Часть II

Коды, исправляющие ошибки

Разделы I

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. входящий поток информации разбить на *сообщения* — непересекающиеся блоки фиксированной длины k;
2. каждый блок кодировать —

   а) либо независимо от других — *блоковое кодирование*;

   б) либо в зависимости от предыдущих — *свёрточное кодирование* (турбо-коды и др.).

Задачи блокового кодирования

Далее рассматривается исключительно **блоковое кодирование**.

- Есть набор *сообщений* $S_1, \ldots, S_t$, длины k каждое, которые нужно передать по каналу связи с шумом.
- Для обеспечения помехозащишённости вместо этих сообщений передают блоки длины $n > k$ каждое — *кодовые слова*.

Задачи блокового кодирования

Далее рассматривается исключительно **блоковое кодирование**.

- Есть набор *сообщений* $S_1, \ldots, S_t$, длины k каждое, которые нужно передать по каналу связи с шумом.
- Для обеспечения помехозащишённости вместо этих сообщений передают блоки длины $n > k$ каждое — *кодовые слова*.

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

Задачи блокового кодирования

Далее рассматривается исключительно **блоковое кодирование**.

- Есть набор *сообщений* $S_1, \ldots, S_t$, длины k каждое, которые нужно передать по каналу связи с шумом.
- Для обеспечения помехозащишённости вместо этих сообщений передают блоки длины $n > k$ каждое — *кодовые слова*.

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, $\ldots$);
- r — максимальное количество исправимых ошибок.

Требуется построить код, максимизирующий число t сообщений, которое можно передать.

Некоторые понятия, связанные с булевым кубом

Решаем вспомогательную задачу — она проще.

Напоминание из дискретной математики

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

$$\rho(\widetilde{\alpha},\, \widetilde{\beta}) \;=\; \left\|\widetilde{\alpha} \oplus \widetilde{\beta}\right\|.$$

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

$$S_r(\widetilde{\alpha}) \;\stackrel{\text{def}}{=}\; \left\{ \widetilde{\beta} \in B^n \;\mid\; \rho(\widetilde{\alpha}, \widetilde{\beta}) \leqslant r \right\}.$$

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.

В его честь 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

Определение

Минимальное расстояние между словами кода называется *кодовым расстоянием*, символически d.

Утверждение

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

Кодовое расстояние

Определение

Минимальное расстояние между словами кода называется *кодовым расстоянием*, символически d.

Утверждение

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

Доказательство

Если при передаче сообщения $\widetilde{\alpha}$ сделано не более r ошибок, то набор останется в шаре $S_r(\widetilde{\alpha})$.
Если шары не пересекаются, то искомое кодовое слово α — ближайшее к полученному набору.

Кодовое расстояние...

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 — обратное преобразование.

Блоковое кодирование и декодирование: определения и тривиальный пример

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

Декодирование — обратное преобразование.

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

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

$$0 \mapsto 000 \qquad 1 \mapsto 111$$

исправляет одну ошибку!
Однако такое кодирование (выбор $k = 1$) крайне неэффективно: длина сообщения утраивается.

Блоковое кодирование: обозначения и определения

Обозначим одно сообщение длины k вектором-столбцом (**полужирный шрифт**) $\boldsymbol{u} \in \{0,1\}^k$:

$$\boldsymbol{u} = \begin{bmatrix} u_1 \\ \dots \\ u_k \end{bmatrix},$$

содержащим *информационные биты* $u_1, \dots, u_k$.

Определение

- $\boldsymbol{v}$ — кодовое слово длины $n = k + m$, содержащее помимо k информационных, m *проверочных бит*;
- Множество $\{\boldsymbol{v}_1, \dots, \boldsymbol{v}_{2^k}\}$ всех 2^k кодовых слов длины n — *(n,k)-код* (иногда указывают кодовое расстояние и пишут *(n,k,d)-код*);
- $R = k/n$ — скорость, $m/n = 1 - R$ — избыточность кода.

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

Блоковое кодирование не вызывает принципиальных трудностей: отображение $S \to C$ всегда может быть осуществлено с использованием таблицы размера $2^k \times n$ (что, однако, весьма неэффективно).

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

Блоковое кодирование не вызывает принципиальных трудностей: отображение $S \to C$ всегда может быть осуществлено с использованием таблицы размера $2^k \times n$ (что, однако, весьма неэффективно).

При передаче по каналу с шумом кодовое слово $\boldsymbol{v}$ превращается в принятое слово $\boldsymbol{w}$ той же длины n:

$$\boldsymbol{v} \to \boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}\,.$$

Здесь $\boldsymbol{e} \in \{0,1\}^n$ — *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 исправить не менее $[\,(d-1)/2\,]$ ошибок.

Блоковый (n, k) код: декодирование

Декодирование любых кодов всегда значительно сложнее кодирования.

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

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

Блоковый (n, k) код: два этапа декодирования

1-й этап: Восстановление переданного кодового слова $\widehat{\boldsymbol{v}}$ — как ближайшего к $\boldsymbol{w}$ в метрике Хэмминга, т.е. 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 (кодового слова) превышает величину $r = [\,(d-1)/2\,]$, то при передаче произошло больше ошибок, чем может исправить код и алгоритм декодирования должен выдать отказ.

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

Блоковое кодирование: общая схема и сложность

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

Блоковое кодирование: общая схема и сложность

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

Из приведённых оценок следует: использование произвольного (n, k)-блокового кода возможно лишь при небольших значениях n и k.

Блоковое кодирование: общая схема и сложность

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

Из приведённых оценок следует: использование произвольного (n, k)-блокового кода 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 блоковых кодов специального вида: групповых, а из групповых — циклических.

Плотная упаковка шаров в булев куб

Чтобы построить код максимального размера, исправляющий r 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 «без остатка»?

Плотная упаковка шаров в булев куб

Чтобы построить код максимального размера, исправляющий r 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 «без остатка»?

Ответ: Такое удаётся в случаях:

1. $n = 2^m - 1$, $r = 1$ — *коды Хэмминга*;
2. $n = 23$, $r = 3$ — *код Голея*.

— это *совершенные* или *экстремальные коды*.

Количество кодовых слов

Теорема (Хэмминга)

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

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}} \leqslant t \leqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}}.$$

Количество кодовых слов

Теорема (Хэмминга)

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

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}} \leqslant t \leqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}}.$$

Доказательство

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

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

Продолжение доказательства

Для оценки снизу построим 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* $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2r}$ *точек* $\Rightarrow$ *шаров не менее*

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

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

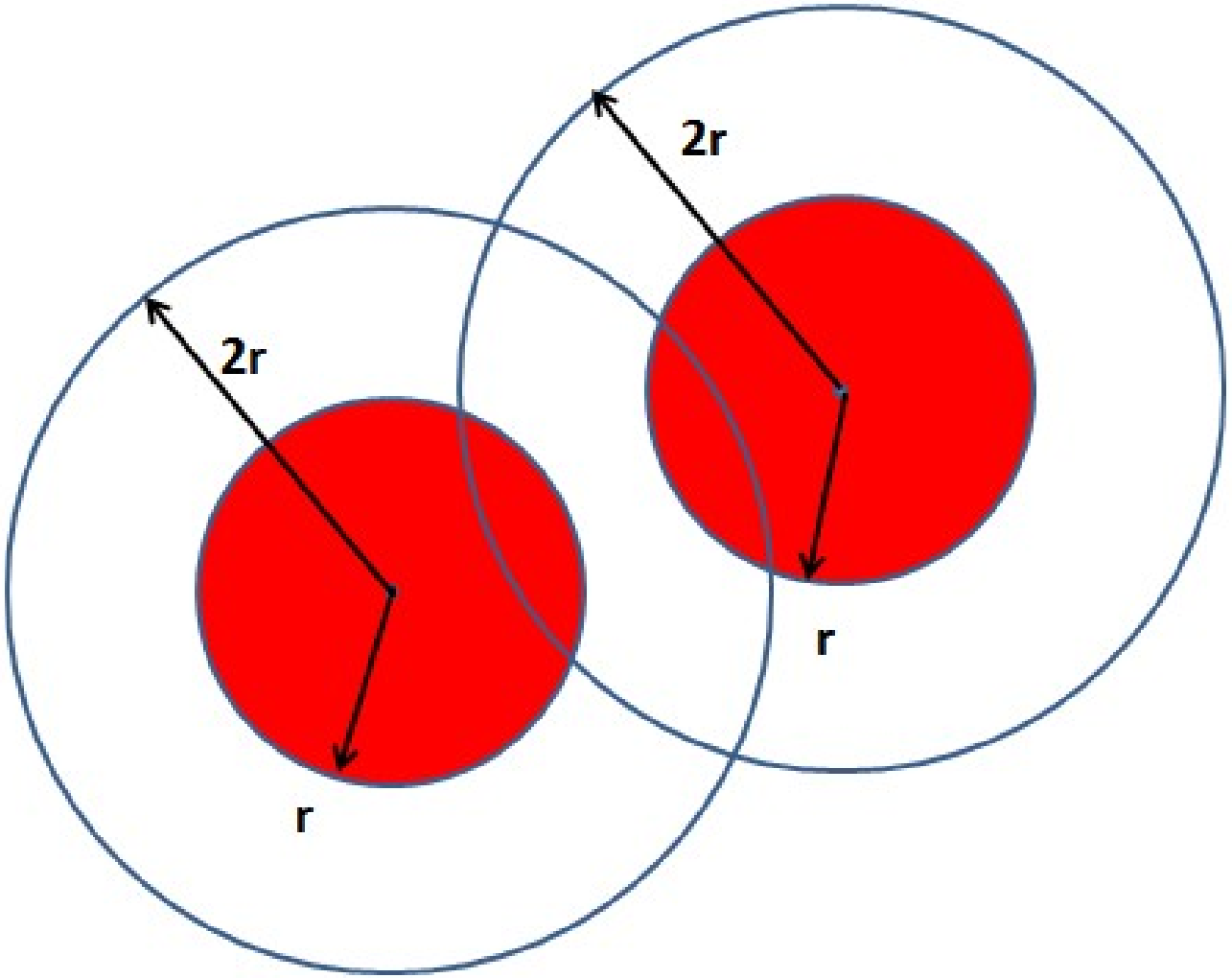


Рис. 1. К теореме Хэмминга

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:

$$\left.\begin{array}{ll} 100\ldots000 & 1100\ldots000 \\ 010\ldots000 & 1010\ldots000 \\ 001\ldots000 & 1001\ldots000 \\ \ldots & \ldots \\ 000\ldots100 & 1111\ldots101 \\ 000\ldots010 & 1111\ldots110 \\ 000\ldots001 & 1111\ldots111 \end{array}\right\} k = 2^m - (m+1)$$

$$\underbrace{\qquad\qquad}_{k = 2^m - (m+1)} \quad \underbrace{\qquad\qquad}_{m}$$

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–кодовых 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–кодовых 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: если сложить

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

не менее трёх строк — в левой части будет не менее трех единиц,

т.е. всегда $\rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) \geqslant 3 \Rightarrow$ шары единичного радиуса с центрами в полученных наборах не пересекаются.

Код Хэмминга длины 7

Пример

Выбирем $m = 3$, тогда $n = 2^3 - 1 = 7$, $k = 7 - 3 = 4$ и 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 $\mathrm{mod}\,2$ все совокупности данных 4-х строк (включая пустую), получаем $2^4 = 16 = 2^7/(1+7)$ различных бинарных наборов, которыми можно закодировать 16 сообщений: например,

$$10 \text{ цифр} \,\big|\, \text{разделитель} \,\big|\, = \,\big|\, + \,\big|\, - \,\big|\, \times \,\big|\, \div .$$

Код Хэмминга длины 7

Пример

Выбирем $m = 3$, тогда $n = 2^3 - 1 = 7$, $k = 7 - 3 = 4$ и 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 $\bmod 2$ все совокупности данных 4-х строк (включая пустую), получаем $2^4 = 16 = 2^7/(1+7)$ различных бинарных наборов, которыми можно закодировать 16 сообщений: например,

$$10 \text{ цифр} \,|\, \text{разделитель} \,|\, = \,|\, + \,|\, - \,|\, \times \,|\, \div .$$

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

Код Голея — $(23, 12, 7)$-код

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

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

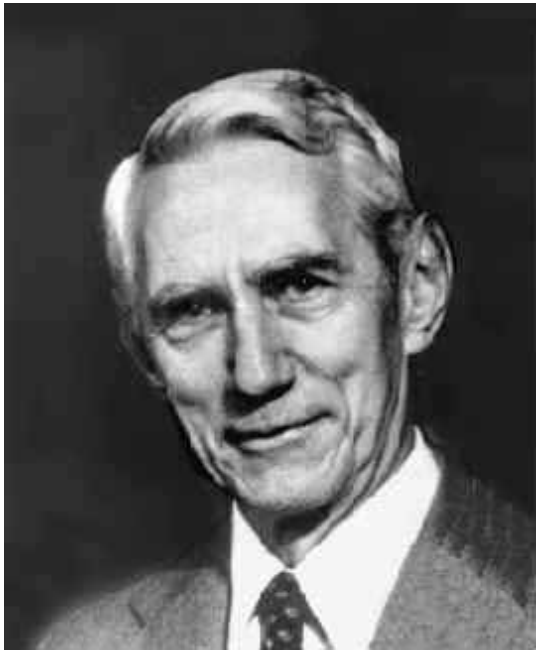
также достигается — имеем плотную упаковку, как и в кодах Хэмминга.

Других пар (n, r), удовлетворяющих условию

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

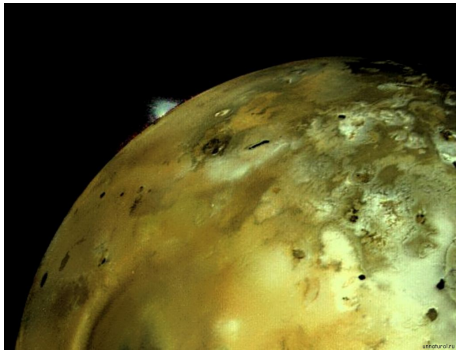
неизвестно (а если таковые и есть, то у них $n \gg 1$ и такой код не представляет практического интереса).

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 1949 г. по теории информации 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*
$$t(n,\ d) \leqslant 2\left[\frac{d}{2d-n}\right];$$
2. *нечётно и* $2d+1 > n$, *то*
$$t(n,\ d) \leqslant 2\left[\frac{d+1}{2d+1-n}\right].$$

Существуют коды, для которых граница Плоткина достигается.

Разделы I

Разделы

Групповые коды: определение

Бóльшая часть теории блокового кодирования построена на *линейных* или *групповых* кодах, образующих группу относительно $\oplus$ (двоичные коды) и позволяющих реализовывать эффективные алгоритмы кодирования/декодирования.

Утверждение

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

Групповые коды: определение

Бóльшая часть теории блокового кодирования построена на *линейных* или *групповых* кодах, образующих группу относительно $\oplus$ (двоичные коды) и позволяющих реализовывать эффективные алгоритмы кодирования/декодирования.

Утверждение

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

Доказательство

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

Ассоциативность: *свойство операции* $\oplus$;

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

Противоположные элементы: $-\widetilde{\alpha} = \widetilde{\alpha}$ — *см. выше.*

Свойство кодового расстояния линейного кода

Теорема

Кодовое расстояние d *линейного кода* C *равно*

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

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

Свойство кодового расстояния линейного кода

Теорема

Кодовое расстояние d *линейного кода* C *равно*

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

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

Доказательство

Для произвольных кодовых слов $\widetilde{\alpha}$ *и* $\widetilde{\beta}$ *всегда существует их сумма — кодовое слово* γ: $\rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) = \left\|\widetilde{\alpha} \oplus \widetilde{\beta}\right\| = \|\widetilde{\gamma}\|$,

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

Отсюда получаем оценку $\min\limits_{\widetilde{\alpha} \neq \widetilde{\beta}} \rho\left(\widetilde{\alpha}, \widetilde{\beta}\right) \geqslant \min\limits_{\widetilde{\gamma} \neq \widetilde{0}} \|\widetilde{\gamma}\|$.

Эта оценка достигается, например, при $\widetilde{\beta} = \widetilde{0}$.

Характеристики кода Хэмминга:

- исправляет одну ошибку;
- избыточность — $\dfrac{m}{2^m - 1}$;
- 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

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

Определение

Блоковый (n,k)-код C называется *линейным* (то же, что и групповым в двоичном случае), если он образует линейное подпространство размерности k координатного пространства $\{0,1\}^n$.

Линейные коды

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

Определение

Блоковый (n,k)-код C называется *линейным* (то же, что и групповым в двоичном случае), если он образует линейное подпространство размерности k координатного пространства $\{0,1\}^n$.

Это означает, что в линейном коде C —

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

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

Элемент линейного кода: матричное представление

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

— *порождающая матрица* кода.

Элемент линейного кода: матричное представление

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

— *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:

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

Разделы

Линейные коды: кодирование

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

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 ($\widehat{\boldsymbol{v}} \to \widehat{\boldsymbol{u}}$, 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:

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

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

Ортогональное дополнение к подпространству кода

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

пространство	$\{0,1\}^n$	$=$	C	$+$	$C^\perp$
$\dim$	n		k		$m = n - k$

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

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

($\boldsymbol{v}^T$ — транспонированный вектор $\boldsymbol{v}$).

Линейные коды: проверочная матрица

Определение

Пусть $\{ \boldsymbol{h}_0, \ldots, \boldsymbol{h}_{m-1} \} \in \{0,1\}^n$ — базис $C^\perp$. Тогда матрица

$$H_{m\times n} = \begin{bmatrix} \boldsymbol{h}_0^T \\ \boldsymbol{h}_1^T \\ \ddots \\ \boldsymbol{h}_{m-1}^T \end{bmatrix}$$

называется *проверочной матрицей* кода C.

Ясно, что

- $\forall\, \boldsymbol{v} \in C \ (H\boldsymbol{v} = \boldsymbol{0})$;
- 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

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

то проверочной матрицей H кода C будет

$$H_{m\times n} = \begin{bmatrix} P_{m\times k} & I_m \end{bmatrix}$$

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

Действительно, в этом случае

$$H\boldsymbol{v} = H\widetilde{G}\boldsymbol{u} = (P+P)\boldsymbol{u} = \mathbf{0}.$$

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 — никто не знает) и, следовательно, к увеличению количества ошибок, которые может исправить код.

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

Блоковый линейный код: пример кодирования...

1 (a). Несистематическое кодирование находим непосредственно:

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

Блоковый линейный код: пример кодирования...

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

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \xrightarrow{1\leftarrow1+2} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \widetilde{G}.$$

В последней матрице в строках $(3, 5, 1)$ стоит единичная подматрица.
Можно дальше не переставлять её строки, а просто учесть, что биты исходного сообщения последовательно перейдут в 3-й, 5-й и 1-й биты кодового слова.

Блоковый линейный код: пример кодирования...

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

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

2. Находим проверочную матрицу H, формируя матрицу $P_{3\times 3}$ из строк $\widetilde{G}$, 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-ом, 5-ом и 1-ом её столбцах соответственно,
- остальные 2-ой, 4-ый и 6-ой столбцы H должны образовывать единичную подматрицу.

В итоге получим

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

Блоковый линейный код: пример кодирования...

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

$$H \times [\, \boldsymbol{v}_1^n \, \boldsymbol{v}_2^n \, \boldsymbol{v}_1^s \, \boldsymbol{v}_2^s \,] = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} =$$

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

Блоковый линейный код: пример кодирования...

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

$$[\boldsymbol{v}_1 \ldots \boldsymbol{v}_8] = G \times [\boldsymbol{u}_1 \ldots \boldsymbol{u}_8] =$$

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

$\boldsymbol{u}_1, \ldots, \boldsymbol{u}_8$ — все 8 возможных сообщений,
$\boldsymbol{v}_1, \ldots, \boldsymbol{v}_8$ — 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

Декодирование группового кода: синдром

Определение

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

Свойства синдрома:

- $\boldsymbol{s} = \boldsymbol{0} \Leftrightarrow \boldsymbol{w}$ — кодовое слово;
- $\boldsymbol{s} = H\boldsymbol{w} = H(\boldsymbol{v} + \boldsymbol{e}) = H\boldsymbol{v} + H\boldsymbol{e} = H\boldsymbol{e}$,
  т.е. вектор ошибок $\boldsymbol{e}$ удовлетворяет системе линейных уравнений $H_{m\times n}\boldsymbol{e} = \boldsymbol{s}$.

Вычисление вектора ошибок по синдрому

Решение СЛАУ

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

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

Подставляя его в $(*)$, получим

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

где

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

Ясно, что $G\boldsymbol{u} \in \{0,1\}^n$ — некоторое решение однородной системы $H\boldsymbol{x} = \boldsymbol{0}$.

Групповые коды: общая схема декодирования

После нахождения частного решения $\widehat{e}$, все возможные кодовые слова $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{2^k}$ входного вектора дадут 2^k вариантов вектора $\boldsymbol{e}_i = \widehat{\boldsymbol{e}} + G\boldsymbol{u}_i$.
Решение с наименьшим хэммингов весом $\|\boldsymbol{e}_i\|$ дает искомый вектор ошибок.

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

Схема декодирования:

$$\boldsymbol{w} \longrightarrow \boldsymbol{s} = H\boldsymbol{w} \xrightarrow[H\boldsymbol{e}=\boldsymbol{s}]{} \boldsymbol{e} = \widehat{\boldsymbol{e}} + G\boldsymbol{u} \xrightarrow[\|\boldsymbol{e}\|\to\min]{} \widehat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e}$$

Для каждого из 2^m синдромов необходимо перебирать 2^k решений очередной СЛАУ — 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 $\boldsymbol{u} = [0\ 1\ 1]^T$.
Систематическое кодирование для него было получено раньше:

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

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

Декодирование

1. Найдём синдром принятого сообщения $\boldsymbol{w}$:

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

Декодирование линейного кода: пример...

2. Находим все решения системы $H\boldsymbol{e} = \boldsymbol{s}$.

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

2.a Все решения однородной системы $H\boldsymbol{e} = \mathbf{0}$ уже были найдены раньше при вычислении кодового расстояния d:

$$G \times [\,\boldsymbol{u}_1\ \ldots\ \boldsymbol{u}_8\,] = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Декодирование линейного кода: пример...

Таким образом, все 8 решений системы $H\boldsymbol{e} = \boldsymbol{s}$ записываются как сумма вектора $\widehat{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$ со всеми столбцами матрицы $G \times [\,\boldsymbol{u}_1\ \ldots\ \boldsymbol{u}_8\,]$:

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

Выбираем среди них решение с наименьшим весом — это первый столбец $\boldsymbol{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$. Отсюда $\widehat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e} = [1\ 0\ 0\ 0\ 1\ 0]^T + [0\ 1\ 0\ 0\ 0\ 0]^T = [1\ 1\ 0\ 0\ 1\ 0]^T = \boldsymbol{v}$ 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

Разделы

Циклические коды: определение

Определение

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

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

Циклические коды: определение

Определение

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

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

Ранее рассматривалось и было показано:

- В кольце $\mathbb{F}_p[x]/(x^n-1)$, рассматриваемом как линейное векторное пространство над полем $\mathbb{F}_p$, имеется базис
$$\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}.$$
Циклический сдвиг координат в этом базисе равносилен умножению на x.

Циклические коды: определение

Определение

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

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

Ранее рассматривалось и было показано:

- В кольце $\mathbb{F}_p[x]/(x^n-1)$, рассматриваемом как линейное векторное пространство над полем $\mathbb{F}_p$, имеется базис
$$\left\{ \overline{1}, \overline{x}, \ldots, \overline{x^{n-1}} \right\}.$$
Циклический сдвиг координат в этом базисе равносилен умножению на x.
- Теорема: *Линейное подпространство* $I \subseteq \mathbb{F}_p[x]/(x^n-1)$ *является циклическим iff* $I \lhd \mathbb{F}_p[x]/(x^n-1)$.

Циклические коды: идея построения

Поэтому построить двоичный циклический код можно так:

1. выбираем некоторый делитель $g(x)$ многочлена $x^n + 1$. Многочлен $g(x)$ называют *порождающим* или образующим.
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 $g(x)$ многочлена $x^n + 1$. Многочлен $g(x)$ называют *порождающим* или образующим.
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.

Линейные циклические коды

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

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

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

Тогда свойство главного идеала переформулируется:
для каждого (n, k)-циклического кода найдется порождающий полином $g(x)$ такой, что

1. $g(x) \,\big|\, x^n + 1$;
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

Циклические коды: кодирование

Пусть задан порождающий полином $g(x)$ степени m (это число 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 (это число 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: $v(x) = g(x)u(x)$.

В порождающей матрице $G_{n\times k} = [\boldsymbol{g}_0 \dots \boldsymbol{g}_{k-1}]$ данного кода базисные векторы $\boldsymbol{g}_i$ соответствуют полиномам $x^i g(x)$, $i = \overline{0, k-1}$.

Циклические коды: систематическое кодирование...

Систематическое кодирование

Образуем полином $x^m u(x)$ (степени $m+k-1=n-1$) и поделим его на $g(x)$ с остатком:

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

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

и систематическое кодирование может быть задано как

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

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

В порождающей матрице $G_{n\times k} = [\boldsymbol{g}_0 \dots \boldsymbol{g}_{k-1}]$ данного кода базисные векторы $\boldsymbol{g}_i$ 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 $\mathbb{F}_2[x]/\left(x^7 + 1\right)$.

Циклический код: пример кодирования

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

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 смежные корни вида β^2, β^{2^2}, ...;
- если f приводим, то имеется несколько серий таких смежных 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 смежные классы:

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

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

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

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 смежные классы:

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

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

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

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...

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

Циклический код: пример кодирования...

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

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 $\boldsymbol{v} = [0010111]$ $(n = 7)$.

Циклический код: пример кодирования...

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

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 $\boldsymbol{v} = [0010111]$ $(n = 7)$.

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

или в векторном представлении $\boldsymbol{v} = [0100011]$ $(n = 7)$.

Мы видим, что биты входного сообщения $\boldsymbol{u}$ воспроизводятся в крайних правых битах кодового слова $\boldsymbol{v}$.

Циклический код: пример кодирования...

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

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 $\boldsymbol{v} = [0010111]$ $(n = 7)$.

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

или в векторном представлении $\boldsymbol{v} = [0100011]$ $(n = 7)$.

Мы видим, что биты входного сообщения $\boldsymbol{u}$ воспроизводятся в крайних правых битах кодового слова $\boldsymbol{v}$.
(Декодировать $\boldsymbol{v}$ с одной ошибкой будем при рассмотрении БЧХ-кодов.)

Циклические коды: декодирование

Определение

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

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;
- $0 \leqslant \deg s(x) < m = n - k$;
- $s(x) \equiv_{g(x)} v(x) + e(x) \equiv_{g(x)} e(x) \equiv_{x^n+1} w(x)h(x)$.

Циклические коды: декодирование... и свойства

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 $k-1$;
3. определяется полином ошибок как решение с минимальным числом ненулевых слагаемых;
4. восстанавливается переданное сообщение $u(x) = w(x) + e(x)$.

Циклические групповое коды (n, k): резюме

- Циклические коды — подкласс групповых.
- Кодирование производится с помощью порождающего полинома, являющийся делителем многочлена $x^n + 1$. При этом:
  - для задания циклических кодов достаточно указать порождающий полином;
  - выбор делителя, порождающего код с большим кодовым расстоянием — сложная задача.
- Декодирование осуществляется с помощью вычисляемого синдрома принятого полинома, в результате:
  - вместо умножения матриц на векторы и решение СЛАУ (как в линейных кодах общего вида) используются более простые операции умножения полиномов и их деления с остатком;
  - однако общий алгоритм декодирования по-прежнему имеет экспоненциальную сложность по k.

Разделы I

Разделы

Коды БЧХ

Рассматриваемый далее способ построения «хорошего» кода, исправляющего «много» ошибок предложили Р.Ч. Боуз и Д.К. Рей-Чоудхури в 1960 г. независимо от на год ранее опубликованной работы А. Хоквингема.

Они называются *кодами Боуза-Чоудхури-Хоквингема* или *БЧХ-кодами* (BCH, Bose-Chaudhuri-Hocquenghem) — это класс циклических кодов, исправляющих кратные (2 и более, $d \geqslant 5$) ошибки.

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.

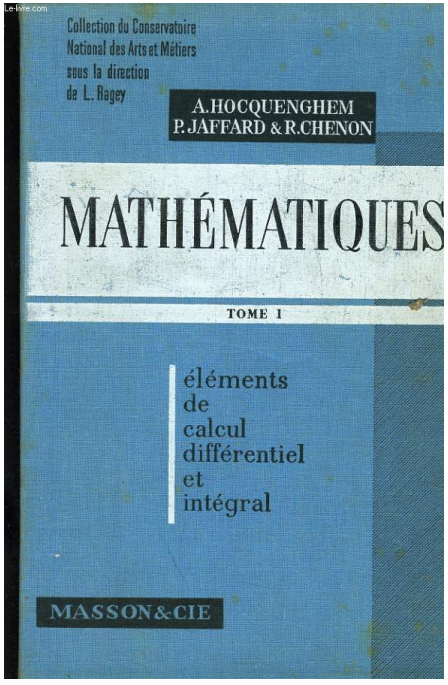
Коды Хэмминга — частный случай БЧХ-кодов.

Р.Ч. Боуз и Д.К. Рей-Чоудхури

Радж Чандра Боуз
(Raj Chandra Bose, 1901–1987) — индийский математик, работавший в США. Известен работой (в соавторстве), опровергающей гипотезу Л.Эйлера о несуществовании двух взаимно ортогональных латинских квадратов порядка $2n+2$ для любого натурального n.

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.

А. Хоквингем



Алексис Хоквингем
(Alexis Hocquenghem, 1908?–1990) — французский математик.
В его работе 1959 г. содержится первое описание линейных циклических кодов, исправляющих кратные ошибки.

Правильное чтение его фамилии — *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 $\deg m_\beta(x) = b \leqslant n$;
2. Если $\mathbb{F}_p^n = \mathbb{F}_p[x]/(a(x))$, то $a_n^{-1}a(x)$ — м.м. для $\overline{x}$;
3. $f(\beta) = 0 \ \Rightarrow\ f(x) \vdots m_\beta(x)$;
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

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

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

Циклотомический смежный класс элемента поля

Определение

Пусть $n \leqslant N$.

Циклотомическим классом (или *классом смежности*) над полем $\mathbb{F}_p^n$, порождённым элементом $\alpha \in \mathbb{F}_p^N$ называется множество всех различных элементов $\mathbb{F}_p^N$, являющихся p^n-ыми степенями α.

Циклотомический смежный класс элемента поля

Определение

Пусть $n \leqslant N$.
Циклотомическим классом (или *классом смежности*) над полем $\mathbb{F}_p^n$, порождённым элементом $\alpha \in \mathbb{F}_p^N$ называется множество всех различных элементов $\mathbb{F}_p^N$, являющихся p^n-ыми степенями α.

Свойства циклотомических классов

- Циклотомические классы смежности различных элементов либо совпадают, либо не пересекаются.
  Т.е. совокупность всех циклотомических классов поля $\mathbb{F}_p^N$ образует его разбиение его мультипликативной группы.

Свойства циклотомических классов...

- Если α — примитивный элемент поля $\mathbb{F}_p^{mn}$, то его циклотомический класс $\left\{ \alpha, \alpha^{p^n}, \alpha^{p^{2n}} \ldots, \alpha^{p^{(m-1)n}} \right\}$ над полем $\mathbb{F}_p^n$ содержит ровно m элементов.

Свойства циклотомических классов...

- Если α — примитивный элемент поля $\mathbb{F}_p^{mn}$, то его циклотомический класс $\left\{ \alpha, \alpha^{p^n}, \alpha^{p^{2n}} \ldots, \alpha^{p^{(m-1)n}} \right\}$ над полем $\mathbb{F}_p^n$ содержит ровно m элементов.

Примеры ($p = 2$: разложения мультипликативных групп полей $\mathbb{F}_2^{mn}$ на циклотомические классы над $\mathbb{F}_2^n$)

1. $n = 1, m = 3$ и α — примитивный элемент $\mathbb{F}_2^3$.
   Тогда $\alpha^7 = 1$ и рассматриваемое разложение над $\mathbb{F}_2$ есть
   $$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5\}.$$

Свойства циклотомических классов...

- Если α — примитивный элемент поля $\mathbb{F}_p^{mn}$, то его циклотомический класс $\left\{ \alpha, \alpha^{p^n}, \alpha^{p^{2n}} \ldots, \alpha^{p^{(m-1)n}} \right\}$ над полем $\mathbb{F}_p^n$ содержит ровно m элементов.

Примеры ($p = 2$: разложения мультипликативных групп полей $\mathbb{F}_2^{mn}$ на циклотомические классы над $\mathbb{F}_2^n$)

1. $n = 1, m = 3$ и α — примитивный элемент $\mathbb{F}_2^3$.
   Тогда $\alpha^7 = 1$ и рассматриваемое разложение над $\mathbb{F}_2$ есть
   $$\{1\}, \{\alpha, \alpha^2, \alpha^4\}, \{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5\}.$$
2. $n = 2, m = 2$ и α — примитивный элемент $\mathbb{F}_2^4$.
   Тогда $\alpha^{15} = 1$ и рассматриваемое разложение 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...

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

$$g(x) = \prod_{i=0}^{m-1} (x + \alpha^{2^i}) = x^{m-1} + \lambda_{m-2} x^{m-2} + \ldots + \lambda_1 x + \lambda_0$$

является м.м. α (а также для всех элементов, входящих в его циклотомический класс смежности).

Свойства циклотомических классов...

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

$$g(x) = \prod_{i=0}^{m-1} (x + \alpha^{2^i}) = x^{m-1} + \lambda_{m-2} x^{m-2} + \ldots + \lambda_1 x + \lambda_0$$

является м.м. α (а также для всех элементов, входящих в его циклотомический класс смежности).

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 многочленов $x + \alpha^{2^i}$ 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 дли́ны (есть способ обойти это ограничение — использование т.н. *укороченных кодов БЧХ*, которые мы не рассматриваем).

БЧХ-коды: построение (в простейшем случае)

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

Код БЧХ есть циклический (n, k)-код, в котором порождающий многочлен $g(x)$ имеет корнями элементы $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{d-1}$ поля $F = \mathbb{F}_2^q$ (называемые *нулями БЧХ-кода*), 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 произведение полиномов, соответствующих всем циклотомическим классам, в которые попали нули БЧХ-кода (или как НОК их м.м.);
- кодовое расстояние построенного кода оказывается не менее выбранного конструктивного расстояния d.

БЧХ-код: кодовое расстояние не менее конструктивного

Теорема

Пусть БЧХ-код длиной $n = 2^q - 1$ *задаётся кодирующим многочленом*

$$g(x) = HOK\left(m_1(x), \ldots, m_{d-1}(x)\right),$$

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

Тогда кодовое расстояние данного БЧХ-кода не менее d.

Доказательство

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

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

$$g(x) = b_1 x^{n_1} + b_2 x^{n_2} + \ldots + b_{d-1} x^{n_{d-1}}.$$

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

Поскольку $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ — корни $g(x)$, его коэффициенты $b_1, \ldots, b_{d-1}$ удовлетворяют линейной системе

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

Матрица A коэффициентов 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, $b_1 = \ldots = b_{d-1} = 0$ — противоречие.

Коды БЧХ: синдромы

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

Построение кодов БЧХ: пример для $q = 3$, $n = 2^3 - 1 = 7$

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 неприводимый многочлен $a(x) = x^3 + x + 1$.

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

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

Построение кодов БЧХ: пример для $q = 3$, $n = 2^3 - 1 = 7$

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 неприводимый многочлен $a(x) = x^3 + x + 1$.

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

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

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

Тогда $d - 1 = 2r = 2$ и элементы α, α^2 попадают в один циклотомический класс.
Минимальный многочлен для элементов этого класса — $a(x)$.
Поэтому порождающий полином $g(x) = a(x)$,
$m = \deg a(x) = 3$ и в результате получаем уже известный $(7, 4, 3)$-код.

Построение кодов БЧХ: пример для $q = 3$, $n = 2^3 - 1 = 7$...

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 α, α^2, α^3, α^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:

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

Построение кодов БЧХ: пример для $q = 3,\ n = 7$...

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

$$\begin{aligned} \alpha^3 + \alpha^5 + \alpha^6 &= \alpha + 1 + (\alpha + 1)^2 + \alpha^2(\alpha + 1) = \\ &= \alpha + 1 + \alpha^2 + 1 + \alpha^3 + \alpha^2 = 1\,, \\ \alpha^8 + \alpha^9 + \alpha^{11} &= \alpha^2 + \alpha + \alpha^4 = \alpha^2 + \alpha + \alpha(\alpha + 1) = 0\,, \\ \alpha^{14} &= 1\,. \end{aligned}$$

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

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

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

Построение кодов БЧХ: пример для $q = 4,\ n = 15,\ d = 7$

Построим БЧХ-код длины $n = 15$, исправляющий 3 ошибки (т.е. $q = 4,\ d = 7$).

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

Пусть α — генератор F^* (т.е. $\alpha^{15} = 1,\ \alpha^4 = \alpha + 1$).
Нулями конструируемого БЧХ-кода будут $\alpha, \alpha^2, \ldots, \alpha^6$, которые попадают в циклотомические классы

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\},\ \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9 = \alpha^{24}\},\ \{\alpha^5, \alpha^{10}\}.$$

Построение кодов БЧХ: пример для $q = 4,\ n = 15,\ d = 7$

Построим БЧХ-код длины $n = 15$, исправляющий 3 ошибки (т.е. $q = 4,\ d = 7$).

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

Пусть α — генератор F^* (т.е. $\alpha^{15} = 1,\ \alpha^4 = \alpha + 1$).
Нулями конструируемого БЧХ-кода будут $\alpha, \alpha^2, \ldots, \alpha^6$, которые попадают в циклотомические классы

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\},\ \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9 = \alpha^{24}\},\ \{\alpha^5, \alpha^{10}\}.$$

Минимальные многочлены для элементов-представителей этих классов суть $g_\alpha(x) = x^4 + x + 1,\ g_{\alpha^3}(x) = x^4 + x^3 + x^2 + x + 1$ и $g_{\alpha^5}(x) = x^2 + x + 1$, а порождающим полиномом полученного $(15, 5, 7)$-кода БЧХ есть

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = \\ = x^{10} + x^8 + x^5 + x4 + x^2 + x + 1.$$

Разделы

Декодирование кода Хэмминга ($n = 2^q - 1$)

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

Декодирование кода Хэмминга ($n = 2^q - 1$)

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

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

При

$s_1 = 0$ — ошибки не произошло и $v(x) = w(x)$;

$s_1 \neq 0$ — произошли ошибки и

- если $s_1 = \alpha^j$ для некоторого $j \in \{0, \ldots, n-1\}$, то j — искомая позиция ошибки (при единичной ошибке в j-ой позиции $e(x) = x^j$) и $v(x) = w(x) + x^j$;
- иначе, произошло более одной ошибки.

Декодирование кода Хэмминга: пример

Рассматриваем $(7,4)$-код Хэмминга, построенный в примере для циклических кодов (порождающий полином $g(x) = x^3 + x + 1$).

Там было найдено систематическое кодирование входного полинома $u(x) = x^3 + x^2$: $v(x) = x^6 + x^5 + x$.

Теперь мы построили этот же код с использованием поля $F = \mathbb{F}_2[x]/\left(x^3 + x + 1\right)$. Для примитивного элемента α этого поля имеем $\alpha^7 = 1$ и $\alpha^3 = \alpha + 1$.

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

$$s_1 = w(\alpha) = \alpha^6 + \alpha = \left(\alpha^3\right)^2 + \alpha = (\alpha + 1)^2 + \alpha = \\ = \alpha^2 + \alpha + 1 \neq 0.$$

Декодирование кода Хэмминга: пример...

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

$$\alpha^0 = 1,$$
$$\alpha^1 = \alpha,$$
$$\alpha^2 = \alpha^2,$$
$$\alpha^3 = \alpha + 1,$$
$$\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha,$$
$$\alpha^5 = \alpha^2(\alpha + 1) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1 = \mathbf{s_1},$$
$$\alpha^6 \text{ — можно уже не вычислять!}$$

Отсюда следует, что ошибка произошла в позиции 5 и, таким образом, $\widehat{v}(x) = w(x) + x^5 = x^6 + x^5 + 1 = v(x)$.

Коды БЧХ: декодирование

Пусть при передаче сообщения, закодированого кодом БЧХ в поле $\mathbb{F}_2^q \cong \mathbb{F}[x]/(a(x))$ произошло ν ошибок.
Тогда $e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}$, где степени $j_1, \ldots, j_\nu$ — позиции (*локаторы*) ошибок, $\nu \leqslant r = [(d-1)/2]$.

Коды БЧХ: декодирование

Пусть при передаче сообщения, закодированого кодом БЧХ в поле $\mathbb{F}_2^q \cong \mathbb{F}[x]/(a(x))$ произошло ν ошибок.
Тогда $e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}$, где степени $j_1, \ldots, j_\nu$ — позиции (*локаторы*) ошибок, $\nu \leqslant r = [(d-1)/2]$.

Запишем равенства $s_i = w(\alpha^i) = e(\alpha^i)$, $i = \overline{1, 2r}$ как систему:

$$\begin{cases} s_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_\nu}, \\ s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_\nu})^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = (\alpha^{j_1})^{2r} + \ldots + (\alpha^{j_\nu})^{2r}. \end{cases}$$

Коды БЧХ: декодирование

Пусть при передаче сообщения, закодированого кодом БЧХ в поле $\mathbb{F}_2^q \cong \mathbb{F}[x]/(a(x))$ произошло ν ошибок.
Тогда $e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}$, где степени $j_1, \ldots, j_\nu$ — позиции (*локаторы*) ошибок, $\nu \leqslant r = [(d-1)/2]$.

Запишем равенства $s_i = w(\alpha^i) = e(\alpha^i)$, $i = \overline{1, 2r}$ как систему:

$$\begin{cases} s_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_\nu}, \\ s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_\nu})^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = (\alpha^{j_1})^{2r} + \ldots + (\alpha^{j_\nu})^{2r}. \end{cases}$$

Любое решение данной системы $(j_1, \ldots, j_\nu)$ для некоторого $\nu \leqslant r$ будет искомым (такое решение всегда существует и единственно, т.к. код по построению способен исправлять до r ошибок).

Коды БЧХ: декодирование...

Введя обозначения $\beta_i = \alpha^{j_i}$, $i = \overline{1, 2r}$, перепишем систему:

$$\begin{cases} s_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ s_2 = \beta_1^2 + \beta_2^2 + \ldots + \beta_\nu^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{2r} = \beta_1^{2r} + \beta_2^{2r} + \ldots + \beta_\nu^{2r}. \end{cases} \qquad (1)$$

Рассмотрим *полином локаторов ошибок*

$$\sigma(x) = \prod_{i=1}^{\nu}(1 + \beta_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \cdots + \sigma_\nu x^\nu,$$

корнями которого являются величины $\beta_i^{-1} = \alpha^{-j_i}$, $i = \overline{1, 2r}$.

Для продвинутых: это *производящий полином*.

Коды БЧХ: декодирование...

Связь между σ_k и β_i определяет теорема Виета:

$$\begin{cases} \sigma_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ \sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3 + \ldots + \beta_{\nu-1}\beta_\nu, \\ \sigma_3 = \sum\limits_{i_1<i_2<i_3} \beta_{i_1}\beta_{i_2}\beta_{i_3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_\nu = \beta_1\beta_2\ldots\beta_\nu. \end{cases} \qquad (2)$$

Коды БЧХ: декодирование...

Связь между σ_k и β_i определяет теорема Виета:

$$\begin{cases} \sigma_1 = \beta_1 + \beta_2 + \ldots + \beta_\nu, \\ \sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3 + \ldots + \beta_{\nu-1}\beta_\nu, \\ \sigma_3 = \sum\limits_{i_1<i_2<i_3} \beta_{i_1}\beta_{i_2}\beta_{i_3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \sigma_\nu = \beta_1\beta_2\ldots\beta_\nu. \end{cases} \qquad (2)$$

Введённые системы задают величины синдромов и коэффициентов полинома локаторов ошибок соответственно как значения симметрических полиномов:

(1) — суммы k-ых степеней β_i, $k = \overline{1, 2r}$;
(2) — элементарного.

Соотношения между этими двумя типами симметрических полиномов задаются *тождествами Ньютона-Жирара*.

Коды БЧХ: декодирование...

В двоичной арифметике тождества Ньютона-Жирара записываются как

$$
\begin{aligned}
& s_1 + \sigma_1 = 0, \\
& s_2 + \sigma_1 s_1 + 2\sigma_2 = 0, \\
& s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0, \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& s_\nu + \sigma_1 s_{\nu-1} + \ldots + \sigma_{\nu-1} s_1 + \nu\sigma_\nu = 0, \\
& s_{\nu+1} + \sigma_1 s_\nu + \ldots + \sigma_{\nu-1} s_2 + \sigma_\nu s_1 = 0, \\
& s_{\nu+2} + \sigma_1 s_{\nu+1} + \ldots + \sigma_{\nu-1} s_3 + \sigma_\nu s_2 = 0, \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
& s_{2r} + \sigma_1 s_{2r-1} + \ldots + \sigma_{\nu-1} s_{2r-\nu+1} + \sigma_\nu s_{2r-\nu} = 0.
\end{aligned}
$$

Ключевое уравнение

Коды БЧХ: декодирование...

В литературе по кодам последние $2r - \nu + 1$ уравнений данной системы получили название *ключевого уравнения* — оно является СЛАУ относительно $\sigma_1, \ldots, \sigma_\nu$.

Решение ключевого уравнения позволяет найти полином локаторов ошибок $\sigma(x)$.

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

Коды БЧХ: декодирование...

В литературе по кодам последние $2r - \nu + 1$ уравнений данной системы получили название *ключевого уравнения* — оно является СЛАУ относительно $\sigma_1, \ldots, \sigma_\nu$.

Решение ключевого уравнения позволяет найти полином локаторов ошибок $\sigma(x)$.

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

Основная трудность в решении ключевого уравнения состоит в том, что значение ν неизвестно.

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

Коды БЧХ: декодирование...

1. *Декодер PGZ (Peterson-Gorenstein-Zierler)* — состоит в последовательном решении ключевого уравнения для $\nu = r, r-1, \ldots$ 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*

$$s(x) = 1 + s_1 x + s_2 x^2 + \ldots + s_{2r} x^{2r},$$

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

Коды БЧХ: декодирование...

1. *Декодер PGZ (Peterson-Gorenstein-Zierler)* — состоит в последовательном решении ключевого уравнения для $\nu = r, r-1, \ldots$ 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*

$$s(x) = 1 + s_1 x + s_2 x^2 + \ldots + s_{2r} x^{2r},$$

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

Для продвинутых: это тоже производящий полином.

Коды БЧХ: декодирование...

Перемножим полиномы — синдромный и локаторов ошибок:

$$\lambda(x) = s(x)\sigma(x) = 1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{2r+\nu} x^{2r+\nu}.$$

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

Поскольку $\sigma_0 = 1$ ключевое уравнение эквивалентно условию $\lambda_{\nu+1} = \lambda_{\nu+2} = \ldots = \lambda_{2r} = 0$, т.е.

$$\lambda(x) = \left(1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_\nu x^\nu\right) + \left(\lambda_{2r+1} x^{2r+1} + \ldots + \lambda_{2r+\nu} x^{2r+\nu}\right).$$

Коды БЧХ: декодирование...

Перемножим полиномы — синдромный и локаторов ошибок:

$$\lambda(x) = s(x)\sigma(x) = 1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_{2r+\nu} x^{2r+\nu}.$$

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

Поскольку $\sigma_0 = 1$ ключевое уравнение эквивалентно условию $\lambda_{\nu+1} = \lambda_{\nu+2} = \ldots = \lambda_{2r} = 0$, т.е.

$$\lambda(x) = \left(1 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_\nu x^\nu\right) + \\ + \left(\lambda_{2r+1} x^{2r+1} + \ldots + \lambda_{2r+\nu} x^{2r+\nu}\right).$$

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

$$\lambda(x) \equiv_{x^{2r+1}} 1 + \lambda_1 x + \cdots + \lambda_\nu x^\nu.$$

Коды БЧХ: декодирование...

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

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

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

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

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

Коды БЧХ: декодирование...

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

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

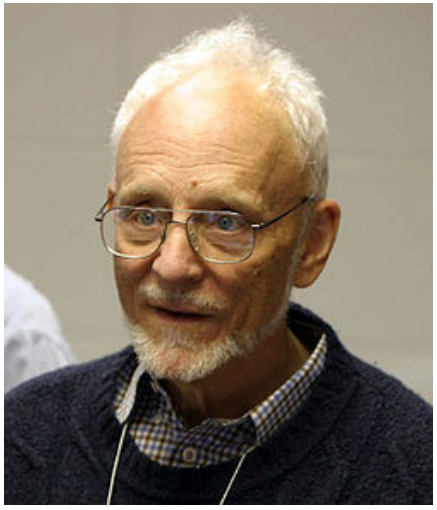
(напоминание: работаем в поле $\mathbb{F}_2^q \cong \mathbb{F}_2[x]/(a(x))$).

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

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

Замечание: наиболее эффективным декодером 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, в соавторстве разработал
шифры SAFER и IDEA).

Коды БЧХ: общая схема декодирования

Пусть принято слово $w(x)$, являющееся сообщением, закодированным БЧХ (n, k, d)-кодом и, возможно, содержащее ошибки.

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 $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$.
4. Найти позиции ошибок $j_i \equiv_n -k_i$, $i = \overline{1, \nu}$.
5. Исправить ошибки, получив слово
$$\widehat{v}(x) = w(x) + x^{j_1} + \ldots + x^{j_\nu}.$$
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 $\mathbb{F}_2^4 \cong \mathbb{F}_2[x]/\left(x^4 + x + 1\right)$.

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

При систематическом кодировании (опустим этот этап) кодовое слово есть

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

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

Пусть полином ошибок $e(x) = x^{12} + x^6 + 1 \leftrightarrow$
$$\leftrightarrow [1000001000000100],$$

тогда принятое слово —

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

Коды БЧХ: пример декодирования...

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

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	α^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}	α^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

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

Коды БЧХ: пример декодирования...

2. Выбираем декодер на базе расширенного алгоритма Евклида — решаем уравнение $x^7 a(x) + s(x)\sigma(x) = \lambda(x)$:

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

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...

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

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

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

Таким образом, полином локаторов ошибок найден:

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

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 α^3, α^9, α^{15} вычисляем позиции ошибок:

$$\begin{aligned} j_1 &= -3 \equiv_{15} 12, \\ j_2 &= -9 \equiv_{15} 6, \\ j_3 &= -15 \equiv_{15} 0. \end{aligned}$$

5. Отсюда $e(x) = x^{12} + x^6 + 1$,

$$\begin{aligned} \widehat{v}(x) &= w(x) + e(x) = \\ &= x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2 + x = v(x) \end{aligned}$$

и кодовое слово восстановлено.

6. Легко проверяется, что $\widehat{v}(\alpha) = \widehat{v}(\alpha^2) = \ldots = \widehat{v}(\alpha^6) = 0$, (т.е. восстановление верное).

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

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

В системах передачи данных широко используется двоичный $(255, 231, 15)$-код, построенный с помощью примитивного элемента $\alpha \in \mathbb{F}_2^8$ 255-го порядка:

- степень порождающего многочлена $g(x)$ — $m = n - k = 24$;
- корни $g(x)$ — α, α^2, α^3, α^4, α^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.
- Важное 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 (Берлекэмпа-Мэсси, Питерсона-Горенстейна-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, $d/n \to 0$, 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 характеризуется вектором ошибок (1 — символ ошибочен, 0 — нет) таких, что первый и последний из них отличны от нуля.

Коды Рида–Соломона:

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

Разделы I

Задача ТК-1

Линейный код задан своей проверочной матрицей

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

Требуется

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

$$\boldsymbol{u}_1 = [110]^T,\ \boldsymbol{u}_2 = [101]^T.$$

Задача ТК-1...

Решение

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_3 \end{bmatrix}$, где I_3 — единичная матрица порядка размера 3.

Задача ТК-1...

Решение

Порождающая матрица кода G, обеспечивающая требуемое систематическое кодирование, должна иметь вид $\begin{bmatrix} P \\ I_3 \end{bmatrix}$, где I_3 — единичная матрица порядка размера 3.

Матрицу P можно получить, если привести проверочную матрицу H к виду $\begin{bmatrix} I_3 & P \end{bmatrix}$, т.е. с помощью эквивалентных преобразований строк выделить в первых трех колонках единичную матрицу:

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \xrightarrow{1 \leftrightarrow 3} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1 \leftarrow 1+2}$$

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \xrightarrow{1 \leftarrow 1+3} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Задача ТК-1...

Теперь можно построить требуемую порождающую матрицу и осуществить кодирование для $\boldsymbol{u}_1 = [1\ 1\ 0]^T$, $\boldsymbol{u}_2 = [1\ 0\ 1]^T$:

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

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*

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

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*

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

Решение

Для определения минимального кодового расстояния d найдём все кодовые полиномы:

$$v(x) = g(x)(ax^2 + bx + c) = (x^6 + x^3 + 1)(ax^2 + bx + c) =$$
$$= ax^8 + bx^7 + cx^6 + ax^5 + bx^4 + cx^3 + ax^2 + bx + c,\ a, b, c \in \mathbb{F}_2.$$

Задача ТК-2...

В векторном виде все кодовые слова представляются как

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

Следовательно, минимальный хэммингов вес ненулевого кодового слова равен 3, т.е. $d = 3$.

Задача ТК-2...

В векторном виде все кодовые слова представляются как

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

Следовательно, минимальный хэммингов вес ненулевого кодового слова равен 3, т.е. $d = 3$.

Проводим систематическое кодирование сообщения $u(x)$:

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

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

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

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

Задача ТК-3

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/\left(x^3 + x + 1\right)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Задача ТК-3

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/\left(x^3+x+1\right)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Решение

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$:

$$s = w(\alpha) = \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 =$$
$$= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 =$$
$$= \alpha^3 + \alpha = \alpha + 1 + \alpha = 1 \neq 0.$$

Задача ТК-3

Рассмотрим код Хэмминга, ноль которого определяется примитивным элементом $\alpha \in \mathbb{F}_2[x]/\left(x^3+x+1\right)$.
Требуется декодировать полученный полином

$$w(x) = x^7 + x^6 + x^2 + 1.$$

Решение

Вычислим синдром с учётом $\alpha^3 = \alpha + 1$:

$$s = w(\alpha) = \alpha^7 + \alpha^6 + \alpha^2 + 1 = \alpha(\alpha^3)^2 + (\alpha^3)^2 + \alpha^2 + 1 =$$
$$= \alpha(\alpha+1)^2 + (\alpha+1)^2 + \alpha^2 + 1 = \alpha(\alpha^2+1) + \alpha^2 + 1 + \alpha^2 + 1 =$$
$$= \alpha^3 + \alpha = \alpha + 1 + \alpha = 1 \neq 0.$$

Далее необходимо найти полином ошибок вида $e(x) = x^k$ такой, что $e(\alpha) = s$, т.е. найти такое k, что $\alpha^k = 1$.

Очевидно, что $k = 0 \Rightarrow \widehat{v}(x) = w(x) + e(x) = x^7 + x^6 + x^2$.

Задача ТК-4

Для кода БЧХ с нулями $\alpha^i,\ i = 1, \ldots, 4$, *где* α — *примитивный элемент поля* $F = \mathbb{F}_2[x]/\left(x^4 + x + 1\right)$, *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 $\alpha^i,\ i = 1, \ldots, 4$, *где* α — *примитивный элемент поля* $F = \mathbb{F}_2[x]/\left(x^4 + x + 1\right)$, *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...

С помощью этой таблицы вычислим синдромы:

$$
\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.
\end{aligned}
$$

Синдромный полином — $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$.
Синдромов всего четыре, следовательно, $t = 2$.

Задача ТК-4...

С помощью этой таблицы вычислим синдромы:

$$
\begin{aligned}
s_1 &= w(\alpha) = \alpha^{14} + \alpha^{10} + \alpha^5 + \alpha^4 = \alpha^7, \\
s_2 &= w(\alpha^2) = (w(\alpha))^2 = \alpha^{14}, \\
s_3 &= w(\alpha^3) = \alpha^{12} + 1 + 1 + \alpha^{12} = 0, \\
s_4 &= w(\alpha^4) = (w(\alpha^2))^2 = \alpha^{13}.
\end{aligned}
$$

Синдромный полином — $s(x) = \alpha^{13}x^4 + \alpha^{14}x^2 + \alpha^7 x + 1$.
Синдромов всего четыре, следовательно, $t = 2$.

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

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

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

Решаем с помощью расширенного алгоритма Евклида:

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

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

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

Задача ТК-4...

Таким образом, искомый полином локаторов ошибок

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

Задача ТК-5

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

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

$$\begin{aligned}
\sigma(\alpha) &= \alpha^4 + \alpha^7 + 1 = \alpha^3 + 1,\\
\sigma(\alpha^2) &= \alpha^6 + \alpha^8 + 1 = \alpha^3,\\
\sigma(\alpha^3) &= \alpha^8 + \alpha^9 + 1 = \alpha^3 + \alpha^2 + \alpha,\\
\sigma(\alpha^4) &= \alpha^{10} + \alpha^{10} + 1 = 1,\\
\sigma(\alpha^5) &= \alpha^{12} + \alpha^{11} + 1 = 0,\\
\sigma(\alpha^6) &= \alpha^{14} + \alpha^{12} + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^7) &= \alpha + \alpha^{13} + 1 = \alpha^3 + \alpha^2 + 1,\\
\sigma(\alpha^8) &= \alpha^3 + \alpha^{14} + 1 = 0,\\
\sigma(\alpha^9) &= \alpha^5 + 1 + 1 = \alpha^2 + \alpha,\\
\sigma(\alpha^{10}) &= \alpha^7 + \alpha + 1 = \alpha^3,
\end{aligned}$$

Задача ТК-5...

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

$$\begin{aligned}
\sigma(\alpha^{11}) &= \alpha^9 + \alpha^2 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{12}) &= \alpha^{11} + \alpha^3 + 1 = \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{13}) &= \alpha^{13} + \alpha^4 + 1 = \alpha^3 + \alpha^2 + \alpha + 1,\\
\sigma(\alpha^{14}) &= 1 + \alpha^5 + 1 = \alpha^2 + \alpha,\\
\sigma(\alpha^{15}) &= \alpha^2 + \alpha^6 + 1 = \alpha^3 + 1.
\end{aligned}$$

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 $x^4 + x + 1$.

Полином $a(x)$ — примитивен, т.е. является м.м. для x.
Находим циклотомические классы для элементов α, α^2, α^3, α^4 поля F, где $\alpha = x$ — генератор мультипликативной группы F^*, учитывая, что $\alpha^{15} = 1$, $\alpha^4 = \alpha + 1$.

Очевидно, данных циклотомических класса два:

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

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... $\alpha^4 = \alpha + 1$

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

Определим циклотомический класс для элемента α^3, для чего вычислим требуемые его степени:

$$\alpha^6 = \alpha^4\alpha^2 = (\alpha+1)\alpha^2 = \alpha^3 + \alpha^2,$$
$$\alpha^{12} = \left(\alpha^6\right)^2 = \left(\alpha^3 + \alpha^2\right)^2 = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + \alpha + 1,$$
$$\alpha^{24} = \alpha^8 + \alpha^6 + \alpha^4 = (\alpha^2+1) + (\alpha^3+\alpha^2) + (\alpha+1) = \alpha^3 + \alpha,$$
$$\alpha^{48} = \alpha^6 + \alpha^2 = \alpha^3.$$

В результате получаем 4-х элементный циклотомический класс $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}\}$.

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

Вычислим м.м. для α^3:

$$g_{\alpha^3}(x) = (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24}) =$$
$$= \left(x^2 + (\alpha^3 + \alpha^{12}x + \alpha^{15})\right)\left(x^2 + (\alpha^6 + \alpha 24)x + \alpha^{30}\right) =$$
$$= \left(x^2 + (\alpha^2 + \alpha + 1)x + 1\right)\left(x^2 + (\alpha^2 + \alpha)x + 1\right) =$$
$$= x^4 + x^3 + x^2 + x + 1.$$

Таким образом,

$$g(x) = g_\alpha(x) \cdot g_{\alpha^3}(x) = \left(x^4 + x + 1\right)\left(x^4 + x^3 + x^2 + x + 1\right) =$$
$$= x^8 + x^7 + x^6 + x^4 + 1, \quad \deg g(x) = m = 8,\ k = 15 - 8 = 7$$

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

Задача ТК-7

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

Задача ТК-7

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

Решение

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

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

Поле F можно задать так, чтобы в разбиении его мультипликативной группы на циклотомические классы имелся 5-элементный $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}\}$ класс.

Остальные рассматриваемые степени α будут входить в циклотомические классы

$$\{\alpha^3, \alpha^6, \dots\} \text{ и } \{\alpha^5, \alpha^{10}, \dots\}.$$

Задача ТК-7...

Потребуем, чтобы эти классы были также пятиэлементным и из специальных таблиц найдём минимальные многочлены пятой степени для α, α^3 и α^5:

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

Тогда $g(x) = g_\alpha \cdot g_{\alpha^3}(x) \cdot g_{\alpha^5}(x) =$
$= x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1,$

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

Поле F определяется как $\mathbb{F}_2[x]/\left(x^5 + x^3 + 1\right)$.

Разделы I

- Задачи построения кодов, исправляющих ошибки. Основные понятия метрики на единичном кубе.
- Групповые коды: определение, построение, свойства. Кодовое расстояние.
- Теорема Хэмминга. Пример построения кода Хэмминга.
- Циклические коды: определение, кодирование и декодирование, свойства.
- Циклотомические классы. Коды БЧХ — определение построение кодов и их свойства.
- Синдромы — определение, использование при декодировании циклических и БЧХ-кодов.