

Часть II

Коды, исправляющие ошибки

Разделы I

- 1** **Блочное кодирование. Коды Хэмминга**
- 2** **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3** **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4** **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5** **Задачи с решениями**

Задача помехоустойчивого кодирования: подходы к решению

По каналу с шумом проходит поток **битовой** информации.

- Модель потока: случайный некоррелированный.
- Модель шума: некоторые биты **случайно и независимо** могут оказаться инвертированными (*двоичный симметричный канал*, нет добавлений/стираний битов).
- Задача: обеспечить автоматическое исправление ошибок.

Задача помехоустойчивого кодирования: подходы к решению

По каналу с шумом проходит поток **битовой** информации.

- Модель потока: случайный некоррелированный.
- Модель шума: некоторые биты **случайно и независимо** могут оказаться инвертированными (**двоичный симметричный канал**, нет добавлений/стираний битов).
- Задача: обеспечить автоматическое исправление ошибок.

Подход к решению (один из возможных!):

- 1 входной поток информации разбить на **сообщения** — непересекающиеся блоки фиксированной длины k ;
- 2 каждый блок кодировать —
 - а) независимо от других — **блочное кодирование**;
 - б) в зависимости от предыдущих — **свёрточное кодирование** (турбо-коды и др.).

Задачи блочного кодирования

Далее рассматривается исключительно **блочное кодирование**:

- есть набор всех *сообщений* S_1, \dots, S_t , длины k каждое ($t = 2^k$), которые нужно передать по каналу связи с шумом;
- для обеспечения помехозащищённости вместо этих сообщений передают *кодовые слова* — блоки длины $n > k$ каждое.

Задачи блочного кодирования

Далее рассматривается исключительно **блочное кодирование**:

- есть набор всех *сообщений* S_1, \dots, S_t , длины k каждое ($t = 2^k$), которые нужно передать по каналу связи с шумом;
- для обеспечения помехозащищённости вместо этих сообщений передают *кодовые слова* — блоки длины $n > k$ каждое.

Задача (основная): построить код **минимальной длины n** , позволяющий восстановить сообщение, содержащее не более r ошибок.

Задачи блочного кодирования

Далее рассматривается исключительно **блочное кодирование**:

- есть набор всех **сообщений** S_1, \dots, S_t , длины k каждое ($t = 2^k$), которые нужно передать по каналу связи с шумом;
- для обеспечения помехозащищённости вместо этих сообщений передают **кодовые слова** — блоки длины $n > k$ каждое.

Задача (основная): построить код **минимальной длины** n , позволяющий восстановить сообщение, содержащее не более r ошибок.

Задача (вспомогательная): заданы

- n — длина кода (обычно зависит от параметра(ов)) — m, q, \dots ;
- r — максимальное количество исправимых ошибок.

Требуется построить код с **максимальным числом** t кодовых слов (= сообщений, которые можно передать).

Некоторые понятия, связанные с булевым кубом

Решаем **вспомогательную** задачу — она проще.

Напоминание из дискретной математики

- **Норма** $\|\tilde{\gamma}\|$ = число единичных координат в $\tilde{\gamma} \in B^n$.
- Метрика (вспоминаем, что это такое) на множестве бинарных наборов — **хэммингово расстояние** (\oplus — сумма по mod 2):

$$\rho(\tilde{\alpha}, \tilde{\beta}) = \|\tilde{\alpha} \oplus \tilde{\beta}\|.$$

- **Шар Хэмминга с центром в $\tilde{\alpha}$ и радиусом r** —

$$S_r(\tilde{\alpha}) = \left\{ \tilde{\beta} \in B^n \mid \rho(\tilde{\alpha}, \tilde{\beta}) \leq r \right\}.$$

Р.У. Хэмминг



Ричард Уэсли Хэмминг

(Richard Wesley Hamming, 1915–1998)

— американский математик, работы которого в сфере теории информации оказали существенное влияние на компьютерные науки и телекоммуникации.

В 1950 г. опубликовал способ построения кода, исправляющего одну ошибку и названный впоследствии его именем.

Институт инженеров по электротехнике и электронике (*IEEE, Institute of Electrical and Electronics Engineers*) учредил медаль, которой награждаются ученые, внесшие значительный вклад в теорию информации — *медаль Ричарда Хэмминга*.

Кодовое расстояние I

Определение

Минимальное расстояние между словами кода называется *кодowym расстоянием* (символически обычно d).

Утверждение

Множество C образует код с исправлением не менее r ошибок, если $S_r(\tilde{\alpha}) \cap S_r(\tilde{\beta}) = \emptyset$ для всех $\tilde{\alpha}, \tilde{\beta} \in C$ таких, что $\tilde{\alpha} \neq \tilde{\beta}$.

Доказательство

Если при передаче сообщения $\tilde{\alpha}$ сделано не более r ошибок, то набор останется в шаре $S_r(\tilde{\alpha})$.

Если шары не пересекаются, то искомое кодовое слово α — ближайшее к полученному набору.

Кодовое расстояние II

Следствие

У кода, исправляющего r ошибок, кодовое расстояние должно быть не менее $2r + 1$.

Определение кодового расстояния d произвольного кода — сложная задача.

Поэтому при помехоустойчивом кодировании на первый план выходит проблема построения кодов с заданным кодовым расстоянием.

Она решается при использовании, например, т.н. БЧХ-кодов, которые будут рассмотрены далее.

Блоковое кодирование и декодирование: определения и тривиальный пример

Блоковое кодирование — взаимно-однозначное преобразование сообщений длины k в кодовые слова длины $n > k$.

Декодирование — определение сообщения по кодовому слову.

Блочное кодирование и декодирование: определения и тривиальный пример

Блочное кодирование — взаимно-однозначное преобразование сообщений длины k в кодовые слова длины $n > k$.

Декодирование — определение сообщения по кодовому слову.

Пример (тривиальный код $k = 1, n = 3, d = 3$)

Информация разбивается на блоки длины $k = 1$, т.е. передаются $t = 2$ сообщения: $S_0 = 0$ и $S_1 = 1$.

Кодирование

$$0 \mapsto 000 \quad 1 \mapsto 111$$

исправляет одну ошибку!

Однако такое кодирование (выбор $k = 1$) крайне неэффективно: длина сообщения **утраивается**.

Блочное кодирование: обозначения и определения

Будем обозначать каждое сообщение вектором-столбцом (полужирный шрифт) $\mathbf{u} \in \{0, 1\}^k$:

$$\mathbf{u} = \begin{bmatrix} u_1 \\ \cdots \\ u_k \end{bmatrix} \quad u_1, \dots, u_k \text{ — информационные биты}$$

Определение

- \mathbf{v} — кодовое слово длины $n = k + m$, содержащее помимо k информационных ещё и m проверочных бит (разделимое блочное кодирование).
- Множество $\{\mathbf{v}_1, \dots, \mathbf{v}_{2^k}\}$ всех 2^k кодовых слов длины n — (n, k) -код (с кодовым расстоянием — (n, k, d) -код).
- $R = k/n$ — скорость, $m/n = 1 - R$ — избыточность кода.

Блочный (n, k) код: кодирование и ошибки передачи

Блочное кодирование не вызывает принципиальных трудностей: отображение $S \rightarrow C$ всегда может быть осуществлено с использованием таблицы размера $2^k \times n$. Однако такое «табличное» кодирование весьма неэффективно: n может достигать *десятков и сотен тысяч*.

Блочный (n, k) код: кодирование и ошибки передачи

Блочное кодирование не вызывает принципиальных трудностей: отображение $S \rightarrow C$ всегда может быть осуществлено с использованием таблицы размера $2^k \times n$. Однако такое «табличное» кодирование весьма неэффективно: n может достигать *десятков и сотен тысяч*.

При передаче по каналу с шумом кодовое слово v превращается в принятое слово w той же длины n :

$$v \rightarrow w = v + e.$$

Здесь $e \in \{0, 1\}^n$ — *вектор ошибок*:

$$e_i = \begin{cases} 1, & \text{если в } i\text{-ом бите произошла ошибка.} \\ 0, & \text{если ошибки нет.} \end{cases}$$

(n, k, d) -код может исправить не менее $\left\lfloor \frac{d-1}{2} \right\rfloor$ ошибок.

Блочный (n, k) код: декодирование

Декодирование кодов обычно **значительно сложнее** кодирования (известны т.н. «экспандерные» коды с линейным декодированием, для которых неизвестны субквадратичные алгоритмы кодирования, но это — исключение...).

Декодирование (n, k, d) -кода основано на:

- разбиении единичного куба B^n на k областей, содержащих шары радиуса $r = \lfloor (d - 1)/2 \rfloor$ с центрами в кодовых словах;
- предположении, что при передаче произошло не более r ошибок.

Блочный (n, k) код: два этапа декодирования

1-й этап: Восстановление переданного кодового слова \hat{w} как ближайшего к w в метрике Хэмминга — нахождение центра соответствующего шара. Для этого надо, вообще говоря, перебрать все 2^k строк в $2^k \times n$ -таблице кодовых слов.

Если расстояние до ближайшего центра шара (кодového слова) превышает величину $r = \lfloor (d - 1)/2 \rfloor$, то при передаче произошло больше ошибок, чем может исправить код и алгоритм декодирования должен выдать **отказ**.

2-й этап: Восстановление по \hat{w} исходного сообщения \hat{u} путём удаления проверочных бит. В общем случае это потребует использования таблицы размера $2^k \times k$.

Блочное кодирование: общая схема и сложность

$$\mathbf{u} \xrightarrow[\text{избыточность}]{\text{кодирование}} \mathbf{v} \xrightarrow[+e]{\text{ошибка}} \mathbf{w} \xrightarrow[\text{ближ. код. слово}]{\text{декод.-1}} \hat{\mathbf{v}} \xrightarrow[\text{удаление избыт.}]{\text{декод.-2}} \hat{\mathbf{u}}$$

Из приведённых оценок следует:

использование блочного (n, k) -кода **общего вида** возможно лишь при **небольших значениях** n и k .

Блочное кодирование: общая схема и сложность

$$\mathbf{u} \xrightarrow[\text{избыточность}]{\text{кодирование}} \mathbf{v} \xrightarrow[+e]{\text{ошибка}} \mathbf{w} \xrightarrow[\text{ближ. код. слово}]{\text{декод.-1}} \hat{\mathbf{v}} \xrightarrow[\text{удаление избыт.}]{\text{декод.-2}} \hat{\mathbf{u}}$$

Из приведённых оценок следует:

использование блочного (n, k) -кода **общего вида** возможно лишь при **небольших значениях** n и k .

Однако, приняв ряд дополнительных ограничений на множество кодовых слов, можно перейти от **экспоненциальных** (2^k) требований по памяти для хранения кода и по сложности алгоритмов кодирования/декодирования к **линейным** по n и k .

Эти ограничения приводят к использованию блочных кодов специального вида: **групповых**, а из групповых — **циклических**.

Плотная упаковка шаров в булев куб

Чтобы построить код максимального размера, исправляющий t ошибок, нужно вложить в единичный куб B^n максимально возможное число непересекающихся шаров радиуса r — *задача плотной упаковки*.

Вопрос: При каких n и r в куб B^n можно уложить непересекающиеся шары радиуса r «плотно», «без зазоров»?

Плотная упаковка шаров в булев куб

Чтобы построить код максимального размера, исправляющий t ошибок, нужно вложить в единичный куб B^n максимально возможное число непересекающихся шаров радиуса t — *задача плотной упаковки*.

Вопрос: При каких n и t в куб B^n можно уложить непересекающиеся шары радиуса t «плотно», «без зазоров»?

Ответ: Такое удаётся в случаях:

- 1 $n = 2^m - 1, t = 1$ — *коды Хэмминга* и
- 2 $n = 23, t = 3$ — *код Голея*
— это *совершенные* или *экстремальные коды*.

Количество кодовых слов

Теорема (Хэмминга)

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

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

Количество кодовых слов

Теорема (Хэмминга)

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

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

Доказательство

t есть максимальное число непересекающихся шаров радиуса r , помещающихся в кубе B^n .

Верхняя оценка (граница Хэмминга) — шар радиуса r содержит точки: сам центр + все точки с одной, двумя, ..., r измененными координатами, т.е. всего $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{r}$ штук и шары не пересекаются.

Продолжение доказательства

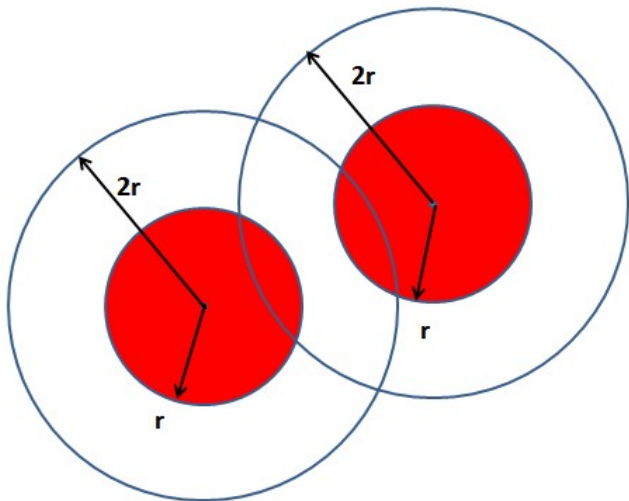
Для *оценки снизу* построим негрупповой код:

- 1 берем произвольную точку B^n и строим вокруг неё шар радиуса $2r$;
- 2 берем произвольную точку вне построенного шара и строим вокруг неё шар радиуса $2r$;
- 3 и т.д., каждая новая точка выбирается *вне* построенных шаров. В результате:
 - шары, возможно, пересекаются, но каждый шар занимает $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{2r}$ точек \Rightarrow шаров не менее 2^n

$$\frac{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{2r}}{2^n};$$

- шары радиуса r с центрами в выбранных точках не пересекаются.

Иллюстрация к теореме Хэмминга



Граница Варшавова–Гильберта

Замечание: оценка нижней границы количества t кодовых слов, исправляющих r ошибок в поле $GF(p^n)$ —

$$\frac{p^n}{\binom{n}{0}(p-1)^0 + \binom{n}{1}(p-1)^1 + \dots + \binom{n}{2r}(p-1)^{2r}} \leq t.$$

Граница Варшавова–Гильберта

Замечание: оценка нижней границы количества t кодовых слов, исправляющих r ошибок в поле $GF(p^n)$ —

$$\frac{p^n}{\binom{n}{0}(p-1)^0 + \binom{n}{1}(p-1)^1 + \dots + \binom{n}{2r}(p-1)^{2r}} \leq t.$$

Ром Рубенович Варшавов (1927–1999) — чл.-корр. АН АрмССР, основоположник алгебраической теории кодирования.



Эдгар Гильберт (Edgar Nelson Gilbert, 1923–2013) — американский математик, специалист в области теории кодирования.

Код Хэмминга $n = 2^m - 1, r = 1$: построение

Покажем, что в случае $n = 2^m - 1$ получим $t = \frac{2^n}{1+n}$, т.е. **верхняя оценка** в теореме Хэмминга **достигается**.

Построим код, а потом определим его кодовое расстояние.

Рассмотрим таблицу:

$$\begin{array}{l}
 k = 2^m - (m+1) \left\{ \begin{array}{ll}
 100 \dots 000 & 1100 \dots 000 \\
 010 \dots 000 & 1010 \dots 000 \\
 001 \dots 000 & 1001 \dots 000 \\
 \dots & \dots \\
 000 \dots 100 & 1111 \dots 101 \\
 000 \dots 010 & 1111 \dots 110 \\
 000 \dots 001 & 1111 \dots 111
 \end{array} \right. \\
 \underbrace{\hspace{10em}}_{k = 2^m - (m+1)} & \underbrace{\hspace{10em}}_m
 \end{array}$$

Слева — единичная матрица порядка $2^m - (m + 1)$, справа — все бинарные наборы длины m , содержащие **не менее двух** единиц.

Код Хэмминга $n = 2^m - 1$, $r = 1$: кодовое расстояние

Просуммируем всевозможные совокупности строк этой таблицы, получив всего $2^k = 2^{2^m - (m+1)}$ различных наборов-слов. Но

$$2^{2^m - (m+1)} = \frac{2^{2^m - 1}}{2^m} = \frac{2^n}{n+1} = \max t.$$

Код Хэмминга $n = 2^m - 1$, $r = 1$: кодовое расстояние

Просуммируем всевозможные совокупности строк этой таблицы, получив всего $2^k = 2^{2^m - (m+1)}$ различных наборов-слов. Но

$$2^{2^m - (m+1)} = \frac{2^{2^m - 1}}{2^m} = \frac{2^n}{n+1} = \max t.$$

Найдём кодовое расстояние построенного кода:

- в каждой строке таблицы — не менее 3 единиц;
- если сложить

две строки — в левой части будет 2 единицы, а в правой — хотя бы 1,

не менее трёх строк — в левой части будет не менее 3 единиц.

Т.е. всегда $\rho(\tilde{\alpha}, \tilde{\beta}) \geq 3 \Rightarrow$ шары единичного радиуса с центрами в полученных наборах не пересекаются.

Код Хэмминга длины 7

Пример ($m = 3$, $n = 2^3 - 1 = 7$, $k = 7 - 3 = 4$)

Для данного параметра $m = 3$ составим таблицу кода Хэмминга:

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

Складывая по $\text{mod } 2$ все совокупности приведённых 4 строк (включая пустую), получаем $2^4 = 16$ различных бинарных слов длины 7, которыми можно закодировать 16 сообщений. Эти кодовые слова располагаются в 0-м, 3-м, 4-м и 7-м слоях единичного куба B^7 .

Код Хэмминга длины 7

Пример ($m = 3$, $n = 2^3 - 1 = 7$, $k = 7 - 3 = 4$)

Для данного параметра $m = 3$ составим таблицу кода Хэмминга:

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

Складывая по mod 2 все совокупности приведённых 4 строк (включая пустую), получаем $2^4 = 16$ различных бинарных слов длины 7, которыми можно закодировать 16 сообщений. Эти кодовые слова располагаются в 0-м, 3-м, 4-м и 7-м слоях единичного куба B^7 .

Является ли кодом Хемминга тривиальный $(3, 1)$ -код?

Код Голя — (23, 12, 7)-код

В данном случае верхняя граница числа вложенных шаров радиуса 3 в 23-мерный единичный куб

$$t = \frac{2^{23}}{1 + 23 + \frac{23 \cdot 22}{1 \cdot 2} + \frac{23 \cdot 22 \cdot 21}{1 \cdot 2 \cdot 3}} = \frac{2^{23}}{2048} = \frac{2^{23}}{2^{11}} = 2^{12} = 4096$$

также достигается, т.е. имеем плотную упаковку, как и в кодах Хэмминга.

Других пар (n, r) , удовлетворяющих условию

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r}} \quad \text{— целое}$$

НЕИЗВЕСТНО.

М. Голей



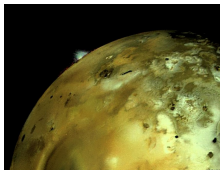
Марсель Голей

(Marcel J. E. Golay, 1902–1989)

— швейцарский математик и физик, работавший в США и занимавшийся проблемами газовой хроматографии и оптической спектроскопии.

В своей единственной работе по теории информации (1949) предложил совершенный двоичный код, исправляющий три ошибки.

В ходе космической программы *Вояджер* (1979-81) для передачи цветных изображений Юпитера и Сатурна использовался код Голея.



Граница Плоткина

Пусть $t(n, d)$ — максимально возможное количество кодовых слов среди всех двоичных кодов длины n с кодовым расстоянием d .

Граница Плоткина даёт верхний предел $t(n, d)$.

Теорема

Если d —

- ① чётно и $2d > n$, то

$$t(n, d) \leq 2 \left\lfloor \frac{d}{2d - n} \right\rfloor;$$

- ② нечётно и $2d + 1 > n$, то

$$t(n, d) \leq 2 \left\lfloor \frac{d + 1}{2d + 1 - n} \right\rfloor.$$

Существуют коды, для которых граница Плоткина достигается.

Разделы I

- 1 Блочное кодирование. Коды Хэмминга
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 Циклические коды
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 Коды Боуза-Чоудхури-Хоквингема
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 Задачи с решениями

Разделы

- 1 Блочное кодирование. Коды Хэмминга
- 2 Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 Циклические коды
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 Коды Боуза-Чоудхури-Хоквингема
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 Задачи с решениями

Групповые коды: определение

Большая часть теории блочного кодирования построена на *линейных* кодах, позволяющих реализовывать эффективные алгоритмы кодирования/декодирования. В двоичном случае их называют *групповыми*, т.к. они образуют *группу относительно* \oplus .

Утверждение

Устойчивая совокупность кодовых слов $C = \{ \tilde{\alpha}^1, \dots, \tilde{\alpha}^t \}$ образует группу по сложению относительно операции \oplus .

Групповые коды: определение

Большая часть теории блочного кодирования построена на *линейных* кодах, позволяющих реализовывать эффективные алгоритмы кодирования/декодирования. В двоичном случае их называют *групповыми*, т.к. они образуют *группу относительно* \oplus .

Утверждение

Устойчивая совокупность кодовых слов $C = \{\tilde{\alpha}^1, \dots, \tilde{\alpha}^t\}$ образует группу по сложению относительно операции \oplus .

Доказательство

Устойчивость (предполагается): для любых кодовых слов $\tilde{\alpha}^i, \tilde{\alpha}^j \in C$ выполняется $\tilde{\alpha}^i \oplus \tilde{\alpha}^j = \tilde{\alpha}^k \in C$;

Ассоциативность: свойство операции \oplus ;

Существование 0: $\tilde{\alpha} \oplus \tilde{\alpha} = (0, \dots, 0) \stackrel{\text{def}}{=} \tilde{0} \in C$;

Противоположные элементы: $-\tilde{\alpha} = \tilde{\alpha} - \text{см. выше.}$

Свойство кодового расстояния группового кода

Теорема

Кодовое расстояние d группового кода C равно

$$d = \min_{\tilde{\alpha} \neq \tilde{\beta}} \rho(\tilde{\alpha}, \tilde{\beta}) = \min_{\tilde{\gamma} \neq \tilde{0}} \|\tilde{\gamma}\|,$$

где $\tilde{\alpha}$, $\tilde{\beta}$ и $\tilde{\gamma}$ — кодовые слова из C .

Свойство кодового расстояния группового кода

Теорема

Кодовое расстояние d группового кода C равно

$$d = \min_{\tilde{\alpha} \neq \tilde{\beta}} \rho(\tilde{\alpha}, \tilde{\beta}) = \min_{\tilde{\gamma} \neq \tilde{0}} \|\tilde{\gamma}\|,$$

где $\tilde{\alpha}$, $\tilde{\beta}$ и $\tilde{\gamma}$ — кодовые слова из C .

Доказательство

Для произвольных кодовых слов $\tilde{\alpha}$ и $\tilde{\beta}$ всегда существует их

сумма — кодовое слово $\tilde{\gamma}$: $\rho(\tilde{\alpha}, \tilde{\beta}) = \|\tilde{\alpha} \oplus \tilde{\beta}\| = \|\tilde{\gamma}\|$,

причем $\tilde{\gamma} \neq \tilde{0}$ при $\tilde{\alpha} \neq \tilde{\beta}$.

Отсюда получаем оценку $\min_{\tilde{\alpha} \neq \tilde{\beta}} \rho(\tilde{\alpha}, \tilde{\beta}) \geq \min_{\tilde{\gamma} \neq \tilde{0}} \|\tilde{\gamma}\|$, которая

достигается, например, при $\tilde{\beta} = \tilde{0}$.

Характеристики кода Хэмминга:

- исправляет **одну** ошибку;
- избыточность — $\frac{m}{2^m - 1}$;
- **совершенный код**: осуществляет плотную упаковку — куб B^{2^m-1} разбивается на

$$t = \frac{2^n}{n+1} = 2^{2^m-(m+1)}.$$

шаров радиуса $r = 1$ с центрами в кодовых словах;

- код Хэмминга — групповой $(2^m - 1, 2^m - 1 - m, 3)$ -код.

Линейные коды: определение

$\{0, 1\}^n$ — n -мерное координатное векторное пространство над конечным полем $\mathbb{F}_2 = \{0, 1\}$.

Определение

Блочный (n, k) -код C называется *линейным*, если он образует **векторное подпространство** размерности k координатного пространства $\{0, 1\}^n$ (двоичный случай).

Линейные коды: определение

$\{0, 1\}^n$ — n -мерное координатное векторное пространство над конечным полем $\mathbb{F}_2 = \{0, 1\}$.

Определение

Блочный (n, k) -код C называется *линейным*, если он образует **векторное подпространство** размерности k координатного пространства $\{0, 1\}^n$ (двоичный случай).

Это означает, что в линейном коде C —

- 1 сумма любых кодовых слов — кодовое слово;
- 2 кодовое расстояние $d = \min_{\tilde{\gamma} \in C} \|\tilde{\gamma}\|$;
- 3 существует базис из k векторов $\{\mathbf{g}_0, \mathbf{g}_1, \dots, \mathbf{g}_{k-1}\}$ и любой вектор $\mathbf{v} \in C$ может быть представлен как

$$\mathbf{v} = \sum_{i=0}^{k-1} u_i \mathbf{g}_i, \quad u_i \in \{0, 1\}.$$

Линейный код: матричное представление

$$\mathbf{v} = \sum_{i=0}^{k-1} u_i \mathbf{g}_i = \mathbf{G}\mathbf{u}, \text{ где } \mathbf{G}_{n \times k} = [\mathbf{g}_0 \mathbf{g}_1 \dots \mathbf{g}_{k-1}] -$$

— порождающая матрица кода.

Линейный код: матричное представление

$$\mathbf{v} = \sum_{i=0}^{k-1} u_i \mathbf{g}_i = G\mathbf{u}, \text{ где } G_{n \times k} = [\mathbf{g}_0 \mathbf{g}_1 \dots \mathbf{g}_{k-1}] -$$

— порождающая матрица кода.

Пример ((7, 4)-код Хэмминга)

Ранее была получена таблица, сложением произвольных строк которой получаются все $2^4 = 16$ кодовых слов. Порождающая матрица получается **транспонированием** этой таблицы:

$$G_{7 \times 4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

— при кодировании этой матрицей исходные сообщения помещаются в **первые 4 бита** кодового слова

Линейный код: проверочная матрица

Проверочная матрица $H_{m \times n}$, $m = n - k$ для линейного (n, k) -кода обладает свойством $Hv = \mathbf{0}$ для любого кодового слова v .

Если порождающая матрица имеет вид $\begin{bmatrix} I_k \\ P \end{bmatrix}$, то матрица $\begin{bmatrix} P & I_m \end{bmatrix}$ будет проверочной (I_k и I_m — единичные матрицы).

Пример ((7, 4)-код Хэмминга, продолжение)

Для построенной порождающей матрицы $G_{7 \times 4}$ проверочной будет

$$H_{3 \times 7} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Упражнение: Закодируйте матрицей G какое-нибудь 4-битное сообщение, получив код v , и убедитесь, что $Hv = \mathbf{0}$.

Разделы

- 1 Блочное кодирование. Коды Хэмминга
- 2 Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 Циклические коды
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 Коды Боуза-Чоудхури-Хоквингема
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 Задачи с решениями

Линейные коды: кодирование

$$\mathbf{u} \xrightarrow[\text{избыточность}]{\text{кодирование}} \mathbf{v} = G\mathbf{u}$$

На практике используют

систематическое кодирование, при котором k бит исходного сообщения копируются в **фиксированные позиции** кодового слова, а затем вычисляются остальные $m = n - k$ проверочных бит.

Такая возможность основана на том, что матрица G определена с точностью до эквивалентных преобразований **столбцов** (переход к другому базису).

При систематическом кодировании **2-й этап декодирования** ($\hat{\mathbf{v}} \rightarrow \hat{\mathbf{u}}$, удаление избыточности) становится тривиальным.

Систематическое кодирование: пример

Пусть линейный код задан порождающей матрицей G .

- С помощью эквивалентных преобразований столбцов матрица G может быть приведена к виду, в котором (без потери общности) **первые** k строк образуют единичную подматрицу I_k :

$$G_{n \times k} \longrightarrow \tilde{G}_{n \times k} = \begin{bmatrix} I_k \\ P_{m \times k} \end{bmatrix}$$

- Тогда кодирование $v = \tilde{G}u$ будет систематическим: **первые** k бит кодового слова v являются битами исходного сообщения u .

Ортогональное дополнение к подпространству кода

Разложение пространства $\{0, 1\}^n$ в прямую сумму подпространств:

$$\frac{\text{пространство} \quad \left| \quad \{0, 1\}^n \quad \leftrightarrow \quad C \quad + \quad C^\perp \right.}{\text{dim} \quad \left| \quad n \quad \quad \quad k \quad \quad \quad m = n - k \right.}$$

C^\perp — ортогональное дополнение (подпространство) к подпространству кода C , т.е.

$$\forall (v \in C, w \in C^\perp) \quad \underbrace{v^T \times w}_{\text{скалярное произведение}} = 0$$

(v^T — транспонированный вектор v).

Линейные коды: проверочная матрица

Определение

Пусть $\{h_0, \dots, h_{m-1}\} \in \{0, 1\}^n$ — базис C^\perp . Тогда матрица

$$H_{m \times n} = \begin{bmatrix} h_0^T \\ h_1^T \\ \vdots \\ h_{m-1}^T \end{bmatrix}$$

называется *проверочной матрицей* кода C .

Ясно, что

- $\forall v \in C: Hv = \mathbf{0}$;
- проверочная матрица определена с точностью до эквивалентных преобразований **строк**.

Построение систематической проверочной матрицы

Если линейный код C задан исходной порождающей матрицей G и построена матрица

$$\tilde{G}_{n \times k} = \begin{bmatrix} I_k \\ P_{m \times k} \end{bmatrix},$$

то проверочной матрицей H кода C будет

$$H_{m \times n} = [P_{m \times k} \quad I_m]$$

(I_k и I_m — единичные матрицы порядков k и m).

Действительно, в этом случае

$$Hv = H\tilde{G}u = (P + P)u = \mathbf{0}.$$

Линейный систематический код: задание

Таким образом, линейный код для сообщений длины k имеет длину $n = k + m$ и задаётся

- либо порождающей матрицей размера $n \times k$,
- либо проверочной матрицей размера $m \times n$.

Эти матрицы

- определены с точностью до эквивалентных преобразований столбцов и строк соответственно, что соответствует выбору различных базисов в пространствах C и C^\perp ,
- однако фиксирование позиций информационных бит при систематическом кодировании задаёт порождающую и проверочную матрицу однозначно.

Увеличение m ведёт к увеличению кодового расстояния d (как конкретно — трудный вопрос) и, следовательно, к увеличению количества ошибок, которые может исправить код.

Блочный линейный код: пример кодирования

Дано: линейный $(6, 3)$ -код C задан порождающей матрицей

$$G_{6 \times 3} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Требуется:

- 1 с использованием данного кода осуществить
(а) несистематическое и (б) систематическое кодирование векторов $\mathbf{u}_1 = [0 \ 1 \ 1]^T$ и $\mathbf{u}_2 = [1 \ 0 \ 1]^T$;
- 2 построить проверочную матрицу H кода C ;
- 3 определить кодовое расстояние d кода C .

Блочный линейный код: пример кодирования...

1(a). Несистематическое кодирование находим непосредственно:

$$[v_1^n \ v_2^n] = G \times [u_1 \ u_2] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Блочный линейный код: пример кодирования...

1 (6). Для систематического кодирования с помощью эквивалентных преобразований столбцов выделим в матрице G единичную подматрицу размера 3×3 (над стрелкой указано проводимое преобразование над столбцами):

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{(1)+(2) \mapsto (1)} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \tilde{G}.$$

В последней матрице в строках 3, 5 и 1 стоит единичная подматрица — это приведёт к тому, что 1, 2 и 3-й биты исходного сообщения последовательно перейдут в 3, 5 и 1-й биты кодового слова.

Блочный линейный код: пример кодирования...

Найдём систематическое кодирование $\mathbf{u}_1, \mathbf{u}_2$:

$$[\mathbf{v}_1^s \ \mathbf{v}_2^s] = \tilde{G} \times [\mathbf{u}_1 \ \mathbf{u}_2] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

2. Находим проверочную матрицу H , формируя матрицу $P_{3 \times 3}$ из строк \tilde{G} , отличных от строк с единичной подматрицей:

$$P_{3 \times 3} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Блоковый линейный код: пример кодирования...

Для построения проверочной матрицы H нужно

- последовательно разместить столбцы P в 3, 5 и 1-м её столбцах соответственно,
- остальные 2, 4 и 6-й столбцы H должны образовывать единичную подматрицу.

В итоге получим

$$H_{3 \times 6} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Блочный линейный код: пример кодирования...

Проверим, что в результате как систематического, так и несистематического кодирования были действительно найдены кодовые слова:

$$\begin{aligned}
 H \times [v_1^n \ v_2^n \ v_1^s \ v_2^s] &= \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} = \\
 &= \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.
 \end{aligned}$$

Блочный линейный код: пример кодирования...

3. Найдем **кодвое расстояние** d : построим матрицу **всех** $2^3 = 8$ кодовых слов и найдем минимальный ненулевой хэммингов вес:

$$\begin{aligned}
 [v_1 \dots v_8] &= G \times [u_1 \dots u_8] = \\
 &= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} =
 \end{aligned}$$

u_1, \dots, u_8 — все 8
возможных сообщений,
 v_1, \dots, v_8 — все 8
возможных кодовых слов.
Оказалось $d = 3$

$$= \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Разделы

- 1 Блочное кодирование. Коды Хэмминга
- 2 Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов**
- 3 Циклические коды
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 Коды Боуза-Чоудхури-Хоквингема
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 Задачи с решениями

Декодирование группового кода: синдром

Определение

Синдромом принятого слова w , закодированного групповым (n, k) -кодом и, возможно, содержащего ошибки, назовём вектор $s = Hw \in \{0, 1\}^m$, где H — проверочная матрица, $m = n - k$.

(*Синдром* — совокупность явлений, вызванных отклонением от нормы)

Свойства синдрома:

- $s = \mathbf{0} \Leftrightarrow w$ — кодовое слово;
- $s = Hw = H(v + e) = \underbrace{Hv}_{=0} + He = He,$

т.е. вектор ошибок e удовлетворяет системе линейных уравнений $H_{m \times n} e = s$.

Вычисление вектора ошибок по синдрому

Решение СЛАУ

$$H_{m \times n} e = s \quad (*)$$

относительно вектора ошибок e будем искать в виде суммы частного \hat{e} решения $(*)$ и общего Gu решения соответствующей однородной системы: $e = \hat{e} + Gu \in \{0, 1\}^n$.

Подставляя его в $(*)$, получим

$$\underbrace{H\hat{e}}_{=s} + \underbrace{HG}_{O}u = s,$$

где

- \hat{e} — произвольное частное решение системы $H\hat{e} = s$;
- u — произвольный вектор длины k ;
- O — матрица нулей размера $m \times k$.

Ясно, что $Gu \in \{0, 1\}^n$ — некоторое решение однородной системы $Hx = 0$.

Групповые коды: общая схема декодирования

После нахождения частного решения \hat{e} , все возможные кодовые слова u_1, \dots, u_{2^k} входного вектора дадут 2^k вариантов вектора $e_i = \hat{e} + Gu_i$.

Решение с **наименьшим хэмминговым весом** $\|e_i\|$ дает искомый вектор ошибок.

Получив вектор ошибок e , декодирование осуществляют по правилу $\hat{v} = w + e$.

Схема декодирования:

$$w \longrightarrow s = Hw \xrightarrow{He=s} e = \hat{e} + Gu \xrightarrow{\|e\| \rightarrow \min} \hat{v} = w + e$$

Для каждого из 2^m синдромов необходимо перебирать 2^k решений очередной СЛАУ, т.е. алгоритм декодирования линейного кода в общем случае имеет **экспоненциальную трудоёмкость** и по памяти, и по числу операций.

Декодирование линейного кода: пример

Возьмём линейный $(6, 3)$ -код из рассмотренного ранее примера: вектор сообщения есть $\mathbf{u} = [0 \ 1 \ 1]^T$.

Систематическое кодирование для него было получено раньше:

$$\mathbf{v} = [1 \ 1 \ 0 \ 0 \ 1 \ 0]^T.$$

Пусть при передаче происходит ошибка во втором бите, т.е. принятый вектор $\mathbf{w} = [1 \ 0 \ 0 \ 0 \ 1 \ 0]^T$.

Декодирование

1. Найдём **синдром** принятого сообщения \mathbf{w} :

$$H\mathbf{w} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \mathbf{s}.$$

Декодирование линейного кода: пример...

2. Находим все решения системы $He = s$.

2.a Находим частное решение \hat{e} этой системы. Поскольку в столбцах 2, 4, 6 проверочной матрицы H стоит единичная подматрица, возьмём координаты 1, 3 и 5 вектора \hat{e} нулевыми: $\hat{e}_1 = \hat{e}_3 = \hat{e}_5 = 0$ и тогда $\hat{e}_2 = s_1 = 1$, $\hat{e}_4 = s_2 = 0$, $\hat{e}_6 = s_3 = 0$, т.е. $\hat{e} = [0 \ 1 \ 0 \ 0 \ 0 \ 0]^T$.

2.a Все решения однородной системы $He = 0$ уже были найдены раньше при вычислении кодового расстояния d :

$$G \times [u_1 \ \dots \ u_8] = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Декодирование линейного кода: пример...

Таким образом, все 8 решений системы $He = s$ записываются как сумма вектора $\hat{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$ со всеми столбцами матрицы $G \times [u_1 \dots u_8]$:

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Выбираем среди них решение с наименьшим весом — это первый столбец $e = [0\ 1\ 0\ 0\ 0\ 0]^T$.

Отсюда

$$\hat{v} = w + e = [1\ 0\ 0\ 0\ 1\ 0]^T + [0\ 1\ 0\ 0\ 0\ 0]^T = [1\ 1\ 0\ 0\ 1\ 0]^T = v$$

и исходное сообщение восстановлено верно.

Групповое коды (n, k) : резюме

Требование **линейности** позволяет реализовывать **более эффективные алгоритмы** кодирования и декодирования.

Кодирование осуществляется особенно просто: для этого надо умножить вектор-сообщения на порождающую матрицу. Но вопрос «**как найти подходящую порождающую матрицу?**» остаётся открытым.

Декодирование также значительно упрощается:

- осуществляется с помощью легко вычисляемых синдромов;
- **этап 2** при систематическом кодировании элементарен.

Однако в общем случае требуется перебрать 2^k решений СЛАУ, т.е. несмотря на указанные упрощения, процесс декодирования остаётся всё ещё достаточно трудоёмким (**экспоненциальная сложность по k**).

Разделы I

- 1 **Блочное кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

Разделы

- 1 **Блочное кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

Циклические коды

Определение и основные свойства

Циклические коды: определение

Определение

Код C называется *циклическим (сдвиговым)*, если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leq s \leq n - 1$ справедливо

$$(\alpha_0, \dots, \alpha_{n-1}) \in C \Rightarrow (\alpha_s, \alpha_{s+1}, \dots, \alpha_{n-1}, \alpha_0, \dots, \alpha_{s-1}) \in C.$$

Циклические коды: определение

Определение

Код C называется *циклическим (сдвиговым)*, если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leq s \leq n - 1$ справедливо

$$(\alpha_0, \dots, \alpha_{n-1}) \in C \Rightarrow (\alpha_s, \alpha_{s+1}, \dots, \alpha_{n-1}, \alpha_0, \dots, \alpha_{s-1}) \in C.$$

Ранее рассматривалось и было показано:

- В кольце $\mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как векторное пространство над полем \mathbb{F}_p , имеется базис

$$\{ \bar{1}, \bar{x}, \dots, \overline{x^{n-1}} \}.$$

Циклический сдвиг координат в этом базисе равносителен умножению на x .

Циклические коды: определение

Определение

Код C называется *циклическим (сдвиговым)*, если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leq s \leq n - 1$ справедливо

$$(\alpha_0, \dots, \alpha_{n-1}) \in C \Rightarrow (\alpha_s, \alpha_{s+1}, \dots, \alpha_{n-1}, \alpha_0, \dots, \alpha_{s-1}) \in C.$$

Ранее рассматривалось и было показано:

- В кольце $\mathbb{F}_p[x]/(x^n - 1)$, рассматриваемом как векторное пространство над полем \mathbb{F}_p , имеется базис

$$\{ \overline{1}, \overline{x}, \dots, \overline{x^{n-1}} \}.$$

Циклический сдвиг координат в этом базисе равносителен умножению на x .

- **Теорема:** Векторное подпространство $I \subseteq \mathbb{F}_p[x]/(x^n - 1)$ является циклическим iff $I \triangleleft \mathbb{F}_p[x]/(x^n - 1)$.

Циклические коды: идея построения

Поэтому построить двоичный циклический код можно так:

- 1 выбираем некоторый делитель $g(x)$ бинорма $x^n - 1$; многочлен $g(x)$ называют *порождающим*.
- 2 в кольце $\mathbb{F}_2[x]/(x^n - 1)$ образуем идеал $(g(x))$.

Циклические коды: идея построения

Поэтому построить двоичный циклический код можно так:

- 1 выбираем некоторый делитель $g(x)$ бинома $x^n - 1$; многочлен $g(x)$ называют *порождающим*.
- 2 в кольце $\mathbb{F}_2[x]/(x^n - 1)$ образуем идеал $(g(x))$.

Оказывается, при удачном выборе $g(x)$ коэффициенты многочленов из данного идеала будут давать хороший код — с малой избыточностью m/n при большом d .

Однако:

- есть только несколько конструкций циклических кодов с хорошими параметрами;
- в общем случае определение кодового расстояния циклического кода чрезвычайно сложно.

Циклический код — англ. CRC, Cyclic Redundancy Code.

Линейные циклические коды

Из всех **линейных** (n, k) -кодов будем далее рассматривать те, которые являются одновременно и **циклическими**.

Установим соответствие вектора v координатного пространства $\{0, 1\}^n$ и полинома $v(x) \in \mathbb{F}_2[x]$:

$$v = [v_0, v_1, \dots, v_{n-1}]^T \leftrightarrow v(x) = v_0 + v_1x + \dots + v_{n-1}x^{n-1}.$$

Тогда свойство главного идеала переформулируется:

для каждого (n, k) -циклического кода найдется порождающий полином $g(x)$ такой, что

- 1 $g(x) \mid x^n - 1$;
- 2 любое кодовое слово $v(x)$ представляется в виде $v(x) = g(x)q(x)$, где $q(x)$ — некоторый полином.

Любой делящий $x^n - 1$ полином является порождающим для некоторого циклического кода длины n .

Разделы

- 1 Блочное кодирование. Коды Хэмминга
- 2 Групповые (линейные) коды
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 Коды Боуза-Чоудхури-Хоквингема
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 Задачи с решениями

Циклические коды: кодирование

Пусть задан порождающий полином $g(x)$ степени m
(= числу проверочных битов у будущего кода C).

Рассмотрим возможные методы построения линейных
циклических (n, k) -кодов ($n = m + k$), кодирующих
сообщение-полином $u(x)$ степени $k - 1$: $u(x) \mapsto v(x)$.

Результат — кодовое слово-полином $v(x) \in C$ степени $n - 1$.

Циклические коды: кодирование

Пусть задан порождающий полином $g(x)$ степени m
(= числу проверочных битов у будущего кода C).

Рассмотрим возможные методы построения линейных
циклических (n, k) -кодов ($n = m + k$), кодирующих
сообщение-полином $u(x)$ степени $k - 1$: $u(x) \mapsto v(x)$.

Результат — кодовое слово-полином $v(x) \in C$ степени $n - 1$.

Несистематическое кодирование осуществляется путём
умножения кодируемого вектора на порождающий полином:

$$u(x) \mapsto v(x) = g(x)u(x).$$

В порождающей матрице $G_{n \times k} = [g_0 \dots g_{k-1}]$ данного кода
базисные векторы g_i соответствуют полиномам $x^i g(x)$,
 $i = \overline{0, k-1}$.

Циклические коды: систематическое кодирование...

Систематическое кодирование осуществляется путём «дописывания» к кодируемому слову остатка $r(x)$ от деления $x^m u(x)$ на $g(x)$:

$$x^m u(x) = g(x)q(x) + r(x) \quad \text{и} \quad \deg r(x) < m.$$

Отсюда $x^m u(x) + r(x) = g(x)q(x) \in C$,

систематическое кодирование может быть задано как

$$v(x) = x^m u(x) + r(x), \quad \text{где} \quad r(x) \equiv_{g(x)} x^m u(x),$$

и полином $v(x)$ имеет в k крайних правых позициях (т.е. при старших степенях x) k коэффициентов полинома $u(x)$.

В порождающей матрице $G_{n \times k} = [g_0 \dots g_{k-1}]$ данного кода базисные векторы g_i соответствуют полиномам $x^{m+i} + r_i(x)$, где $r_i(x) \equiv_{g(x)} x^{m+i}$, $i = \overline{0, k-1}$.

Циклический код: пример кодирования

Пусть требуется построить циклический код длины $n = 7$.
Это означает, что работаем в **кольце** $\mathbb{F}_2[x]/(x^7 - 1)$.

Циклический код: пример кодирования

Пусть требуется построить циклический код длины $n = 7$.
Это означает, что работаем в **кольце** $\mathbb{F}_2[x]/(x^7 - 1)$.

1. Находим разложение полинома $x^7 - 1$ на неприводимые множители.

Так как $7 = 2^3 - 1$, то корнями $x^7 - 1$ являются **все ненулевые элементы поля** \mathbb{F}_2^3 .

Известно, что:

- каждый многочлен f над конечным полем содержит в расширении этого поля вместе с любым своим корнем β также сопряжённые корни вида $\beta^2, \beta^{2^2}, \dots$;
- если f приводим, то имеется несколько серий таких сопряжённых корней.

Циклический код: пример кодирования...

Пусть α — произвольный примитивный элемент поля $F = \mathbb{F}_2^3$. Тогда с учетом $\alpha^7 = 1$ находим разбиение корней $x^7 - 1$ (= всех элементов F^*) на орбиты:

$$\{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}, \{1\}.$$

Таким образом, многочлен $x^7 + 1$ имеет один неприводимый делитель 1-й степени и два неприводимых делителя 3-й степени. В результате получаем разложение

$$x^7 - 1 = x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Циклический код: пример кодирования...

Пусть α — произвольный примитивный элемент поля $F = \mathbb{F}_2^3$. Тогда с учетом $\alpha^7 = 1$ находим разбиение корней $x^7 - 1$ (= всех элементов F^*) на орбиты:

$$\{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}, \{1\}.$$

Таким образом, многочлен $x^7 + 1$ имеет один неприводимый делитель 1-й степени и два неприводимых делителя 3-й степени. В результате получаем разложение

$$x^7 - 1 = x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

2. Выбираем порождающий полином $g(x)$.

Можно выбрать любой делитель $x^7 + 1 \Rightarrow$ выберем

$g(x) = x^3 + x + 1$, тогда $\deg g(x) = 3 = m$, $k = n - m = 4$
и построен **циклический (7, 4)-код**.

Его кодовое расстояние — **надо выяснять...**

Циклический код: пример кодирования $g(x) = x^3 + x + 1 \dots$

3. Проведём кодирование полинома $u(x) = x^3 + x^2$ или в векторном представлении $\mathbf{u} = [0011]^T$ ($k = 4$).

Циклический код: пример кодирования $g(x) = x^3 + x + 1 \dots$

3. Проведём кодирование полинома $u(x) = x^3 + x^2$ или в векторном представлении $\mathbf{u} = [0011]^T$ ($k = 4$).

3.1. Несистематическое кодирование:

$v(x) = u(x)g(x) = (x^3 + x^2)(x^3 + x + 1) = x^6 + x^5 + x^4 + x^2$
или в векторном представлении $\mathbf{v} = [0010111]^T$ ($n = 7$).

Циклический код: пример кодирования $g(x) = x^3 + x + 1 \dots$

3. Проведём кодирование полинома $u(x) = x^3 + x^2$ или в векторном представлении $\mathbf{u} = [0011]^T$ ($k = 4$).

3.1. Несистематическое кодирование:

$v(x) = u(x)g(x) = (x^3 + x^2)(x^3 + x + 1) = x^6 + x^5 + x^4 + x^2$
или в векторном представлении $\mathbf{v} = [0010111]^T$ ($n = 7$).

3.2. Систематическое кодирование. Находим остаток $r(x)$ от деления многочлена $x^3u(x)$ на $g(x)$:

$$x^3(x^3 + x^2) = x^6 + x^5 = (x^3 + x^2 + x)(x^3 + x^2 + 1) + x,$$

поэтому $v(x) = x^3u(x) + r(x) = x^6 + x^5 + x$

или в векторном представлении $\mathbf{v} = [0100011]^T$ ($n = 7$),

т.е. биты входного сообщения \mathbf{u} воспроизводятся в крайних правых битах кодового слова \mathbf{v} .

Циклические коды: декодирование

Определение

Синдромом принятого полинома $w(x)$, закодированного циклическим (n, k) -кодом с порождающим полиномом $g(x)$ (и, возможно, содержащим ошибки), назовём остаток $s(x)$ от деления $w(x)$ на $g(x)$: $s(x) \equiv_{g(x)} w(x)$.

Определение синдрома для циклического кода, очевидно, есть перефразировка **в терминах полиномов** синдрома для групповых кодов.

Свойства синдрома $w(x)$:

- $s(x) \equiv 0 \Leftrightarrow w(x)$ — кодовое слово;
- $0 \leq \deg s(x) < m = n - k$;
- $s(x) \equiv_{g(x)} (v(x) + e(x)) \equiv_{g(x)} e(x)$.

Циклические коды: декодирование...

Декодирование циклического кода проходит по общей схеме декодирования линейного кода:

- 1 вычисляется синдром $s(x)$ принятого слова $w(x)$;
- 2 ищутся решения системы $e(x) = s(x) + g(x)u(x)$ для всех 2^k возможных полиномов $u(x)$ степени $k - 1$ (экспоненциальная сложность по k);
- 3 определяется полином ошибок как решение с минимальным числом ненулевых слагаемых;
- 4 восстанавливается переданное сообщение $u(x) = w(x) + e(x)$.

Примеры декодирования циклических кодов (с одной ошибкой) будут даны при рассмотрении БЧХ-кодов.

Циклические групповые коды (n, k) : резюме

- Линейные коды общего вида могут иметь произвольные параметры длины n и числа информационных бит k . Линейные циклические коды также могут иметь произвольную длину n , но параметры m и, следовательно, $k = n - m$ (число информационных бит) уже не произвольны: полином $g(x)$ степени m должен делиться бином $x^n - 1$.
- Циклический код будет групповым, только если он принадлежит идеалу $(g(x))$, $\deg g(x) = m$ кольца многочленов $\mathbb{F}_2[x]$: в нём циклические сдвиги кодового слова получаются умножением на x, x^2, \dots , что и обеспечивается равенством $x^n = 1$.

Циклические групповые коды (n, k) : резюме...

- **Кодирование** производится умножением сообщения на полином $g(x)$. Однако выбор $g(x)$, порождающего код с большим кодовым расстоянием d — **сложная задача** (оценка сверху: $d \leq m + 1$ число мономов в $g(x)$).
- **Декодирование** осуществляется с помощью вычисляемого синдрома принятого полинома, в результате:
 - вместо матричных умножений и решения СЛАУ (как в линейных кодах общего вида) используются операции умножения и деления (с остатком) полиномов, **легко реализуемые** на регистрах сдвига с обратными связями;
 - однако общий алгоритм декодирования по-прежнему имеет **экспоненциальную сложность** по k .

Существуют и альтернативные методы декодирования циклических кодов общего вида (декодеры Меггита, Касами-Рудольфа, мажоритарный, ...) — тоже плохие.

Разделы I

- 1 **Блочное кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

Разделы

- 1 **Блоковое кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

БЧХ-коды: первые сведения

Коды Боуза-Чоудхури-Хоквингема (БЧХ, BCH) — подкласс циклических кодов, исправляющих не менее **заранее заданного числа ошибок**.

Предложены Р.Ч. Боузом и Д.К. Рей-Чоудхури в 1960 г. независимо от опубликованной на год ранее работы А. Хоквингема.

Теоретически коды БЧХ могут исправлять **произвольное количество ошибок**, но при этом существенно увеличивается длина кодового слова n , что приводит к уменьшению скорости передачи данных и усложнению приёмно-передающей аппаратуры.

Коды Хэмминга — частный случай БЧХ-кодов.

Р.Ч. Боуз и Д.К. Рей-Чоудхури



Радж Чандра Боуз (Бошу)

(Raj Chandra Bose, 1901–1987) —

индийский математик, работавший в США.

Известен работой (в соавторстве),

опровергающей гипотезу Л. Эйлера

о несуществовании латинских квадратов

специального вида.



Двайджендра Камар Рей-Чоудхури

(Dwijendra Kumar Ray-Chaudhuri, 1933) —

индийский математик, работающий в США.

Обладатель медали Эйлера, присуждаемой

Институтом комбинаторики и приложений

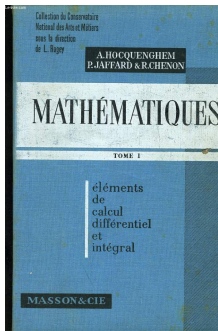
(Institute of Combinatorics and its Applications,

Канада) за вклад в развитие комбинаторики.

Коды Боуза-Чоудхури-Хоквингема

Определение и основные свойства

А. Хоквингем



Алексис Хоквингем

(Alexis Hocquenghem, 1908?–1990) — французский математик.

В его работе 1959 г. содержится первое описание линейных циклических кодов, исправляющих кратные ошибки.

Hocquenghem является галицинизированной формой германской или фламандской фамилии.

Правильное её чтение — *Окенгем*.

Свойства минимальных многочленов $m_\beta(x)$ поля \mathbb{F}_p^n

Вспоминаем:

- 1 $\forall \beta \in \mathbb{F}_p^n \exists! m_\beta(x)$ и $\deg m_\beta(x) \leq n$;
- 2 Если $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, то $a_n^{-1}a(x)$ — м.м. для x ;
- 3 $f(\beta) = 0 \Rightarrow f(x) : m_\beta(x)$;
- 4 Минимальный многочлен неприводим.
- 5 Минимальный многочлен генератора мультипликативной группы поля (примитивного элемента) называется *примитивным многочленом*.

Если β — корень **неприводимого** многочлена $\varphi(x) \in \mathbb{F}_p[x]$ степени n , то

$$\left\{ \beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}} \right\}$$

— **все** n различных (сопряжённых) корней $\varphi(x)$.

Циклотомический сопряжённый класс элемента поля

Определение (для случая $p = 2$)

Пусть $n \mid N$.

Циклотомическим классом (или *классом сопряжённости*) над полем \mathbb{F}_2^n элемента $\alpha \in \mathbb{F}_2^N$ называется множество всех различных элементов \mathbb{F}_2^N , являющихся 2^n -ми степенями α .

Циклотомический сопряжённый класс элемента поля

Определение (для случая $p = 2$)

Пусть $n \mid N$.

Циклотомическим классом (или *классом сопряжённости*) над полем \mathbb{F}_2^n элемента $\alpha \in \mathbb{F}_2^N$ называется множество всех различных элементов \mathbb{F}_2^N , являющихся 2^n -ми степенями α .

Свойства циклотомических классов

- Циклотомические классы сопряжённости различных элементов либо совпадают, либо не пересекаются. Т.е. совокупность всех циклотомических классов поля \mathbb{F}_2^N образует его **разбиение** его мультипликативной группы.
- Циклотомический класс $\left\{ \alpha, \alpha^{2^n}, \alpha^{2^{2n}}, \dots, \alpha^{2^{(k-1)n}} \right\}$ над полем \mathbb{F}_2^n **примитивного элемента** α поля \mathbb{F}_2^{kn} содержит ровно k элементов.

Свойства циклотомических классов...

Примеры.

Рассмотрим разложения мультипликативных групп полей \mathbb{F}_2^{kn} на циклотомические классы над \mathbb{F}_2^n .

- ① $n = 1$, $k = 3$ и α — примитивный элемент $\mathbb{F}_2^3 = F$.

Тогда $\alpha^7 = 1$ и разложение F^* над \mathbb{F}_2 есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5\}.$$

Свойства циклотомических классов...

Примеры.

Рассмотрим разложения мультипликативных групп полей \mathbb{F}_2^{kn} на циклотомические классы над \mathbb{F}_2^n .

- ① $n = 1, k = 3$ и α — примитивный элемент $\mathbb{F}_2^3 = F$.

Тогда $\alpha^7 = 1$ и разложение F^* над \mathbb{F}_2 есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5\}.$$

- ② $n = 2, k = 2$ и α — примитивный элемент $\mathbb{F}_2^4 = F$.

Тогда $\alpha^{15} = 1$ и разложение F^* над \mathbb{F}_2^2 есть

$$\{1\}, \{\alpha, \alpha^4\}, \{\alpha^2, \alpha^8\}, \{\alpha^3, \alpha^{12}\}, \{\alpha^5\}, \{\alpha^{10}\}, \\ \{\alpha^6, \alpha^9\}, \{\alpha^7, \alpha^{13}\}, \{\alpha^{11}, \alpha^{14}\}.$$

Свойства циклотомических классов...

Примеры.

Рассмотрим разложения мультипликативных групп полей \mathbb{F}_2^{kn} на циклотомические классы над \mathbb{F}_2^n .

- ① $n = 1$, $k = 3$ и α — примитивный элемент $\mathbb{F}_2^3 = F$.

Тогда $\alpha^7 = 1$ и разложение F^* над \mathbb{F}_2 есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5\}.$$

- ② $n = 2$, $k = 2$ и α — примитивный элемент $\mathbb{F}_2^4 = F$.

Тогда $\alpha^{15} = 1$ и разложение F^* над \mathbb{F}_2 есть

$$\{1\}, \{\alpha, \alpha^4\}, \{\alpha^2, \alpha^8\}, \{\alpha^3, \alpha^{12}\}, \{\alpha^5\}, \{\alpha^{10}\}, \\ \{\alpha^6, \alpha^9\}, \{\alpha^7, \alpha^{13}\}, \{\alpha^{11}, \alpha^{14}\}.$$

- ③ $n = 1$, $k = 4$ и α — примитивный элемент $\mathbb{F}_2^4 = F$.

Тогда $\alpha^{15} = 1$ и разложение F^* над \mathbb{F}_2 есть

$$\{1\}, \{\alpha, \alpha^2, \alpha^4, \alpha^8\}, \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9\}, \\ \{\alpha^5, \alpha^{10}\}, \{\alpha^7, \alpha^{14}, \alpha^{28} = \alpha^{13}, \alpha^{26} = \alpha^{11}\}.$$

Свойства циклотомических классов...

- Если $\alpha \in \mathbb{F}_2^N$ и m — мощность некоторого его циклотомического класса над подполем \mathbb{F}_2^n , то полином

$$m_\alpha(x) = \prod_{i=0}^{m-1} (x + \alpha^{2^i}) = x^{m-1} + \lambda_{m-2}x^{m-2} + \dots + \lambda_1x + \lambda_0$$

является м.м. α , а также для всех элементов, входящих в данный циклотомический класс.

Свойства циклотомических классов...

- Если $\alpha \in \mathbb{F}_2^N$ и m — мощность некоторого его циклотомического класса над подполем \mathbb{F}_2^n , то полином

$$m_\alpha(x) = \prod_{i=0}^{m-1} (x + \alpha^{2^i}) = x^{m-1} + \lambda_{m-2}x^{m-2} + \dots + \lambda_1x + \lambda_0$$

является м.м. α , а также для всех элементов, входящих в данный циклотомический класс.

Отсюда выводится метод построения м.м. для данного элемента поля α :

- 1 определить число m элементов циклотомического класса элемента α ;
- 2 найти коэффициенты полинома $m_\alpha(x)$ путем перемножения скобок $(x + \alpha^{2^i})$ для всех $i = \overline{0, m-1}$.

Специальные циклические коды

Если длина циклического кода $n = 2^q - 1$, то:

- 1 **корнями многочлена $x^n + 1$** являются все ненулевые элементы поля \mathbb{F}_2^q ;
- 2 **порождающими многочленами циклического кода** могут быть только произведения минимальных многочленов для некоторых совокупностей элементов \mathbb{F}_2^q .

Такие коды:

- 1 **являются подмножеством циклических кодов**, имеющим указанную удобную связь между порождающим полиномом и элементами из \mathbb{F}_2^q ;
- 2 уже не могут иметь произвольные длины (есть способ обойти это ограничение — использование т.н. **укороченных кодов БЧХ**, которые мы не рассматриваем).

БЧХ-коды: определение (простейший случай)

Пусть выбраны параметры: q , определяющий длину кода $n = 2^q - 1$ и *конструктивное расстояние* $d \leq n$.

Код БЧХ есть циклический (n, k) -код, в котором порождающий многочлен $g(x)$ имеет корнями элементы $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{d-1}$ поля $F = \mathbb{F}_2^q$ (называемые *нулями БЧХ-кода*) и где

α — генератор мультипликативной группы F^* ,

$\deg g(x) = m$ — число проверочных бит,

$k = n - m$ — число информационных бит.

При этом:

- $g(x)$ выбирают как **НОК полиномов** (часто это просто их произведение), являющихся минимальными многочленами для всех нулей кода, попавших в данный циклотомический класс;
- кодовое расстояние построенного кода оказывается **не менее выбранного** конструктивного расстояния d .

БЧХ-код: кодовое расстояние не менее конструктивного

Теорема

Пусть БЧХ-код длиной $n = 2^q - 1$ с конструктивным расстоянием d задаётся кодирующим многочленом

$$g(x) = \text{НОК}(m_1(x), \dots, m_{d-1}(x)),$$

где $m_i(x)$, $i = \overline{1, d-1}$ — минимальные многочлены нулей $\alpha, \alpha^2, \dots, \alpha^{d-1}$ кода.

Тогда кодовое расстояние данного БЧХ-кода не менее d .

Доказательство

Покажем, что многочлен $h(x)$ с корнями $\alpha, \alpha^2, \dots, \alpha^{d-1}$ имеет не менее d ненулевых элементов.

Предположим противное. Тогда $h(x)$ можно записать в виде

$$h(x) = b_1x^{n_1} + b_2x^{n_2} + \dots + b_{d-1}x^{n_{d-1}}.$$

БЧХ-код: кодовое расстояние не менее конструктивного...

Доказательство (продолжение)

Поскольку $\alpha, \alpha^2, \dots, \alpha^{d-1}$ — корни $h(x)$, его коэффициенты b_1, \dots, b_{d-1} должны удовлетворять линейной системе

$$\begin{cases} b_1\alpha^{n_1} & + & \dots & + & b_{d-1}\alpha^{n_{d-1}} & = & 0 \\ b_1\alpha^{2n_1} & + & \dots & + & b_{d-1}\alpha^{2n_{d-1}} & = & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \\ b_1\alpha^{(d-1)n_1} & + & \dots & + & b_{d-1}\alpha^{(d-1)n_{d-1}} & = & 0 \end{cases}$$

Матрица A системы невырождена, т.к. её определитель Вандермонда отличен от нуля:

$$|A| = \prod_{i>j} (\alpha^{n_i} - \alpha^{n_j}) \neq 0, \quad n_j < n_i < 2^q.$$

Следовательно, $b_1 = \dots = b_{d-1} = 0$ — противоречие.

Коды БЧХ: синдромы

Поскольку все кодовые слова циклического кода C делятся на полином $g(x)$ с корнями $\alpha, \alpha^2, \dots, \alpha^{d-1}$, то

$$v(x) \in C \Leftrightarrow v(\alpha^i) = 0, i = \overline{1, d-1}.$$

Определение

Синдромами принятого полинома $w(x)$, закодированного БЧХ-кодом с нулями $\alpha^i, i = \overline{1, d-1}$ и, возможно, содержащего ошибки, назовём значения $w(x)$ в нулях кода: $s_i = w(\alpha^i)$.

Ясно, что

«все синдромы равны нулю» $\Leftrightarrow w(x)$ — кодовое слово.

Определение синдрома для БЧХ-кода, очевидно, есть **перефразировка в терминах нулей кода полиномов** синдрома для циклического кода.

Разделы

- 1 **Блочное кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

Построения кодов БЧХ для $q = 3$, $n = 7$, $a(x) = x^3 + x + 1$

Пусть $q = 3$, т.е. строим БЧХ-коды для поля $F = \mathbb{F}_2^3$ и $n = 7$.

В качестве порождающего поле $F = \mathbb{F}_2[x]/(a(x))$ многочлена возьмём примитивный многочлен $a(x) = x^3 + x + 1$.

$a(x)$ — м.м. для генератора $x = \alpha \in F^*$ и F^* разбивается на следующие циклотомические классы над \mathbb{F}_2 (было ранее):

$$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}.$$

Построения кодов БЧХ для $q = 3$, $n = 7$, $a(x) = x^3 + x + 1$

Пусть $q = 3$, т.е. строим БЧХ-коды для поля $F = \mathbb{F}_3$ и $n = 7$.

В качестве порождающего поле $F = \mathbb{F}_2[x]/(a(x))$ многочлена возьмём примитивный многочлен $a(x) = x^3 + x + 1$.

$a(x)$ — м.м. для генератора $x = \alpha \in F^*$ и F^* разбивается на следующие циклотомические классы над \mathbb{F}_2 (было ранее):

$$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^5\}.$$

1. Код БЧХ, исправляющий $r = 1$ ошибку (код Хэмминга).

Тогда $d - 1 = 2r = 2$ и элементы α, α^2 попадают в **один** циклотомический класс.

М.м. для всех элементов этого класса — $a(x)$, поэтому порождающий полином $g(x) = a(x)$, $m = \deg g(x) = 3$ и в результате получаем уже известный **(7, 4, 3)**-код.

Построения кодов БЧХ для $q = 3$, $n = 7$, $a(x) = x^3 + x + 1 \dots$

2. Код БЧХ, исправляющий не менее $r = 2$ ошибок.

Поскольку $d - 1 = 2r = 4$, то порождающий полином $g(x)$ есть многочлен минимальной степени с корнями $\alpha, \alpha^2, \alpha^3, \alpha^4$ из поля F .

Данные элементы входят в **два** циклотомических класса: $\{\alpha, \alpha^2, \alpha^4\}$ и $\{\alpha^3, \alpha^6, \alpha^5\}$, порождаемых α и α^3 соответственно, следовательно $g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x)$, где $g_\alpha(x)$ и $g_{\alpha^3}(x)$ — м.м. для α и α^3 соответственно.

М.м. для α известен: $g_\alpha(x) = a(x) = x^3 + x + 1$.

Найдем м.м. для α^3 :

$$\begin{aligned} g_{\alpha^3}(x) &= (x + \alpha^3)(x + \alpha^5)(x + \alpha^6) = \\ &= x^3 + (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^8 + \alpha^9 + \alpha^{11})x + \alpha^{14}. \end{aligned}$$

Построения кодов БЧХ для $q = 3$, $n = 7$, $a(x) = x^3 + x + 1 \dots$

Вычислим коэффициенты $g_{\alpha^3}(x)$.

Поскольку α — примитивный элемент поля $\mathbb{F}_2[x]/(x^3 + x + 1)$,
то $\alpha^7 = 1$, $\alpha^3 = \alpha + 1$ и

$$\begin{aligned} \alpha^3 + \alpha^5 + \alpha^6 &= \alpha + 1 + (\alpha + 1)^2 + \alpha^2(\alpha + 1) = \\ &= \alpha + 1 + \alpha^2 + 1 + \alpha^3 + \alpha^2 = 1, \end{aligned}$$

$$\begin{aligned} \alpha^8 + \alpha^9 + \alpha^{11} &= \alpha^2 + \alpha + \alpha^4 = \alpha^2 + \alpha + \alpha(\alpha + 1) = 0, \\ \alpha^{14} &= 1. \end{aligned}$$

Таким образом, $g_{\alpha^3}(x) = x^3 + x^2 + 1$ и

$$\begin{aligned} g(x) &= g_{\alpha}(x) \cdot g_{\alpha^3}(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \quad \deg g(x) = 6, \quad k = 7 - 6 = 1. \end{aligned}$$

В результате построен тривиальный $(7, 1, 7)$ -код, содержащий всего два кодовых слова $\mathbf{v}_1 = [0000000]$, $\mathbf{v}_2 = [1111111]$ и исправляющий **3** ошибки.

Построения кодов БЧХ для $q = 4$, $n = 15$, $a(x) = x^4 + x + 1$

Мы видим, что код получился плохой: хотя он и исправляет больше ошибок, чем планировалось, его скорость равна $R = 1/7$, т.е. очень мала.

Попытаемся построить лучший код для исправления двух ошибок, взяв бóльшую его длину: $q = 4$, $n = 2^q - 1 = 15$.

Построения кодов БЧХ для $q = 4$, $n = 15$, $a(x) = x^4 + x + 1$

Мы видим, что код получился плохой: хотя он и исправляет больше ошибок, чем планировалось, его скорость равна $R = 1/7$, т.е. очень мала.

Попытаемся построить лучший код для исправления двух ошибок, взяв бóльшую его длину: $q = 4$, $n = 2^q - 1 = 15$.

3. Код БЧХ, исправляющий $r = 2$ ошибки.

В качестве порождающего поле $F = \mathbb{F}_2[x]/(a(x))$ многочлена возьмём примитивный многочлен $a(x) = x^4 + x + 1$.

Если α — генератор в F^* , то нулями кода будут $\alpha, \alpha^2, \alpha^3, \alpha^4$, располагающиеся в двух циклотомических классах:

$$\{ \alpha, \alpha^2, \alpha^4, \alpha^8 \} \text{ и } \{ \alpha^3, \alpha^6, \alpha^{12}, \alpha^9 \}.$$

Построения кодов БЧХ для $q = 4$, $n = 15$, $a(x) = x^4 + x + 1 \dots$

Минимальные многочлены для всех элементов этих классов:

первого (α): $g_\alpha(x) = a(x)$.

второго (α^3): $g_{\alpha^3}(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^{12}) =$
 $\dots = x^4 + x^3 + x^2 + x + 1$.

Порождающий полином есть

$$g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x) = x^8 + x^7 + x^6 + x^4 + 1.$$

В результате $k = 15 - 8 = 7$ и, можно показать, $d = 5$, т.е. получен БЧХ $(15, 7, 5)$ -код со скоростью уже $R = 7/15 > 1/7$.

Построения кодов БЧХ для $q = 4$, $n = 15$, $a(x) = x^4 + x + 1 \dots$

В том же поле F построим

4. Код БЧХ, исправляющий $r = 3$ ошибки.

Пусть α — генератор F^* (т.е. $\alpha^{15} = 1$, $\alpha^4 = \alpha + 1$).

Нулями конструируемого БЧХ-кода будут α , α^2 , \dots , α^6 ,
которые попадают в циклотомические классы

$$\{ \alpha, \alpha^2, \alpha^4, \alpha^8 \}, \{ \alpha^3, \alpha^6, \alpha^9, \alpha^{12} \}, \{ \alpha^5, \alpha^{10} \}.$$

Построения кодов БЧХ для $q = 4$, $n = 15$, $a(x) = x^4 + x + 1 \dots$

В том же поле F построим

4. Код БЧХ, исправляющий $r = 3$ ошибки.

Пусть α — генератор F^* (т.е. $\alpha^{15} = 1$, $\alpha^4 = \alpha + 1$).

Нулями конструируемого БЧХ-кода будут α , α^2 , \dots , α^6 ,
которые попадают в циклотомические классы

$$\{ \alpha, \alpha^2, \alpha^4, \alpha^8 \}, \{ \alpha^3, \alpha^6, \alpha^9, \alpha^{12} \}, \{ \alpha^5, \alpha^{10} \}.$$

Минимальные многочлены для элементов этих классов суть

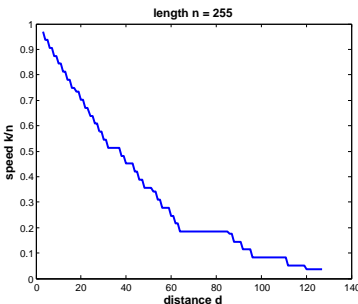
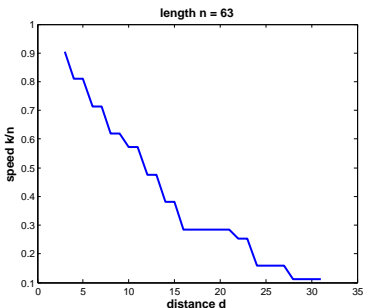
$$g_\alpha(x) = x^4 + x + 1, \quad g_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1 \text{ и}$$

$g_{\alpha^5}(x) = x^2 + x + 1$, а порождающий полином полученного
(15, 5, 7)-кода БЧХ есть их произведение:

$$g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x) \cdot g_{\alpha^5}(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Этот код при той же длине, что и предыдущий, исправляет больше ошибок, но имеет меньшую скорость.

Коды БЧХ: зависимости скорости от кодового расстояния



Графики скорости k/n кодов БЧХ в зависимости от кодового расстояния d для данной длины кода n .

«Ступеньки» на графиках соответствуют ситуации, когда реальное кодовое расстояние оказывается больше конструктивного, задаваемого при построении кода.

Разделы

- 1 **Блоковое кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

Декодирование кода Хэмминга: как это делается

Код Хэмминга является простейшим кодом БЧХ, у которого $r = 1$, $d = 3$, и поэтому его нулями являются α и α^2 , где α — примитивный элемент поля \mathbb{F}_2^n , $n = 2^q - 1$.

Декодирование кода Хэмминга: как это делается

Код Хэмминга является простейшим кодом БЧХ, у которого $r = 1$, $d = 3$, и поэтому его нулями являются α и α^2 , где α — примитивный элемент поля \mathbb{F}_2^n , $n = 2^q - 1$.

Для декодирования принятого слова $w(x)$ вычисляем синдром $s_1 = w(\alpha)$ (синдром $s_2 = w(\alpha^2)$ нам не потребуется).

При

- $s_1 = 0$ — полагаем $\hat{v}(x) = w(x)$ и если ошибок не произошло, то $\hat{v}(x) = v(x)$ (иначе произошло более 3-х ошибок и $\hat{v}(x) \neq v(x)$).
- $s_1 \neq 0$ — определяем значение $j \in \{0, \dots, n-1\}$, для которого $\alpha^j = s_1$, полагаем $\hat{v}(x) = w(x) + x^j$ и если произошла единичная ошибка, то её позиция j и $\hat{v}(x) = w(x)$ (иначе произошло большее количество ошибок и $\hat{v}(x) \neq v(x)$).

Декодирование кода Хэмминга: пример

Рассматриваем $(7, 4)$ -код Хэмминга, построенный в примере для циклических кодов (порождающий полином $g(x) = x^3 + x + 1$), где было найдено систематическое кодирование входного полинома $u(x) = x^3 + x^2 \leftrightarrow [0011]^T$:
 $v(x) = x^6 + x^5 + x \leftrightarrow [0100011]^T$.

Теперь мы построили этот же код с использованием поля $F = \mathbb{F}_2[x]/(x^3 + x + 1)$, в котором $\alpha^3 = \alpha + 1$ и $\alpha^7 = 1$ для примитивного элемента $\alpha \in F^*$.

Пусть при передаче рассматриваемого сообщения произошла ошибка в позиции **5**, т.е. принято слово $w(x) = x^6 + x$ и (неизвестный) полином ошибок $e(x) = x^5$.

Для декодирования $w(x)$ найдем синдром

$$\begin{aligned} s_1 = w(\alpha) &= \alpha^6 + \alpha = (\alpha^3)^2 + \alpha = (\alpha + 1)^2 + \alpha = \\ &= \alpha^2 + \alpha + 1 \neq 0. \end{aligned}$$

Декодирование кода Хэмминга: пример...

Найдём α^j для $j = 0, \dots, 6$, т.е. все ненулевые элементы поля $\mathbb{F}_2[x]/(x^3 + x + 1)$:

$$\alpha^0 = 1,$$

$$\alpha^3 = \alpha + 1,$$

$$\alpha^1 = \alpha,$$

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

$$\alpha^2 = \alpha^2,$$

$$\alpha^5 = \alpha^2(\alpha + 1) = \alpha^3 + \alpha^2 =$$

$$= \alpha^2 + \alpha + 1 = s_1,$$

$$\alpha^6 = (\alpha + 1)^2 = \alpha^2 + 1 \quad \text{— можно уже не вычислять}$$

Отсюда следует, что ошибка произошла в позиции 5 и, таким образом, $\hat{v}(x) = w(x) + x^5 = x^6 + x^5 + x = v(x)$.

Если же произошло **две ошибки**, например, в 5-й и 4-й позициях, то $w(x) = x^6 + x^4 + x$, $s_1 = 1$, $j = 0$,

$\hat{v}(x) = x^6 + x^4 + x + 1 \leftrightarrow [1100101]^T$ и будет раскодировано сообщение $[0101]^T$ вместо посланного $u(x) \leftrightarrow [0011]^T$.

Коды БЧХ: декодирование

Пусть при передаче сообщения, закодированного кодом БЧХ в поле $\mathbb{F}_2^q \cong \mathbb{F}[x]/(a(x))$ произошло ν ошибок.

Тогда $e(x) = x^{j_1} + x^{j_2} + \dots + x^{j_\nu}$, где степени j_1, \dots, j_ν — позиции ошибок, $\nu \leq r = \lfloor (d-1)/2 \rfloor$.

Коды БЧХ: декодирование...

В двоичной арифметике тождества Ньютона-Жирара записываются как

$$s_1 + \sigma_1 = 0,$$

$$s_2 + \sigma_1 s_1 + 2\sigma_2 = 0,$$

$$s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0,$$

.....

$$s_\nu + \sigma_1 s_{\nu-1} + \dots + \sigma_{\nu-1} s_1 + \nu\sigma_\nu = 0,$$

$$s_{\nu+1} + \sigma_1 s_\nu + \dots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0,$$

$$s_{\nu+2} + \sigma_1 s_{\nu+1} + \dots + \sigma_{\nu-1} s_3 + \sigma_\nu s_2 = 0,$$

.....

$$s_{2r} + \sigma_1 s_{2r-1} + \dots + \sigma_{\nu-1} s_{2r-\nu+1} + \sigma_\nu s_{2r-\nu} = 0.$$

} СЛАУ К.У.

Коды БЧХ: декодирование...

Последние $2r - \nu + 1$ уравнений данной системы являются СЛАУ относительно $\sigma_1, \dots, \sigma_\nu$.

Её решение позволяет найти полином локаторов ошибок $\sigma(x)$.

Далее полным перебором можно отыскать все его корни α^{-j_i} , а по ним — позиции ошибок j_i , $i = \overline{1, 2r}$.

Коды БЧХ: декодирование...

Последние $2r - \nu + 1$ уравнений данной системы являются СЛАУ относительно $\sigma_1, \dots, \sigma_\nu$.

Её решение позволяет найти полином локаторов ошибок $\sigma(x)$.

Далее полным перебором можно отыскать все его корни α^{-j_i} , а по ним — позиции ошибок j_i , $i = \overline{1, 2r}$.

Основная трудность в решении данной СЛАУ состоит в том, что значение ν неизвестно.

Рассмотрим два наиболее простых способа её решения — их называют *декодерами*.

Коды БЧХ: декодирование...

1. Декодер PGZ (Peterson-Gorenstein-Zierler) —

состоит в последовательном решении рассматриваемой СЛАУ для $\nu = r, r - 1, \dots$ до тех пор, пока матрица очередной СЛАУ не окажется невырожденной (при переходе от r к $r - 1$ полагаем $\sigma_r = 0$).

2. Декодер на базе расширенного алгоритма Евклида

Для нахождения полинома локаторов ошибок $\sigma(x)$ и его корней введём вспомогательный *синдромный полином*

$$s(x) = 1 + s_1x + s_2x^2 + \dots + s_{2r}x^{2r},$$

где $s_i = w(\alpha^i)$, $i = 1, \dots, 2r$ — синдромы.

Для продвинутых: это тоже производящий полином.

Коды БЧХ: декодирование...

Перемножим полиномы — синдромный и локаторов ошибок:

$$\lambda(x) = s(x)\sigma(x) = 1 + \lambda_1x + \lambda_2x^2 + \dots + \lambda_{2r+\nu}x^{2r+\nu}.$$

Здесь коэффициенты $\lambda_j = \sum_{i=0}^j s_i\sigma_{j-i}$ определяются соотношением для произведения многочленов.

Поскольку $\sigma_0 = 1$, СЛАУ эквивалентна условию $\lambda_{\nu+1} = \lambda_{\nu+2} = \dots = \lambda_{2r} = 0$, т.е.

$$\begin{aligned} \lambda(x) = & (1 + \lambda_1x + \lambda_2x^2 + \dots + \lambda_{\nu}x^{\nu}) + \\ & + (\lambda_{2r+1}x^{2r+1} + \dots + \lambda_{2r+\nu}x^{2r+\nu}). \end{aligned}$$

Коды БЧХ: декодирование...

Перемножим полиномы — синдромный и локаторов ошибок:

$$\lambda(x) = s(x)\sigma(x) = 1 + \lambda_1x + \lambda_2x^2 + \dots + \lambda_{2r+\nu}x^{2r+\nu}.$$

Здесь коэффициенты $\lambda_j = \sum_{i=0}^j s_i\sigma_{j-i}$ определяются соотношением для произведения многочленов.

Поскольку $\sigma_0 = 1$, СЛАУ эквивалентна условию $\lambda_{\nu+1} = \lambda_{\nu+2} = \dots = \lambda_{2r} = 0$, т.е.

$$\begin{aligned} \lambda(x) = & (1 + \lambda_1x + \lambda_2x^2 + \dots + \lambda_{\nu}x^{\nu}) + \\ & + (\lambda_{2r+1}x^{2r+1} + \dots + \lambda_{2r+\nu}x^{2r+\nu}). \end{aligned}$$

Рассмотрим остаток от деления $\lambda(x)$ на x^{2r+1} . Ясно, что

$$\lambda(x) \equiv_{x^{2r+1}} 1 + \lambda_1x + \dots + \lambda_{\nu}x^{\nu}.$$

Коды БЧХ: декодирование...

Таким образом, некоторый многочлен $\lambda(x)$ и полином локаторов ошибок $\sigma(x)$ удовлетворяют *ключевому уравнению*

$$s(x)\sigma(x) + x^{2r+1}a(x) = \lambda(x) \quad (*)$$

(напоминание: работаем в поле $\mathbb{F}_2^q \cong \mathbb{F}_2[x]/(a(x))$).

Относительно $\sigma(x)$ данное уравнение может быть решено с помощью расширенного алгоритма Евклида для пары многочленов $(x^{2r+1}, s(x))$ со свойствами:

- условие остановки — степень очередного остатка $\leq r$;
- количество фактически совершенных ошибок — $\nu = \deg \sigma(x)$.

Коды БЧХ: декодирование...

Таким образом, некоторый многочлен $\lambda(x)$ и полином локаторов ошибок $\sigma(x)$ удовлетворяют *ключевому уравнению*

$$s(x)\sigma(x) + x^{2r+1}a(x) = \lambda(x) \quad (*)$$

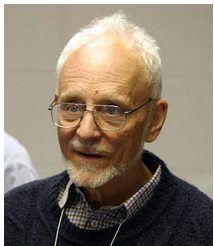
(напоминание: работаем в поле $\mathbb{F}_2^q \cong \mathbb{F}_2[x]/(a(x))$).

Относительно $\sigma(x)$ данное уравнение может быть решено с помощью расширенного алгоритма Евклида для пары многочленов $(x^{2r+1}, s(x))$ со свойствами:

- условие остановки — степень очередного остатка $\leq r$;
- количество фактически совершенных ошибок — $\nu = \deg \sigma(x)$.

Замечание: наиболее эффективным декодером (не слишком длинных) кодов БЧХ является *декодер Берлекэмпа-Мэсси*.

Э. Берлекэмп и Д. Мэсси



Элвин Ральф Берлекэмп

(Elwyn Ralph Berlekamp, 1940)

— американский математик, внесший существенный вклад в теории кодирования и комбинаторных игр (игра Го).

Помимо математики, занимался инвестиционным менеджментом.



Джеймс Ли Мэсси

(James Lee Massey, 1934–2013)

— выдающийся американский ученый, внесший значительный вклад в теорию информации и криптографию.

В частности, разработал (в соавторстве) шифры SAFER и IDEA.

Коды БЧХ: общая схема декодирования

Пусть принято слово $w(x)$, являющееся сообщением, закодированным (n, k, d) -кодом БЧХ и, возможно, содержащее ошибки, а α — генератор мультипликативной группы поля, порождённого кодирующим полиномом.

- 1 Для слова $w(x)$ найти все **синдромы** $s_i = w(\alpha^i)$, $i = \overline{1, d-1}$.
- 2 Найти **полином локаторов ошибок** $\sigma(x)$, используя тот или иной декодер.
- 3 Найти все **корни** $\sigma(x)$ полным перебором всех элементов поля \mathbb{F}_2^q (их $2^q - 1 = n$, т.е. алгоритм линейный по n , чего и добивались!); пусть найденные корни суть $\alpha^{k_1}, \dots, \alpha^{k_\nu}$.
- 4 Найти **позиции ошибок** $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.
- 5 Исправить ошибки, получив слово
$$\widehat{v}(x) = w(x) + x^{j_1} + \dots + x^{j_\nu}.$$
- 6 Найти все значения $\widehat{v}(\alpha^i)$, $i = \overline{1, d-1}$; если не все они равны нулю, то выдать отказ от декодирования.

Коды БЧХ: пример декодирования

Пусть БЧХ $(15, 5, 7)$ -код (т.е. $r = 3$) построен в поле $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(x^4 + x + 1)$.

Пусть имеется сообщение $[01101]^T \leftrightarrow u(x) = x^4 + x^2 + x$.

При систематическом кодировании (опустим этот этап) кодовое слово есть

$$v(x) = x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2 + x \leftrightarrow [011110001001101]^T$$

(убеждаемся, что биты сообщения находятся в крайне правых позициях кодового слова).

Пусть ошибки произошли в 0-й, 6-й и 12-й позициях, т.е. принятое слово —

$$w(x) = x^{14} + x^{11} + x^8 + x^6 + x^4 + x^3 + x^2 + x + 1 \leftrightarrow [\text{напишите сами!}]^T.$$

Коды БЧХ: пример декодирования...

Ненулевые элементы поля $\mathbb{F}_2[x]/(x^4 + x + 1)$:

α^1	α
α^2	α^2
α^3	α^3
α^4	$\alpha + 1$
α^5	$\alpha^2 + \alpha$
α^6	$\alpha^3 + \alpha^2$
α^7	$\alpha^3 + \alpha + 1$
α^8	$\alpha^2 + 1$
α^9	$\alpha^3 + \alpha$
α^{10}	$\alpha^2 + \alpha + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$
α^{14}	$\alpha^3 + 1$
α^{15}	1

Коды БЧХ: пример декодирования...

1. Найдём синдромы для принятого слова ($\alpha^4 = \alpha + 1$):

$$s_1 = w(\alpha) =$$

$$= \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha + \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 +$$

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

$$s_2 = w(\alpha^2) = (w(\alpha))^2 = \alpha^2,$$

$$s_3 = w(\alpha^3) = \alpha^{42} + \alpha^{33} + \alpha^{24} + \alpha^{18} + \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 = \dots$$

$$\dots = \alpha^6 + \alpha^3 + 1 = \alpha^3 + \alpha^2 + \alpha^3 + 1 = \alpha^2 + 1 = \alpha^8,$$

$$s_4 = w(\alpha^4) = (w(\alpha^2))^2 = \alpha^4,$$

$$s_5 = w(\alpha^5) = \alpha^{70} + \alpha^{55} + \alpha^{40} + \alpha^{30} + \alpha^{20} + \alpha^{15} + \alpha^{10} + \alpha^5 + 1 =$$

$$= \alpha^{10} + \alpha^{10} + \alpha^{10} + 1 + \alpha^5 + 1 + \alpha^{10} + \alpha^5 + 1 = 1,$$

$$s_6 = w(\alpha^6) = (w(\alpha^3))^2 = (\alpha^2 + 1)^2 = \alpha^4 + 1 = \alpha.$$

Таким образом, синдромный полином

$$s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \alpha^8 x^3 + \alpha^2 x^2 + \alpha x + 1.$$

Коды БЧХ: пример декодирования...

2. Выбираем декодер на базе расширенного алгоритма

Евклида — решаем уравнение $x^7 a(x) + s(x)\sigma(x) = \lambda(x)$

(находим $\sigma(x)$ по $a(x)$ и $s(x)$):

Шаг 0. $r_{-2}(x) = x^7,$
 $r_{-1}(x) = s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \alpha^8 x^3 +$
 $\quad + \alpha^2 x^2 + \alpha x + 1,$
 $y_{-2}(x) = 0,$
 $y_{-1}(x) = 1.$

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x),$
 $q_0(x) = \alpha^{14}x + \alpha^{13},$
 $r_0(x) = \alpha^8 x^5 + \alpha^{12} x^4 + \alpha^{11} x^3 + \alpha^{13},$
 $y_0(x) = y_{-2}(x) + y_{-1}(x)q_0(x) = q_0(x) = \alpha^{14}x + \alpha^{13}.$

Коды БЧХ: пример декодирования...

$$\begin{aligned} \text{Шаг 2. } r_{-1}(x) &= r_0(x)q_1(x) + r_1(x), \\ q_1(x) &= \alpha^8x + \alpha^2, \\ r_1(x) &= \alpha^{14}x^4 + \alpha^3x^3 + \alpha^2x^2 + \alpha^{11}x, \\ y_1(x) &= y_{-1}(x) + y_0(x)q_1(x) = \alpha^7x^2 + \alpha^{11}x. \end{aligned}$$

$$\begin{aligned} \text{Шаг 3. } r_0(x) &= r_1(x)q_2(x) + r_2(x), \\ q_2(x) &= \alpha^9x, \\ r_2(x) &= \alpha^5x + \alpha^{13}, \\ y_2(x) &= y_0(x) + y_1(x)q_2(x) = \alpha x^3 + \alpha^5x^2 + \alpha^{14}x + \alpha^{13}. \end{aligned}$$

Это последний шаг алгоритма Евклида, т.к. текущий остаток $r_2(x)$ имеет степень $1 \leq r = 3$.

Таким образом, полином локаторов ошибок найден:

$$\sigma(x) = y_2(x) = \alpha x^3 + \alpha^5x^2 + \alpha^{14}x + \alpha^{13}$$

и $\nu = \deg \sigma(x) = 3$.

Коды БЧХ: пример декодирования...

3. Найдём корни $\sigma(x)$ полным перебором ($\alpha^4 = \alpha + 1$):

$$\sigma(\alpha) = \alpha^4 + \alpha^7 + 1 + \alpha^{13} = \alpha^2,$$

$$\sigma(\alpha^2) = \alpha^7 + \alpha^9 + \alpha + \alpha^{13} = \alpha^3 + \alpha^2 + \alpha,$$

$$\sigma(\alpha^3) = \alpha^{10} + \alpha^{11} + \alpha^2 + \alpha^{13} = 0,$$

$$\sigma(\alpha^4) = \alpha^{13} + \alpha^{13} + \alpha^3 + \alpha^{13} = \alpha^2 + 1,$$

$$\sigma(\alpha^5) = \alpha + 1 + \alpha^4 + \alpha^{13} = \alpha^{13},$$

$$\sigma(\alpha^6) = \alpha^4 + \alpha^2 + \alpha^5 + \alpha^{13} = \alpha^3 + \alpha^2,$$

$$\sigma(\alpha^7) = \alpha^7 + \alpha^4 + \alpha^6 + \alpha^{13} = \alpha^3 + 1,$$

$$\sigma(\alpha^8) = \alpha^{10} + \alpha^6 + \alpha^7 + \alpha^{13} = \alpha^3 + \alpha^2 + 1,$$

$$\sigma(\alpha^9) = \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} = 0,$$

$$\sigma(\alpha^{10}) = \alpha + \alpha^{10} + \alpha^9 + \alpha^{13} = \alpha,$$

$$\sigma(\alpha^{11}) = \alpha^4 + \alpha^{12} + \alpha^{10} + \alpha^{13} = \alpha^2 + \alpha,$$

$$\sigma(\alpha^{12}) = \alpha^7 + \alpha^{14} + \alpha^{11} + \alpha^{13} = 1,$$

$$\sigma(\alpha^{13}) = \alpha^{10} + \alpha + \alpha^{12} + \alpha^{13} = \alpha^2 + \alpha + 1,$$

$$\sigma(\alpha^{14}) = \alpha^{13} + \alpha^3 + \alpha^{13} + \alpha^{13} = \alpha^2 + 1,$$

$$\sigma(\alpha^{15}) = \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} = 0.$$

Коды БЧХ: пример декодирования...

4. По найденным корням $\alpha^3, \alpha^9, \alpha^{15}$ вычисляем позиции ошибок:

$$j_1 = -3 \equiv_{15} 12,$$

$$j_2 = -9 \equiv_{15} 6,$$

$$j_3 = -15 \equiv_{15} 0.$$

5. Имеем: полином ошибок $e(x) = x^{12} + x^6 + 1$ определён правильно, $\hat{v}(x) = w(x) + e(x) =$

$$= x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2 + x.$$

и кодовое слово восстановлено.

6. Проверка $\hat{v}(\alpha) = \hat{v}(\alpha^2) = \dots = \hat{v}(\alpha^6) = 0$ говорит о том, что восстановление верное (или же произошло $r \gg 3$ ошибок, что крайне маловероятно).

БЧХ (n, k, d) -коды: исторические сведения

Первым практически реализованным БЧХ-кодом был $(127, 92, 11)$ -код.

В системах передачи данных широко используется двоичный $(255, 231, 7)$ -код, построенный с помощью примитивного элемента $\alpha \in \mathbb{F}_2^8$ 255-го порядка:

- степень порождающего многочлена $g(x) - 24$;
- корни $g(x) - \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ и α^6 .
- в общем числе слов длины 255 доля кодовых — $2^{-24} \approx \frac{1}{16 \cdot 10^6}$ (при вводе случайных слов только примерно одно из шестнадцати миллионов оказалось бы кодовым).

В течении многих лет не было случая, чтобы ошибка передачи прошла незамеченной.

Для выбора минимальных многочленов при построении БЧХ-кодов [составлены специальные таблицы](#).

БЧХ (n, k, d) -коды: резюме

- БЧХ-коды являются **подклассом циклических**.
- **Самое ценное свойство** — возможность построения кода с **заданным кодовым расстоянием d** .
- **Кодирование** осуществляется с помощью порождающего полинома, имеющего корнями степени некоторого примитивного элемента поля.
- **Декодирование** может быть проведено с помощью эффективных алгоритмов (Берлекэмп-Мэсси, Питерсона-Горенштейна-Цирлера, Евклидов алгоритм, ...).
- Среди кодов БЧХ при небольших длинах существуют хорошие (но, как правило, не лучшие из известных) коды. С ростом n при фиксированном значении скорости кода, к сожалению, $d/n \rightarrow 0$, и поэтому при больших длинах приходится использовать другие коды.

Коды Рида–Соломона: общие сведения

Широко используемым частным случаем кодов БЧХ являются *коды Рида-Соломона* (Reed–Solomon codes), которые позволяют исправлять пакеты ошибок.

Пакет ошибок (error burst) — группа битов, в которой два последовательных ошибочных бита всегда разделены правильными битами, число которых менее установленного.

Коды Рида–Соломона:

- **небинарные** (в частности, очень распространены коды, работающие с байтами);
- часто используются в устройствах **цифровой записи звука**, в том числе на компакт-диски.



Пример негруппового блокового кода

Пусть по двоичному симметричному каналу с шумом требуется передавать $t = 4$ битовых сообщения S_1, S_2, S_3, S_4 длины 2. Блоковый разделимый негрупповой код C , исправляющий 1 ошибку задаётся таблицей

S	C
00	00110
01	01101
10	10011
11	11000

«Зазор»: $2^5 - 4 \cdot (1 + 5) = 8$ слов;
 граница Плоткина достигается
 (проверьте)

Кодовое расстояние построенного кода C равно 3 и построен систематический $(5, 2, 3)$ -код, содержащий исходное сообщение в **первых двух** позициях.

Для сравнения: $(7, 4, 3)$ -код Хэмминга кодирует 16 сообщений длины 4.

Применение помехоустойчивого кодирования I

- Далеко не всегда от кода требуется коррекция ошибок. Многие современные каналы связи обладают хорошими характеристиками, и принимающей стороне часто достаточно лишь проверить, успешно ли прошла передача, а конкретные позиции неверных символов её не интересуют.
В этих случаях применяются коды специально предназначенные для обнаружения ошибок, а не для их исправления.
- Коды используются для получения надежной связи, когда мощность принимаемого сигнала близка к мощности тепловых шумов.
- В военных приложениях — для защиты против намеренно организованной противником интерференции.

Применение помехоустойчивого кодирования II

- Передача данных в вычислительных системах обычно чувствительна даже к очень малой доле ошибок. Здесь помехозащищённые коды используются для
 - защиты данных во внутренних и внешних ЗУ (ленты, диски...),
 - защиты данных неправильного функционирования или шумов в цифровых логических цепях,
 - сжатия (плотной упаковки) данных.
- Теория кодирования применяется также для получения устойчивых признаков из биометрических характеристик (сетчатка глаза, отпечатки пальцев, ...).

Вся математика делится на три раздела: небесная механика, гидродинамика и теория кодирования.

В. И. Арнольд

Разделы I

- 1 **Блочное кодирование. Коды Хэмминга**
- 2 **Групповые (линейные) коды**
 - Определение и свойства
 - Кодирование линейными кодами
 - Декодирование линейных кодов
- 3 **Циклические коды**
 - Определение и основные свойства
 - Кодирование циклическими кодами и декодирование
- 4 **Коды Боуза-Чоудхури-Хоквингема**
 - Определение и основные свойства
 - Кодирование БЧХ-кодами
 - Декодирование кодов БЧХ
- 5 **Задачи с решениями**

Задача ТК-1

Для линейного кода, заданного своей *проверочной* матрицей

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

требуется

- 1 построить *порождающую* матрицу G кода для систематического кодирования, при котором биты исходного сообщения переходят в *последние* биты кодового слова;
- 2 найти такое кодирование для векторов

$$\mathbf{u}_1 = [1101]^T, \mathbf{u}_2 = [1001]^T.$$

Задача ТК-1 (I_4 и I_3 — единичные матрицы порядка 4 и 3)...

Решение

Проверочная матрица H имеет размерность 3×7 , следовательно код при длине $n = 7$ содержит $m = 3$ проверочных и $k = 7 - 3 = 4$ информационных бит.

Порождающая матрица кода G , обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_4 \end{bmatrix}$.

Матрицу P можно получить, если привести проверочную матрицу H к виду $[I_3 \ P]$:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{1 \leftrightarrow 3} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1+3 \mapsto 1} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Задача ТК-1...

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\mathbf{u}_1 = [1101]^T$, $\mathbf{u}_2 = [1001]^T$:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad [\mathbf{v}_1, \mathbf{v}_2] = G \times [\mathbf{u}_1, \mathbf{u}_2] = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

Нетрудно видеть, что был задан $(7, 4, 3)$ -код Хэмминга, помещающий проверочные биты в первых 3 позициях кода.

Заметим, что традиционно проверочные биты располагаются в 1, 2, 4, 8, ... позициях кодового слова.

Задача ТК-2

Циклический $(9, 3)$ -код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить минимальное расстояние кода d , а также осуществить систематическое кодирование полинома

$$u(x) = x^2 + x \leftrightarrow [011]^T.$$

Задача ТК-2

Циклический $(9, 3)$ -код задан своим порождающим полиномом

$$g(x) = x^6 + x^3 + 1.$$

Требуется определить минимальное расстояние кода d , а также осуществить систематическое кодирование полинома

$$u(x) = x^2 + x \leftrightarrow [011]^T.$$

Решение

Для определения минимального кодового расстояния d найдём все кодовые полиномы:

$$\begin{aligned}v(x) &= g(x)(ax^2 + bx + c) = (x^6 + x^3 + 1)(ax^2 + bx + c) = \\ &= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c,\end{aligned}$$

$$a, b, c \in \mathbb{F}_2.$$

Задача ТК-2...

В векторном виде все кодовые слова представляются как

$$[a, b, c, a, b, c, a, b, c].$$

Очевидно, что минимальный хэммингов вес ненулевого кодового слова равен 3 и, следовательно, $d = 3$.

Задача ТК-2...

В векторном виде все кодовые слова представляются как

$$[a, b, c, a, b, c, a, b, c].$$

Очевидно, что минимальный хэммингов вес ненулевого кодового слова равен 3 и, следовательно, $d = 3$.

Проводим систематическое кодирование сообщения $u(x)$:

$$v(x) = x^6 u(x) + r(x) \quad \boxed{\equiv}$$

$$r(x) \equiv g(x) x^6 u(x) \equiv_{x^6+x^3+1} x^8 + x^7 = x^5 + x^4 + x^2 + x,$$

$$\boxed{\equiv} x^8 + x^7 + x^5 + x^4 + x^2 + x \leftrightarrow [011011011]^T$$

и убеждаемся, что биты сообщения находятся в крайне правых позициях кодового слова.

Задача ТК-3

Рассмотрим код Хэмминга систематического кодирования с порождающим полиномом $\alpha \in \mathbb{F}_2[x]/(x^3 + x + 1)$.

Требуется декодировать полученные полиномы

- 1 $w_1(x) = x^6 + x^2 + x,$
- 2 $w_2(x) = x^6 + x^5 + x^3 + x^2 + x,$
- 3 $w_3(x) = x^6 + x^3 + x^2 + x.$

Задача ТК-3

Рассмотрим код Хэмминга систематического кодирования с порождающим полиномом $\alpha \in \mathbb{F}_2[x]/(x^3 + x + 1)$.

Требуется декодировать полученные полиномы

❶ $w_1(x) = x^6 + x^2 + x,$

❷ $w_2(x) = x^6 + x^5 + x^3 + x^2 + x,$

❸ $w_3(x) = x^6 + x^3 + x^2 + x.$

Решение Очевидно, имеем $(7, 4, 3)$ -код Хэмминга, в котором сообщение кодирует коэффициенты перед степенями 3, 4, 5 и 6 полинома кодового слова.

Для декодирования необходимо вычислить синдром $s = w(\alpha)$ принятого слова. Если $s = 0$, то считаем, что ошибок при передаче не произошло; иначе необходимо найти такое k , что $\alpha^k = s$ и перед восстановлением сообщения инвертировать k -й разряд $w(\alpha)$ (что, очевидно, имеет смысл при $k \in [3, \dots, 6]$).

Задача ТК-3... ($\alpha^3 = \alpha + 1$)

$$1. \underline{w_1(x) = x^6 + x^2 + x} \leftrightarrow [0110001]$$

$$\begin{aligned} s &= \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ &= (\alpha + 1)^2 + \alpha^2 + \alpha = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1 \neq 0. \end{aligned}$$

Очевидно, $\alpha + 1 = \alpha^3$, т.е. $k = 3$, ошибка произошла в 3-м разряде и $\hat{v}(x) = w(x) + e(x) = x^6 + x^3 + x^2 + x \leftrightarrow [0111001]$,
 $u(x) \leftrightarrow [1001]$.

Задача ТК-3... ($\alpha^3 = \alpha + 1$)

$$1. \underline{w_1(x) = x^6 + x^2 + x} \leftrightarrow [0110001]$$

$$\begin{aligned} s &= \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ &= (\alpha + 1)^2 + \alpha^2 + \alpha = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1 \neq 0. \end{aligned}$$

Очевидно, $\alpha + 1 = \alpha^3$, т.е. $k = 3$, ошибка произошла в 3-м разряде и $\hat{v}(x) = w(x) + e(x) = x^6 + x^3 + x^2 + x \leftrightarrow [0111001]$, $u(x) \leftrightarrow [1001]$.

$$2. \underline{w_2(x) = x^6 + x^5 + x^3 + x^2 + x} \leftrightarrow [0111011]$$

$$\begin{aligned} s &= \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha = (\alpha + 1)^2 + (\alpha + 1)\alpha^2 + \alpha + 1 + \alpha^2 + \alpha = \\ &= \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha^2 + 1 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 \neq 0. \end{aligned}$$

Очевидно, $\alpha^3 + \alpha^2 = (\alpha + 1)\alpha^2 = \alpha^5$, т.е. $k = 5$, ошибка произошла в 5-м разряде и снова $u(x) \leftrightarrow [1001]$.

Задача ТК-3... ($\alpha^3 = \alpha + 1$)

$$1. \underline{w_1(x) = x^6 + x^2 + x} \leftrightarrow [0110001]$$

$$\begin{aligned} s &= \alpha^6 + \alpha^2 + \alpha = (\alpha^3)^2 + \alpha^2 + \alpha = \\ &= (\alpha + 1)^2 + \alpha^2 + \alpha = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1 \neq 0. \end{aligned}$$

Очевидно, $\alpha + 1 = \alpha^3$, т.е. $k = 3$, ошибка произошла в 3-м разряде и $\hat{v}(x) = w(x) + e(x) = x^6 + x^3 + x^2 + x \leftrightarrow [0111001]$, $u(x) \leftrightarrow [1001]$.

$$2. \underline{w_2(x) = x^6 + x^5 + x^3 + x^2 + x} \leftrightarrow [0111011]$$

$$\begin{aligned} s &= \alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha = (\alpha + 1)^2 + (\alpha + 1)\alpha^2 + \alpha + 1 + \alpha^2 + \alpha = \\ &= \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha^2 + 1 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 \neq 0. \end{aligned}$$

Очевидно, $\alpha^3 + \alpha^2 = (\alpha + 1)\alpha^2 = \alpha^5$, т.е. $k = 5$, ошибка произошла в 5-м разряде и снова $u(x) \leftrightarrow [1001]$.

3. $\underline{w_3(x) = x^6 + x^3 + x^2 + x} \leftrightarrow [0111001]$. Убеждаемся, что в этом случае $s = 0$, т.е. ошибок не произошло и $u(x) \leftrightarrow [1001]$

Задача ТК-3... ($\alpha^3 = \alpha + 1$)

Заметим, что декодирование систематического кода Хэмминга можно просто осуществить делением принятого полинома на порождающий. Тогда остаток от деления есть синдром s :

$$w(x) = q(x) \cdot g(x) + r(x), \quad r(x) = s.$$

В нашем случае:

$$\textcircled{1} \quad x^6 + x^2 + x = (x^3 + x + 1)^2 + x + 1;$$

$$\textcircled{2} \quad x^6 + x^5 + x^3 + x^2 + x = \\ = (x^3 + x^2 + x + 1)(x^3 + x + 1) + x^2 + x + 1;$$

$$\textcircled{3} \quad x^6 + x^3 + x^2 + x = (x^3 + x)(x^3 + x + 1) + 0.$$

Задача ТК-4

Для кода БЧХ с нулями α , α^2 , α^3 и α^4 , где α — примитивный элемент поля $F = \mathbb{F}_2[x]/(x^4 + x + 1)$ и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

Задача ТК-4

Для кода БЧХ с нулями $\alpha, \alpha^2, \alpha^3$ и α^4 , где α — примитивный элемент поля $F = \mathbb{F}_2[x]/(x^4 + x + 1)$ и принятого слова

$$w(x) = x^{14} + x^{10} + x^5 + x^4.$$

найти полином локаторов ошибок $\sigma(x)$.

Решение

Для удобства вычислений в поле F построим таблицу соответствий между степенным и полиномиальным представлением элементов поля.

Задача ТК-4... ($\alpha^4 = \alpha + 1$)

α	α
α^2	α^2
α^3	α^3
α^4	$\alpha + 1$
α^5	$\alpha^2 + \alpha$
α^6	$\alpha^3 + \alpha^2$
α^7	$\alpha^3 + \alpha + 1$
α^8	$\alpha^2 + 1$
α^9	$\alpha^3 + \alpha$
α^{10}	$\alpha^2 + \alpha + 1$
α^{11}	$\alpha^3 + \alpha^2 + \alpha$
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^{13}	$\alpha^3 + \alpha^2 + 1$
α^{14}	$\alpha^3 + 1$
α^{15}	1

Задача ТК-4 $w(x) = x^{14} + x^{10} + x^5 + x^4 \dots$

С помощью этой таблицы вычислим синдромы:

$$s_1 = w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7,$$

$$s_2 = w(\alpha^2) = (w(\alpha))^2 = \alpha^{14},$$

$$s_3 = w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0,$$

$$s_4 = w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.$$

Синдромный полином — $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7x + 1$.

Синдромов всего четыре, следовательно, $r = 2$.

Задача ТК-4 $w(x) = x^{14} + x^{10} + x^5 + x^4 \dots$

С помощью этой таблицы вычислим синдромы:

$$s_1 = w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7,$$

$$s_2 = w(\alpha^2) = (w(\alpha))^2 = \alpha^{14},$$

$$s_3 = w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0,$$

$$s_4 = w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.$$

Синдромный полином — $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7x + 1$.

Синдромов всего четыре, следовательно, $r = 2$.

Полином локаторов ошибок $\sigma(x)$ является решением уравнения

$$x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \deg \lambda(x) \leq r.$$

Задача ТК-4... $(x^{2r+1}a(x) + s(x)\sigma(x) = \lambda(x), \deg \lambda(x) \leq t)$

Решаем с помощью расширенного алгоритма Евклида:

Шаг 0. $r_{-2}(x) = x^5$, // Инициализация
 $r_{-1}(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7x + 1$,
 $y_{-2}(x) = 0$,
 $y_{-1}(x) = 1$.

Шаг 1. $r_{-2}(x) = r_{-1}(x)q_0(x) + r_0(x)$,
 // Делим $r_{-2}(x)$ на $r_{-1}(x)$ с остатком
 $q_0(x) = \alpha^2x$,
 $r_0(x) = \alpha x^3 + \alpha^9x^2 + \alpha^2x$,
 $y_0(x) = y_{-2}(x) - y_{-1}(x)q_0(x) = -q_0(x) = \alpha^2x$.

Шаг 2. $r_{-1}(x) = r_0(x)q_1(x) + r_1(x)$,
 // Делим $r_{-1}(x)$ на $r_0(x)$ с остатком
 $q_1(x) = \alpha^{12}x + \alpha^5$,
 $r_1(x) = \alpha^{14}x^2 + 1$,
 $y_1(x) = y_{-1}(x) - y_0(x)q_1(x) =$
 $= 1 + \alpha^2x(\alpha^{12}x + \alpha^5) = \alpha^{14}x^2 + \alpha^7x + 1$.

Задача ТК-4...

Таким образом, искомый полином локаторов ошибок

$$\sigma(x) = \alpha^{14}x^2 + \alpha^7x + 1.$$

Задача ТК-5

Рассмотрим код БЧХ, нули которого определяются степенями α , где α — примитивный элемент поля $\mathbb{F}_2[x]/(x^4 + x + 1)$.

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок $\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$.

Требуется *определить позиции ошибок* в $w(x)$.

Задача ТК-5

Рассмотрим код БЧХ, нули которого определяются степенями α , где α — примитивный элемент поля $\mathbb{F}_2[x]/(x^4 + x + 1)$.

Пусть для некоторого принятого слова $w(x)$ полином локаторов ошибок $\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$.

Требуется *определить позиции ошибок* в $w(x)$.

Решение

Найдём корни полинома локаторов ошибок полным перебором.

Для вычислений будем пользоваться таблицей соответствий между степенным и полиномиальным представлением элементов поля, вычисленной в предыдущей задаче ТК-4.

Задача ТК-5... ($\alpha^4 = \alpha + 1$)

$$\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$$

$$\sigma(\alpha) = \alpha^4 + \alpha^7 + 1 = \alpha^3 + 1,$$

$$\sigma(\alpha^2) = \alpha^6 + \alpha^8 + 1 = \alpha^3,$$

$$\sigma(\alpha^3) = \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,$$

$$\sigma(\alpha^4) = \alpha^{10} + \alpha^{10} + 1 = 1,$$

$$\sigma(\alpha^5) = \alpha^{12} + \alpha^{11} + 1 = 0,$$

$$\sigma(\alpha^6) = \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,$$

$$\sigma(\alpha^7) = \alpha + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,$$

$$\sigma(\alpha^8) = \alpha^3 + \alpha^{14} + 1 = 0,$$

$$\sigma(\alpha^9) = \alpha^5 + 1 + 1 = \alpha^2 + \alpha,$$

$$\sigma(\alpha^{10}) = \alpha^7 + \alpha + 1 = \alpha^3,$$

Задача ТК-5...

$$\sigma(x) = \alpha^2 x^2 + \alpha^6 x + 1$$

$$\sigma(\alpha^{11}) = \alpha^9 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,$$

$$\sigma(\alpha^{12}) = \alpha^{11} + \alpha^3 + 1 = \alpha^2 + \alpha + 1,$$

$$\sigma(\alpha^{13}) = \alpha^{13} + \alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,$$

$$\sigma(\alpha^{14}) = 1 + \alpha^5 + 1 = \alpha^2 + \alpha,$$

$$\sigma(\alpha^{15}) = \alpha^2 + \alpha^6 + 1 = \alpha^3 + 1.$$

Обратные элементы для обнаруженных корней α^5 и α^8 равны, соответственно, α^{10} и α^7 ($\alpha^{15} = 1$).

Отсюда получаем, что полином ошибок есть

$$e(x) = x^{10} + x^7.$$

Задача ТК-6

Построить БЧХ-код длины 15, исправляющий не менее 2-х ошибок.

Задача ТК-6

Построить БЧХ-код длины 15, исправляющий не менее 2-х ошибок.

Решение Имеем $q = 4$, $n = 2^4 - 1 = 15$ и $d = 5$.

Образуем поле $F = \mathbb{F}_2^4 \cong \mathbb{F}_2[x]/(a(x))$, взяв в качестве $a(x)$ неприводимый полином 4-й степени $x^4 + x + 1$ (т.е. приводим более подробное решение [примера 4 Раздела 2](#)).

Полином $a(x)$ — примитивен, т.е. является м.м. для $\alpha = x$ — генератора мультипликативной группы F^* .

Находим циклотомические классы для элементов $\alpha, \alpha^2, \alpha^3, \alpha^4$ поля F , учитывая, что $\alpha^4 = \alpha + 1$, $\alpha^{15} = 1$, $\alpha^{16} = \alpha$, $\alpha^{24} = \alpha^3$:

$$\{ \alpha, \alpha^2, \alpha^4, \alpha^8 \} \text{ и } \{ \alpha^3, \alpha^6, \alpha^9, \alpha^{12} \},$$

так что для порождающего многочлена $g(x)$ конструируемого БЧХ-кода будем иметь $g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x)$.

Задача ТК-6... $\alpha^4 = \alpha + 1$, $\alpha^{15} = 1$

Ясно, что $g_\alpha(x) = a(x) = x^4 + x + 1$.

Вычислим элементы циклотомического класса, в который входит α^3 :

$$\alpha^6 = \alpha^4 \alpha^2 = (\alpha + 1)\alpha^2 = \alpha^3 + \alpha^2,$$

$$\alpha^9 = (\alpha^4)^2 \alpha = (\alpha + 1)^2 \alpha = (\alpha^2 + 1)\alpha = \alpha^3 + \alpha,$$

$$\alpha^{12} = (\alpha^4)^3 = (\alpha + 1)^3 = \alpha^3 + \alpha^2 + \alpha + 1.$$

Вычислим м.м. для циклотомического класса элемента α^3 :

$$\begin{aligned} g_{\alpha^3}(x) &= \underline{(x + \alpha^3)} \cdot \underline{(x + \alpha^6)} \cdot \underline{(x + \alpha^9)} \cdot \underline{(x + \alpha^{12})} = \\ &= \underline{(x^2 + (\alpha^3 + \alpha^{12})x + \alpha^{15})} \cdot \underline{(x^2 + (\alpha^6 + \alpha^9)x + \alpha^{15})} = \\ &= (x^2 + (\alpha^2 + \alpha + 1)x + 1) \cdot (x^2 + (\alpha^2 + \alpha)x + 1) = \\ &= x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Задача ТК-6... $\alpha^4 = \alpha + 1$, $\alpha^{15} = 1$

Таким образом,

$$\begin{aligned}g(x) &= g_\alpha(x) \cdot g_{\alpha^3}(x) = (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) = \\ &= x^8 + x^7 + x^6 + x^4 + 1,\end{aligned}$$

$$\deg g(x) = m = 8, k = 15 - 8 = 7$$

и получен порождающий полином для $(15, 7, 5)$ -кода БЧХ.

Замечание. Ранее было установлено, что имеется всего 3 неприводимых многочлена 4-го порядка. Один из них выбран в качестве $a(x) = g_\alpha(x)$ и поэтому м.м. для α^3 может быть один из двух остальных: $x^4 + x^3 + 1$ или $x^4 + x^3 + x^2 + x + 1$. Убеждаемся, что подстановка $x \mapsto \alpha^3$ обращает первый в $\alpha^2 + 1$, а **второй** — в 0, и поэтому он и есть $g_{\alpha^3}(x)$.

Задача ТК-7

Построить 15-разрядный БЧХ-код для исправления не менее 3 ошибок.

Задача ТК-7

Построить 15-разрядный БЧХ-код для исправления не менее 3 ошибок.

Решение

Имеем $n = 15 = 2^4 - 1$, $r = 3$, $d = 7$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$, где α — примитивный элемент поля $F = \mathbb{F}_2^4$.

При разбиении F^* на циклотомические классы всегда будет присутствовать четырёхэлементный класс $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$.

Остальные рассматриваемые степени α будут входить в циклотомические классы

$$\{\alpha^3, \alpha^6, \dots\} \text{ и } \{\alpha^5, \dots\}.$$

Задача ТК-7...

Нетрудно установить, что это 4- и 2-элементные классы соответственно:

$$\{ \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9 \}, \quad (\text{т.к. } 2 \cdot 9 = 18 \equiv_{15} 3 \text{ и } \alpha^{18} = \alpha^3);$$
$$\{ \alpha^5, \alpha^{10} \}, \quad (\text{т.к. } 2 \cdot 10 = 20 \equiv_{15} 5 \text{ и } \alpha^{20} = \alpha^5).$$

Ранее были найдены неприводимые многочлены четвёртой степени над \mathbb{F}_2 :

❶ $x^4 + x + 1,$

❸ $x^4 + x^3 + x^2 + x + 1,$

❷ $x^4 + x^3 + 1,$

Первые два многочлена — **примитивные** (их корень α будет генератором мультипликативной группы соответствующего поля).

Задача ТК-7...

С другой стороны, многочлен №3 не примитивный, т.к. порядок его корня α равен 5: при условии $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$ имеем

$$\begin{aligned}\alpha^5 &= \alpha\alpha^4 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \\ &= \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha = 1.\end{aligned}$$

Это означает, в качестве порождающего поле полинома $a(x)$ могут быть выбран только какой-либо из первых двух многочленов.

Положим $a(x) = x^4 + x^3 + 1$ (многочлен №2) и тогда $g_\alpha(x) = a(x)$, $\alpha^4 = \alpha^3 + 1$, $\alpha^{15} = 1$.

Далее, сразу ясно, что м.м. для элемента α^5 (и α^{10}) будет единственный неприводимый полином 2-й степени —

$$g_{\alpha^5}(x) = x^2 + x + 1.$$

Задача ТК-7... ($\alpha^4 = \alpha^3 + 1$, $\alpha^{15} = 1$)

Осталось определить м.м. для α^3 (и всего его четырёхэлементного циклотомического класса) — им должен быть либо многочлен №1, либо многочлен №3.

Подстановка в [многочлен №1](#) даёт

$$\begin{aligned} (x^4 + x + 1)|_{x=\alpha^3} &= \alpha^{12} + \alpha^3 + 1 = (\alpha^3 + 1)^3 + \alpha^3 + 1 = \\ &= (\alpha^3 + 1)((\alpha^3 + 1)^2 + 1) = \alpha^4(\alpha^6 + \cancel{1} + \cancel{1}) = \alpha^{10} \neq 0. \end{aligned}$$

Поэтому (можно не проверять) м.м. элемента α^3 будет оставшийся [многочлен №3](#) и

$$\begin{aligned} g(x) &= g_\alpha(x) \cdot g_{\alpha^3}(x) \cdot g_{\alpha^5}(x) = \\ &= (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ &= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1, \quad m = 10, k = 5. \end{aligned}$$

В результате построен БЧХ (15, 5)-код с порождающим полиномом $g(x)$, уже полученный ранее в [Разделе 2](#).

Задача ТК-8

Построить 31-разрядный БЧХ-код для исправления не менее 3 ошибок.

Задача ТК-8

Построить 31-разрядный БЧХ-код для исправления не менее 3 ошибок.

Решение

Имеем $n = 31 = 2^5 - 1$, $r = 3$, $d = 7$.

Порождающий многочлен $g(x)$ конструируемого кода должен иметь корни $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$, где α — примитивный элемент поля $F = \mathbb{F}_2^5$.

При разбиении F^* на циклотомические классы всегда будет присутствовать пятиэлементный класс $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$.
Остальные рассматриваемые степени α будут входить в циклотомические классы

$$\{\alpha^3, \alpha^6, \dots\} \text{ и } \{\alpha^5, \dots\}.$$

Задача ТК-8...

Нетрудно установить, что эти классы также будут пятиэлементными:

$$\{ \alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48} = \alpha^{17} \}, \quad (\text{т.к. } 34 \equiv_{31} 3);$$
$$\{ \alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40} = \alpha^9, \alpha^{18} \}, \quad (\text{т.к. } 36 \equiv_{31} 5).$$

По специальным таблицам*) найдём неприводимые многочлены пятой степени над \mathbb{F}_2 : их шесть —

$$\textcircled{1} \quad x^5 + x^2 + 1,$$

$$\textcircled{2} \quad x^5 + x^3 + 1,$$

$$\textcircled{3} \quad x^5 + x^3 + x^2 + x + 1,$$

$$\textcircled{4} \quad x^5 + x^4 + x^2 + x + 1,$$

$$\textcircled{5} \quad x^5 + x^4 + x^3 + x + 1,$$

$$\textcircled{6} \quad x^5 + x^4 + x^3 + x^2 + 1.$$

*) из списка литературы см., например, монографию
Лидл Р., Нидеррайтер Г. Конечные поля (Том 1, Таблица С).

Задача ТК-8...

Все эти многочлены являются примитивными (их корень $\alpha = x$ будет генератором мультипликативной группы соответствующего поля) и все они могут быть выбраны в качестве порождающего поле полинома $a(x)$.

Положим $a(x) = x^5 + x^3 + 1$ (многочлен №2).

Тогда $g_\alpha(x) = a(x)$, $\alpha^5 = \alpha^3 + 1$, $\alpha^{31} = 1$.

Определим, какие из остальных многочленов соответствуют циклотомическим классам для α^3 и α^5 .

Имеем:

для многочлена №3 —

$$\begin{aligned}(x^5 + x^3 + x^2 + x + 1)|_{x=\alpha^3} &= \alpha^{15} + \alpha^9 + \alpha^6 + \alpha^3 + 1 = \\ &= (\alpha^3 + 1)^3 + \alpha^4(\alpha^3 + 1) + \alpha(\alpha^3 + 1) + \alpha^3 + 1 = \dots = 0,\end{aligned}$$

Задача ТК-8...

для многочлена №5 —

$$\begin{aligned} (x^5 + x^4 + x^3 + x + 1) \Big|_{x=\alpha^5} &= \alpha^{25} + \alpha^{20} + \alpha^{15} + \alpha^5 + 1 = \\ &= (\alpha^3 + 1)^5 + (\alpha^3 + 1)^4 + (\alpha^3 + 1)^3 + \alpha^5 + 1 = \dots = 0. \end{aligned}$$

Таким образом, $g_{\alpha^3}(x) = x^5 + x^3 + x^2 + x + 1$,
 $g_{\alpha^5}(x) = x^5 + x^4 + x^3 + x + 1$ (совпадение номеров
 многочленов со степенями генератора случайно) и

$$\begin{aligned} g(x) &= g_{\alpha}(x) \cdot g_{\alpha^3}(x) \cdot g_{\alpha^5}(x) = \\ &= x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1. \end{aligned}$$

Имеем $\deg g(x) = m = 15$, $k = n - m = 16$ и порождающий
 многочлен для (31, 16)-кода БЧХ, исправляющего не менее 3
 ошибок, построен.