overline{e}_2 \in K_{od\ldots t}$, $\overline{e}_1 \neq \overline{e}_2$, *их синдромы попарно различны:* $S(\overline{e}_1) \neq S(\overline{e}_2)$.

Доказательство. Пусть $\overline{e} \in K_{od\ldots t}$, а $\overline{x}$ — произвольный вектор ошибок, но $S(\overline{e}) = S(\overline{x})$. Тогда $S(\overline{x}-\overline{e}) = \overline{0}$. Это означает, что вектор $\overline{y} = \overline{x}-\overline{e} \in C$. Согласно свойству расстояния Хэмминга

$$w(\overline{x}) = w(\overline{y}+\overline{e}) \geq w(\overline{y}) - w(\overline{e}) \geq w(\overline{y}) \geq d.$$

Предложение 1.6 вместе с очевидной уверенностью, что наиболее вероятны ошибки малого веса, создают теоретическую базу для синдромных методов коррекции ошибок, по значениям синдромов ошибок определяющих соответствующие векторы ошибок из множества $K_{od\ldots t}$.

Выше мы рассмотрели два метода коррекции ошибок — метод максимального правдоподобия и табличный. Основные преимущества синдромных методов в следующем:

1) согласно предложению 1.6 синдромы однозначно соответствуют ошибкам декодируемого многообразия;
2) синдромы имеют существенно меньшие размеры по сравнению с кодовыми словами и векторами ошибок (что особенно наглядно для высокоскоростных кодов, например, для кодов Хемминга);
3) для нахождения синдромов не требуется специальных вычислений, кроме обусловленных необходимостью индикации наличия или отсутствия ошибок в принятом блоке-сообщении;
4) синдром совершенно не связан с передаваемой информацией, а исключительно только с произошедшей ошибкой.

Синдромное декодирование кодов Хэмминга.

Пусть $H=\left(1,\alpha,\ldots,\alpha^{2m-2}\right)$ — проверочная матрица кода Хэмминга. Как установлено выше, код Хэмминга имеет минимальное расстояние 3 и может декодировать только одиночные ошибки. Пусть $\overline{e}_i$ — двоичный вектор-ошибка весом 1 с единственной ненулевой i–й координатой. Ясно, что $S\left(\overline{e}_i\right)=H\cdot\overline{e}_i^T=\alpha^{i-1}$ – i–й столбец матрицы H, однозначно указывающий на ошибочную координату — единственную ненулевую координату вектора $\overline{e}_i$.

Определение 1.13. *Код называется совершенным, если множество его синдромов совпадает по мощности с множеством декодируемых ошибок.*

Название объясняется тем, что у совершенных кодов синдромная информация об ошибках на 100% используется для их коррекции.

Большинство кодов, конечно же, совершенными не являются. Но примеры таких кодов есть.

Очевидно, код Хэмминга относится к разряду совершенных кодов. Другим примером совершенного кода является код Голея. Как установлено выше, он корректирует все ошибки весом 1–3, их общее количество равно $C_{23}^1+C_{23}^2+C_{23}^3=23+23\cdot11+23\cdot11\cdot7=23\cdot89=2047=2^{11}-1$, что совпадает с общим количеством ненулевых синдромов ошибок в коде Голея.

2. Введение в теорию линейных кодовых последовательностей

Equation Chapter 2 Section 1

2.1. Линейные кодовые последовательности сдвигового регистра

Рассмотрим бесконечную последовательность $\boldsymbol{v}=\left(v_0,v_1,v_2,\ldots\right)$, заданную по рекурсии системой разностных уравнений

$$v_{k+n}=a_0v_k+a_1v_{k+1}+\ldots+a_{n-1}v_{k+n-1},\qquad k=0,1,\ldots \tag{2.1}$$

Алфавит, которому принадлежат элементы v_k и a_k, удобно отождествлять с некоторым конечным полем $GF\left(q\right)$ характеристики p. Начало рекурсии задается конечной последовательностью длины n

$$v_0=\tilde{v}_0,v_1=\tilde{v}_1,\ldots,v_{n-1}=\tilde{v}_{n-1}. \tag{2.2}$$

Таким образом строится разностный код [3], который отображает последовательность начальных данных длины n $\boldsymbol{v} = (\tilde{v}_0, \tilde{v}_1, \ldots, \tilde{v}_{n-1})$ в бесконечную рекуррентную последовательность $\boldsymbol{v}$. Физическая реализация процесса построения последовательности $\boldsymbol{v}$ осуществляется с помощью $n-$ уровнего регистра сдвига на триггерах [3, 12, 18]. Блоковая диаграмма данного процесса имеет следующий вид

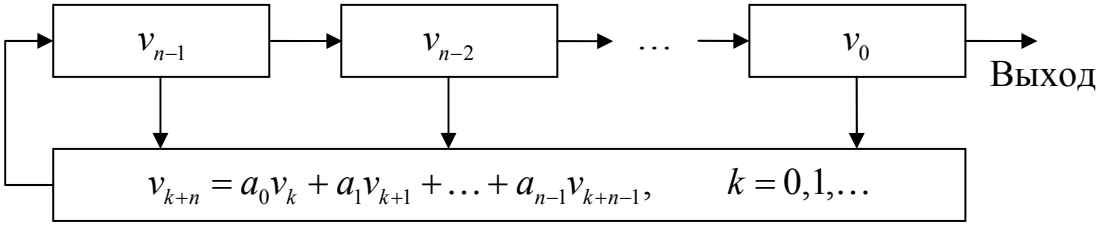

Рис. 2. Блок-схема n-уровнего регистра сдвига с обратной связью.

Последовательность длины n $(v_k, v_{k+1}, \ldots, v_{k+n-1})$ называется состоянием регистра сдвига в данный момент k, $k = 0,1,\ldots$.

Пример 2.1. В поле $GF(2)$ рассмотрим систему уравнений

$$v_{k+3} = v_{k+2} + v_k, \qquad k = 0,1,\ldots$$

Начальному состоянию $\tilde{\boldsymbol{v}} = (1,0,0)$ регистра сдвига соответствует последовательность

$$\boldsymbol{v} = (1,0,0,1,1,1,0,\ldots). \tag{2.3}$$

При этом состояния менялись, как указано на следующей диаграмме

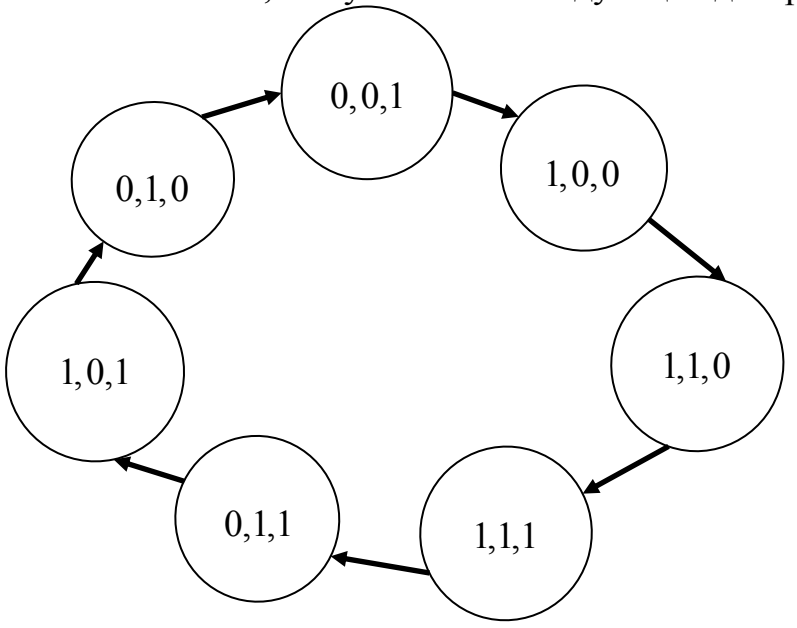

Рис. 3. Блок-схема смены состояний регистра сдвига из примера 2.1.

Циклическая смена состояний объясняет периодический характер кодовой последовательности (2.3).

Определение 2.1. *Последовательность* $\mathbf{v} = (v_0, v_1, \ldots)$, $v_k \in GF(q)$, *называется финально периодической с параметрами* (T, τ), *если выполняется условие*

$$v_{k+T} = v_k, \qquad k \geq \tau, \tag{2.4}$$

где числа T *и* τ *целые,* $T > 0$, $\tau \geq 0$. *Наименьшее число* T, *удовлетворяющее (2.4) называется периодом последовательности. Последовательность* $\mathbf{v}$ *называется* T*–периодической, если* $\tau = 0$. *В таком случае последовательность будем записывать в виде* $\mathbf{v} = (v_0, v_1, \ldots, v_{T-1})$.

Последовательность из примера 2.1 является периодической с периодом $T = 7$.

Заметим, что линейный n–уровневый регистр сдвига с обратной связью (Linear feedback shift register или сокращенно LFSR) имеет q^n различных состояний. Это позволяет доказать следующую теорему.

Теорема 2.1. *Пусть* $\mathbf{v}$ *— последовательность, полученная с помощью LFSR т.е. LFSR последовательность. Тогда ее период* T *удовлетворяет оценке*

$$T \leq q^n - 1. \tag{2.5}$$

Определение 2.2. *LFSR последовательность* $\mathbf{v}$ *называется последовательностью максимальной длины (либо* M *–последовательностью), если ее период* $T = q^n - 1$. *В частности, для* $q = 2$ *период* $T = 2^n - 1$.

Последовательность в примере 2.1 является M–последовательностью.

2.2. Минимальные полиномы и периоды кодовых последовательностей

Можно дать другое, эквивалентное определение LFSR последовательностей в терминах некоторых полиномиальных колец. Пусть $P[x]$ — кольцо полиномов с коэффициентами из поля $P = GF(q)$, $S(P)$ — векторное пространство всех бесконечных последовательностей над полем P с покоординатными операциями сложения и умножения на скаляры поля.

Определение 2.3. *Пусть последовательность* $\mathbf{v} \in S(P)$ *удовлетворяет системе уравнений (2.1). Тогда полином*

$$f(x) = x^n - a_{n-1}x^{n-1} - \ldots - a_0 \tag{2.6}$$

называется характеристическим полиномом последовательности $\mathbf{v}$ *над полем* P.

Принято полагать $f(x)=1$ для нулевой последовательности.

С другой стороны, любой нормированный полином (т.е. с коэффициентом при x^n равным 1) $f(x)\in P[x]$ задает систему уравнений вида (2.1), множество решений которой $S_{f(x)}$ является подпространством $S(P)$.

Теорема 2.2. *Пусть* $f(x)\in P[x]$ *— нормированный полином. Тогда* $S_{f(x)}$ *является линейным пространством размерности* n.

Пример 2.2. Полином $f(x)=x^5+x^3+1$ над полем $P=GF(2)$ является характеристическим следующей последовательности периода 31

$$\mathbf{v}=(1,0,0,0,0,1,0,1,0,1,1,1,0,1,1,0,0,0,1,1,1,1,1,0,0,1,1,0,1,0,0).$$

Легко проверить, что $\mathbf{v}$ является решением системы уравнений

$$v_{k+5}=v_{k+3}+v_k, \qquad k=0,1,\ldots$$

с начальным состоянием $\tilde{\mathbf{v}}=(1,0,0,0,0)$. Всего в пространстве $S_{f(x)}$ имеется $2^5=32$ различных последовательностей.

Следует отметить, что для любой периодической кодовой последовательности существует множество полиномов, задающих данную последовательность. Интерес представляет характеристический полином наименьшей степени.

Определение 2.4. *Нормированный полином* $m(x)$ *наименьшей степени, для которого последовательность* $\mathbf{v}\in S_{m(x)}$ *называется минимальным полиномом последовательности* $\mathbf{v}$ *над полем* P.

Согласно данного определения, минимальный полином последовательности определяет линейный регистр сдвига с обратной связью наименьшей длины, который задает данную последовательность. Следовательно, степень минимального полинома является очень важной характеристикой последовательности, которая называется линейной сложностью (либо linear span) последовательности. Другой, эквивалентной (как показал С. Голомб [13]) характеристикой минимального многочлена является его период. Будем использовать стандартное обозначение $f(x)\,|\,g(x)$ — полином $f(x)$ делит полином $g(x)$.

Определение 2.5. *Периодом полинома* $f(x)$ *над полем* P *называется наименьшее положительное число* $T(f)$ *такое, что*

$$f(x) \mid \left(x^{T(f)} - 1\right). \tag{2.7}$$

Теорема 2.3. *Пусть* $\mathbf{v}$ *является LFSR последовательностью с минимальным полиномом* $m(x)$ *степени* n*, неприводимым над полем* $P = GF(q)$*. Пусть* α *— корень* $m(x)$ *в расширении поля* $GF(q^n)$*. Тогда период последовательности* $\mathbf{v}$*, период минимального многочлена* $m(x)$ *и степень элемента* α *совпадают.*

Установленная в 1955 году, данная теорема послужила мощным стимулом дальнейшего развития теории периодических кодовых последовательностей. Практический интерес представляет возможность разбиения множества $S_{f(x)}$ на эквивалентные классы.

Определение 2.6. *Две периодические последовательности* $\mathbf{v}$ *и* $\mathbf{w}$ *называются циклически эквивалентными (*$\mathbf{v} \sim \mathbf{w}$*), если существует целое* $l \geq 0$*, такое что*

$$v_k = w_{k+l}, \qquad k = 0,1,\ldots \tag{2.8}$$

В противном случае они называются циклически различными.

Теорема 2.4. *Если* $f(x)$ *неприводимый полином над полем* $P = GF(q)$ *степени* n*, то число классов циклически эквивалентных ненулевых последовательностей в* $S_{f(x)}$ *равно*

$$\sigma_n = \frac{q^n - 1}{T(f)}. \tag{2.9}$$

Перефразируя данную теорему на язык диаграмм состояний, можно сделать вывод, что на данной диаграмме имеется σ_n циклов длины $T(f)$ и один цикл длины 1.

2.3. Представление линейных кодовых последовательностей с помощью матриц, функции следа и с помощью формальных степенных рядов

Анализируя работы линейного n-уровневого регистра сдвига с обратной связью, можно отметить, что на каждом шаге k состояние регистра $(v_k, v_{k+1}, \ldots, v_{k+n-1})$ переходит в $(v_{k+1}, v_{k+2}, \ldots, v_{k+n})$. Это отображение может быть задано с помощью матрицы

$$\Omega = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix} \tag{2.10}$$

в силу равенства (2.1). Тогда получаем соотношение

$$\left(v_{k+1}, v_{k+2}, \ldots, v_{k+n}\right) = \left(v_0, v_1, \ldots, v_{n-1}\right)\Omega^{k+1}. \tag{2.11}$$

Равенство (2.11) называется матричным представлением последовательности $\boldsymbol{v}$. По теореме Кэлли–Гамильтона $f(\Omega) = 0$ и если $f(x) \mid \left(x^t - 1\right)$, то $\Omega^t = \mathrm{E}$, где E — единичная матрица. Кроме того $f(x) = \det\left|x\mathrm{E} - \Omega\right|$.

Для аналитического описания и исследования свойств периодических последовательностей удобно использовать функцию следа.

Определение 2.7. *Пусть* $a \in GF\left(q^m\right)$. *Следом* $Tr_{q^m/q}(a)$ *элемента* a *над* $GF(q)$ *называется элемент, определенный равенством*

$$Tr_{q^m/q}(a) = a + a^q + a^{q^2} + \ldots + a^{q^{m-1}}. \tag{2.12}$$

Если q — простое число, то $Tr_{q^m/q}(a)$ называется абсолютным следом элемента и обозначается $Tr_m(a)$.

Функция следа обладает следующими свойствами [14]:

Tr1. $Tr_{q^n/q}(a+b) = Tr_{q^n/q}(a) + Tr_{q^n/q}(b)$, $\forall a, b \in GF\left(q^n\right)$;

Tr2. $Tr_{q^n/q}(\lambda a) = \lambda Tr_{q^n/q}(a)$, $\forall \lambda \in GF(q)$ и $a \in GF\left(q^n\right)$;

Tr3. След $Tr_{q^n/q}$ является линейным отображением векторного пространства $GF\left(q^n\right)$ над полем $GF(q)$ в $GF(q)$;

Tr4. $Tr_{q^n/q}(a) = n \cdot a$, $\forall a \in GF\left(q^n\right)$;

Tr5. $Tr_{q^n/q}\left(a^q\right) = Tr_{q^n/q}(a)$, $\forall a \in GF\left(q^n\right)$.

Имеет место

Теореме 2.5. *Равенство* $Tr_{q^n/q}(a) = 0$ *выполняется тогда и только тогда, когда существует элемент* $b \in GF\left(q^n\right)$ *такой, что* $a = b^q - b$.

Теореме 2.6. *Пусть* α *— корень неприводимого полинома* $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *над полем* $GF(q)$. *Последовательность*

$\boldsymbol{v} \in S_{f(x)}$ тогда и только тогда, когда существует элемент $\beta \in GF\left(q^n\right)$ такой, что выполняется равенство

$$v_k = Tr_n\left(\beta\alpha^k\right), \qquad k = 0,1,\ldots. \tag{2.13}$$

Формула (2.13) называется след-представителем последовательности $\boldsymbol{v}$ с неприводимым характеристическим полиномом.

Пример 2.3. Пусть $f\left(x\right) = x^4 + x^3 + x^2 + x + 1$ и α — корень данного полинома в $GF\left(2^4\right)$. Тогда след-представление последовательности $\boldsymbol{v} = \left(1,0,0,0,1\right) \in S_{f(x)}$ имеет вид

$$v_k = Tr_4\left(\beta\alpha^k\right), \qquad k = 0,1,\ldots, \tag{2.14}$$

где $\beta = 1 + \alpha.$

Для каждой периодической последовательности $\boldsymbol{v} = \left(v_0, v_1, \ldots, v_{T(f)-1}\right) \in S_{f(x)}$, где $f\left(x\right) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ — характеристический полином последовательности $\boldsymbol{v}$, можно записать формальный степенной ряд

$$\boldsymbol{v}\left(x\right) = \sum_{k=0}^{\infty} v_k x^k. \tag{2.15}$$

Обозначим через $g\left(x\right) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + 1$, $a_0 \neq 0$, так называемый обратный к $f\left(x\right)$ полином. Переходя в равенстве (2.1) к записи рекурсии с помощью формальных степенных рядов и анализируя полученное равенство, приходим еще к одному представлению периодических кодовых последовательностей

$$S_{f(x)} = \left\{ \frac{a\left(x\right)}{g\left(x\right)}, \text{ где } a\left(x\right) \in P\left[x\right] \text{ и } \deg a\left(x\right) < n \right\} \tag{2.16}$$

Пример 2.4. Полагая $f\left(x\right) = x^4 + x + 1$ и $a\left(x\right) = x^3 + 1$ над полем $GF\left(2\right)$. Тогда $g\left(x\right) = x^4 + x^3 + 1$ и

$$\frac{a\left(x\right)}{g\left(x\right)} = 1 + x^4 + x^7 + x^8 + x^{10} + x^{13} + x^{14} + \ldots.$$

Таким образом, получаем последовательность $\boldsymbol{v} = \left(1,0,0,0,1,0,0,1,1,0,1,01,1,1\right)$ периода 15.

2.4. Случайные последовательности и их характеристические свойства

Во многих ситуациях, возникающих в электронике, работе компьютеров, криптографии и многочисленных других областях появляется необходимость использования случайных последовательностей. В данном контексте случайность выражается в непредсказуемости последовательности. Более точно, требуются последовательности, которые бы выглядели как случайные, но при более тщательном анализе можно было бы заметить определенную регулярность. Первоначально С. Голомб [12] выделил три характеристических свойства для двоичных последовательностей над полем $GF(2)$, характеризующих их случайность. Это сбалансированность, определенное соотношение для числа идущих подряд 1 и 0 и свойство автокорреляции. Затем эти свойства были обобщены на случай последовательностей над полем $GF(q)$. Всестороннее изучение M –последовательностей привело к открытию ряда новых свойств, которые продолжили аксиоматику случайных последовательностей.

Рассмотрим некоторые основные свойства случайных двоичных последовательностей.

Условие 2.1. На каждом периоде длины T последовательности $\boldsymbol{v} \in S(P)$, где поле $P = GF(2)$ справедливо неравенство

$$\left| \sum_{k=0}^{T-1} (-1)^{v_k} \right| \le 1. \qquad (2.17)$$

Данное условие означает, что несовпадение числа 1 и 0 в последовательности $\boldsymbol{v}$ на каждом периоде не превышает 1. Это условие часто называют условием сбалансированности.

Определение 2.8. *Если в последовательности* $\boldsymbol{v}$ *имеется фрагмент вида* $1\underbrace{00\ldots0}_{k}1$ *(либо* $0\underbrace{11\ldots1}_{k}0$*), то фрагмент* $\underbrace{0\ldots0}_{k}$ *(либо* $\underbrace{1\ldots1}_{k}$*) называют дорожкой (из нулей либо единиц) длины* k.

Условие 2.2. На каждом периоде длины T последовательности $\boldsymbol{v} \in S(P)$, где поле $P = GF(2)$, половина всех дорожек имеет длину 1, одна четвертая — длину 2, одна восьмая — длину 3 и так далее. Этот процесс продолжается, пока число дорожек на k-том шаге больше 1. Кроме того, общее число дорожек из нулей равно общему числу дорожек из единиц.

Определение 2.9. *Автокорреляционная функция* T*-периодической последовательности* $\boldsymbol{v} \in S(P)$*, где поле* $P = GF(2)$*, определяется следующим образом*

$$C_{\boldsymbol{v}}(\tau)=\sum_{k=0}^{T-1}(-1)^{v_k+v_{k+\tau}},\qquad \tau\in\mathbb{Z}. \tag{2.18}$$

Отметим основные свойства функции $C_{\boldsymbol{v}}(\tau)$:

С1. $C_{\boldsymbol{v}}(0)=T$, $\left|C_{\boldsymbol{v}}(\tau)\right|\le T$, $\tau\in\mathbb{Z}$.

С2. $C_{\boldsymbol{v}}(\tau)=C_{\boldsymbol{v}}(\tau+T)$, $\tau\in\mathbb{Z}$.

С3. $C_{\boldsymbol{v}}(\tau)=C_{\sigma(\boldsymbol{v})}(\tau)$, $\tau\in\mathbb{Z}$, $\sigma(v)=(v_{T-1},v_0,v_1,\ldots,v_{T-2})$ — циклический сдвиг.

С4. $C_{\boldsymbol{v}}(\tau)=C_{\boldsymbol{v}}(T-\tau)$, $1<\tau\le\left[\frac{T}{2}\right]$, где $[\cdot]$ — целая часть числа.

Особый интерес представляют кодовые последовательности, обладающие идеальными корреляционными свойствами (M-последовательности, последовательности Фрэнка и др. [15]).

Условие 2.3. Автокорреляционная функция $C_v(\tau)$ является двухуровневой, если она имеет вид

$$C_v(\tau)=\begin{cases}T, & \tau=0,\\ C_0=const, & 1\le\tau<T.\end{cases} \tag{2.19}$$

В частности, при $C_0=-1$ для T нечетного и $C_0=0$ для T четного говорят, что последовательность $\boldsymbol{v}$ имеет идеальную автокорреляционную функцию.

Пример 2.3. Последовательность $\boldsymbol{v}=(0,0,0,1,0,0,1,1,0,1,0,1,1,1,1)$ с минимальным полиномом $m(x)=x^4+x+1$ удовлетворяет всем условиям (2.1)–(2.3). Для нее автокорреляционная функция имеет вид: $R_v(0)=8$, $R_v(\tau)=4$, $1\le\tau\le14$.

Условие 2.4. На каждом периоде длины T последовательности $\boldsymbol{v}\in S(P)$ любая ненулевая подпоследовательность $\boldsymbol{\chi}=(\chi_0,\chi_1,\ldots,\chi_{n-1})$ длины n встречается точно один раз. Число n для такой последовательности называется ее линейной сложностью.

Заметим, что любая M-последовательность удовлетворяет этому условию.

2.5. Классификация двоичных последовательностей периода 2^n-1

Рассмотрим классификацию двоичных [12] последовательностей периода $T=2^n-1$.

Пусть U — множество всех двоичных последовательностей периода T, которые содержат 2^{n-1} единиц и $2^{n-1}-1$ нулей в каждом периоде, т.е. U состоит из всех двоичных последовательностей, удовлетворяющих условию (2.1). Пусть множество $PN \subset U$ состоит из всех M-последовательностей периода T. Далее рассмотрим несколько промежуточных множеств между PN и U:

Множество $R \subset U$ состоит из всех двоичных последовательностей, удовлетворяющих условию (2.2).

Множество $C \subset U$ состоит из всех двоичных последовательностей, удовлетворяющих (2.3).

Множество $S \subset U$ состоит из всех двоичных последовательностей, удовлетворяющих (2.4).

Множество $M \subset U$ состоит из всех двоичных последовательностей, имеющих 2 множителем, т.е. для некоторого циклического сдвига $v' = \left(v'_0 v'_1 \ldots v'_{T-1}\right)$ последовательности $\boldsymbol{v} = \left(v_0 v_1 \ldots v_{T-1}\right)$ выполняется соотношение

$$v'_{2i} = v_i, \qquad i \geq 0. \tag{2.20}$$

Мощность каждого из введенных множеств выражают формулы

$$|U| = \binom{2^n - 1}{2^{n-1}} \Big/ \left(2^n - 1\right), \quad |PN| = \phi\left(2^n - 1\right)/n, \qquad |S| = 2^{2^{n-1}-n},$$

где ϕ — функция Эйлера.

Для n простого имеет место равенство

$$|M| = \binom{2\tau}{\tau}, \text{ где } \quad \tau = \frac{2^{n-1}-1}{n}.$$

Гипотеза 2.1. (S. Golomb, 1980)

$$S \bigcap C = PN. \tag{2.21}$$

Другими словами, если двоичная последовательность удовлетворяет одновременно условиям (2.3) и (2.4), то это M-последовательность.

2.6. Дискретное преобразование Фурье кодовых последовательностей

Обработка кодовых последовательностей основывается на применении дискретного преобразования Фурье в поле Галуа. Данное преобразование играет важную роль в практических задачах кодирования и других инженерных дисциплинах, так как оно устанавливает связь между временным и частотным представлением сигнала. Дискретное преобразование Фурье имеет многочисленные приложения в спектральном и корре-

ляционном анализе, синтезе фильтров, устройств обнаружения или оценки параметров сигналов. Основываясь на преобразовании Фурье, построена спектральная теория кодирования.

Определение 2.10. *Пусть задана T-периодическая последовательность $\boldsymbol{v}=(v_0,v_1,\ldots,v_{T-1})$ над полем $GF(q)$, где T делит q^n-1 при некоторым n, и пусть α — элемент порядка T в поле $GF(q^n)$. Дискретным преобразованием Фурье последовательности $\boldsymbol{v}$ называется последовательность $\boldsymbol{V}=(V_0,V_1,\ldots,V_{T-1})$, задаваемая следующим образом*

$$V_l=\sum_{k=0}^{T-1}\alpha^{kl}v_k, \qquad l=0,1,\ldots,T-1. \tag{2.22}$$

Дискретный индекс k естественно назвать временем, а $\boldsymbol{v}$ — временной функцией или сигналом. Аналогично другой индекс l можно назвать частотой, а $\boldsymbol{V}$ — частотной функцией или спектром.

Заметим, что число T может быть произвольным делителем числа q^n-1, но наиболее важную роль играют периоды вида $T=q^n-1$. В этом случае элемент α является примитивным элементом поля $GF(q^n)$.

Теорема 2.7. *Над полем $GF(q)$ характеристики p последовательность $\boldsymbol{v}$ и ее спектр $\boldsymbol{V}$ связаны соотношением*

$$v_k=\frac{1}{T}\sum_{l=0}^{T-1}\alpha^{-kl}V_l, \qquad k=0,1,\ldots,T-1, \tag{2.23}$$

где число T, стоящее перед единицей, рассматривается как элемент поля (т.е. по модулю p).

Доказательство данной теоремы использует следующее свойство:

$$\sum_{k=0}^{T-1}\alpha^{kl}=\begin{cases}0, & \text{если } l\neq 0\pmod T,\\ T, & \text{если } l\equiv 0\pmod T.\end{cases} \tag{2.24}$$

Пример 2.4. Пусть α — корень примитивного полинома $f(x)=x^3+x+1$ над полем $GF(2)$. Рассмотрим двоичную последовательность $\boldsymbol{v}=(1,1,0,0,0,1,0)$ периода 7. Вычисляя ее дискретное преобразование Фурье по формуле (2.22)

$$V_l=1+\alpha^l+\alpha^{5l}, \qquad l=0,1,\ldots,6,$$

получаем $\boldsymbol{V}=(1,\alpha^2,\alpha^2+\alpha,0,\alpha,0,0)$. Применяя обратное преобразование Фурье (2.23)

$$v_k=1+\alpha^{2-k}+\alpha^{2-2k}+\alpha^{1-2k}+\alpha^{1-4k}, \qquad k=0,1,\ldots,6,$$

убеждаемся, что спектру $\boldsymbol{V}$ соответствует исходная последовательность $\boldsymbol{v}$.

Заметим, что дискретное преобразование Фурье осуществляет взаимно-однозначное соответствие между последовательностями и их спектрами.

Для описания многих важных свойств дискретного преобразования Фурье и получения формулы для обратного преобразования Фурье весьма полезным является введение на множестве $\mathbb{Z}_T = \{0,1,\ldots,T-1\}$ с операциями сложения и умножения по модулю T специального отношения эквивалентности, которое разбивает это множество на циклотомические классы.

Определение 2.10. *Пусть T — натуральное число, являющееся делителем числа $q^n - 1$ для некоторого натурального n. Циклотомическим классом C_s по модулю T над $GF(q)$ для $s \in \{0,1,\ldots,T-1\}$ называется множество*

$$C_s = \left\{s, sq, sq^2, \ldots, sq^{l_s-1}\right\},$$

где l_s — наименьшее натуральное такое, что $sq^{l_s} \equiv s \pmod{T}$.

Заметим, если числа s и T взаимно просты, то $l_s = l$, где l — наименьшее натуральное такое, что $q^l \equiv 1 \pmod{T}$. Это число l называется показателем, которому q принадлежит по модулю T.

Имеется место следующая [13]

Теорема 2.8. *Числа q, T, n и l_s из определения 2.10 удовлетворяют условиям:*

i). $l_s = |C_s|$.

ii). l_s равно степени минимального полинома элемента α^s над полем $GF(q)$, где α — элемент порядка T в $GF(q^n)$.

iii). l_s делит n.

В качестве индекса s циклотомического класса C_s удобно выбирать наименьшее число из данного класса, называемое лидером. Множество всех лидеров циклотомических классов по модулю T обозначим через $L(T)$. Множество $\mathbb{Z}_T$ разбивается на непересекающееся циклотомические классы, т.е.

$$\mathbb{Z}_T = \coprod_{s \in L(T)} C_s. \qquad (2.25)$$

Пример 2.4. Полагаем $q=2$ и $T=2^7-1=127$. Тогда имеет место разбиение

$$\Omega_{127}=C_0\cup C_1\cup C_3\cup C_5\cup C_7\cup C_9\cup C_{11}\cup C_{13}\cup C_{15}\cup C_{19}\cup C_{21}\cup C_{23}\cup$$
$$\cup C_{27}\cup C_{29}\cup C_{31}\cup C_{43}\cup C_{47}\cup C_{55}\cup C_{63},$$

где

$C_0=\{0\}$

$C_1=\{1,2,4,8,16,32,64\}$

$C_3=\{3,6,12,24,48,96,65\}$

$C_5=\{5,10,20,40,80,33,66\}$

$C_7=\{7,14,28,56,112,97,67\}$

$C_9=\{9,18,36,72,17,34,68\}$

$C_{11}=\{11,22,44,88,49,98,69\}$

$C_{13}=\{13,26,52,104,81,35,70\}$

$C_{15}=\{15,30,60,120,113,99,71\}$

$C_{19}=\{19,38,76,25,50,100,73\}$

$C_{21}=\{21,42,84,41,82,37,74\}$

$C_{23}=\{23,46,92,57,114,101,75\}$

$C_{27}=\{27,54,108,89,51,102,77\}$

$C_{29}=\{29,58,116,105,83,39,78\}$

$C_{31}=\{31,62,124,121,115,103,79\}$

$C_{43}=\{43,86,45,90,53,106,85\}$

$C_{47}=\{47,94,61,122,117,107,87\}$

$C_{55}=\{55,110,93,59,118,109,91\}$

$C_{63}=\{63,126,125,123,119,111,95\}$

Теорема 2.9. *Формула обратного представления последовательности* $\mathbf{v}$ *по ее спектру* $\mathbf{V}$ *имеет вид*

$$v_k=-\sum_{s\in L(T)}Tr_{q^{n_s}/q}\left(V_s\alpha^{-sk}\right),\qquad k=0,1,\ldots,T-1, \tag{2.26}$$

где $V_s\in GF\left(q^{n_s}\right)$, $n_s=|C_s|$, $\alpha^{-sk}\in GF\left(q^{n_s}\right)$.

При $q=2$ формула (2.26) принимает вид

$$v_k=\sum_{s\in L(T)}Tr_{n_s}\left(V_s\alpha^{-sk}\right),\qquad k=0,1,\ldots,T-1,\qquad V_s\in GF\left(2^{n_s}\right).$$

Следует особо отметить, что число ненулевых членов спектральной последовательности $\boldsymbol{V}$ равно линейной сложности (условие 2.4) T-периодической последовательности $\boldsymbol{v}$ над $GF(q)$, где T делит q^n-1. Для практического вычисления дискретного преобразования Фурье разработаны, так называемые "быстрые" алгоритмы вычисления, использующие след-представление последовательности $\boldsymbol{V}$. Кроме того, важный для приложений класс последовательностей максимальной длины обладает свойствами циклотомической инвариантности [16].

Теорема 2.10. *Пусть* $\alpha \in GF(q^n)$ *— произвольный примитивный элемент поля и* $\boldsymbol{v}$ *— T-периодическая M-последовательность, т.е.*

$$v_k = Tr(\alpha^k), \qquad k = 0,1,\ldots,T-1, \quad T = q^n - 1, \tag{2.27}$$

и $\boldsymbol{V}$ *— ее дискретное преобразование Фурье. Тогда значение* v_k *и* V_k *для индексов* k*, принадлежащих одному циклотомическому классу* C_S *по модулю* T*, постоянны.*

Пример 2.6. Пусть $q=2$ и $T=127$, $\alpha \in GF(2^7)$ — корень примитивного многочлена $f(x)=x^7+x+1$. Тогда сжатие последовательности (2.27) на циклотомические классы из примера 2.4 имеет вид

$$\boldsymbol{v}_{C_S} = (1,0,0,0,1,1,0,1,1,1,1,1,0,1,0,0,0,0,1),$$

а сжатие ее дискретного преобразования Фурье

$$V_{C_S} = (0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0).$$

Следовательно, линейная сложность 127-периодической последовательности $\boldsymbol{v}$ равна мощности ненулевых циклотомических классов C_S, т.е. 7.

Литература

1. Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. – 732 с.

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

3. Биркгоф Г., Барти Т. Современная прикладная алгебра. — М.: Мир, 1976. — 400 с.

4. Блейхут Р. Теория и практика кодов, контролирующих ошибки. — М.: Мир, 1986. – 576 с.

5. Питерсон У., Уэндон Э. Коды, исправляющие ошибки. — М.: Мир, 1976. – 574 с.

6. Кассами Т., Токура Н., Ивадари Ё., Инагаки Я. Теория кодирования. — М.: Мир, 1978. – 576 с.

7. Самсонов Б.Б., Плохов Е.М., Филоненков А.И., Кречет Т.В. Теория информации и кодирование. — Ростов-на-Дону: Феникс, 2002. – 288 с. (Серия «Учебники и учебные пособия»).

8. Конопелько В.К., Липницкий В.А. и др. Прикладная теория кодирования. Т. 1 – 2. – Учебное пособие для ВУЗов. — Мн.: БГУИР, 2004. – 688 с.

9. Вернер М. Основы кодирования. — Учебник для ВУЗов. – М.: Техносфера, 2006. – 288 с.

10. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – Учебное пособие для ВУЗов. – М.: Техносфера, 2006. – 320 с.

11. Артин Э. Геометрическая алгебра. — М.: Наука, 1969. – 284 с.

12. Golomb, S.: Shift Register Sequences. Holden-Day Inc., San Francisco (1967); revised edition Aegean Park Press, Laguna Hills, CA (1982).

13. Golomb, S., Gong, G.: Signal Design for Good Correlation — for Wireless Communication, Cryptography, and Radar. Cambridge University Press, Cambridge (2005).

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

15. Дворников В.Д., Конопелько В.К., Липницкий В.А. Теория и практика низкоскоростных кодов. Монография — Мн.: БГУИР, 2002. – 210 с.

16. Липницкий В.А., Чесалин Н.В. Дискретное преобразование Фурье M-последовательностей в полях Галуа. — Тезисы докладов — Мн.: Межд. науч. конф. “X Белорусская математическая конференция”, 2008. — с. 50

17. A. Robert Calderbank: The Art of Signaling: Fifty Years of Coding Theory. IEEE Transactions on Information Theory 44(6): 2561-2595 (1998).

18. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические и компьютерные основы криптологии. Учеб. пособие. — Мн.: Новое знание, 2003. — 382 с.

Содержание

Учебное издание

Липницкий Валерий Антонович
Чесалин Николай Владимирович

ЛИНЕЙНЫЕ КОДЫ И КОДОВЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ

Учебно-методическое пособие для студентов механико-математического факультета БГУ

В авторской редакции

Ответственный за выпуск *Н. В. Чесалин*

Подписано в печать 30.12.2008. Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Усл. печ. л.2,44. Уч.-изд. л.1,95. Тираж 50 экз. Зак.

Белорусский государственный университет.
Лицензия на осуществление издательской деятельности
№ 02330/0056804 от 02.03.2004.
220050, Минск, проспект Независимости, 4.

Отпечатано с оригинала-макета заказчика
на копировально-множительной технике
механико-математического факультета
Белорусского государственного университета.
220050, Минск, проспект Независимости, 4.