Алгоритмы кодирования/декодирования для линейных, циклических и БЧХ кодов

Везде в тексте все вычисления проводятся в двоичной арифметике.

Рассмотрим задачу передачи потока битовой информации по каналу с шумом с возможностью автоматического исправления ошибок, допущенных при передаче. При *блоковом кодировании* входящий поток информации разбивается на блоки фиксированной длины k. Обозначим один такой блок через $\boldsymbol{u} \in \{0,1\}^k$. Предполагается, что во входном потоке данных, вообще говоря, нет избыточности. Поэтому для реализации схемы, способной исправлять ошибки, необходимо закодировать блок $\boldsymbol{u}$ в некоторое кодовое слово большей длины путем добавления избыточности в передаваемые данные. Обозначим кодовое слово через $\boldsymbol{v} \in \{0,1\}^n$, $n > k$, а через $m = n - k$ – количество требуемых дополнительных бит. Для кодирования всевозможных блоков $\boldsymbol{u}$ необходимо использовать 2^k кодовых слов длины n. Определим минимальное расстояние кода d как минимальное хэммингово расстояние для всех различных пар кодовых слов. Назовём множество 2^k кодовых слов длины n с минимальным расстоянием d (n,k,d)-блоковым кодом, а величину $r = k/n$ – скоростью кода. При передаче по каналу с шумом кодовое слово $\boldsymbol{v}$ превращается в принятое слово $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}$, где $\boldsymbol{e} \in \{0,1\}^n$ – вектор ошибок ($e_i = 1$, если в i-ом бите произошла ошибка). Далее алгоритм декодирования пытается восстановить переданное слово $\boldsymbol{v}$ путем поиска среди всевозможных кодовых слов ближайшего к $\boldsymbol{w}$. Обозначим результат работы алгоритма декодирования через $\hat{\boldsymbol{v}}$. На последнем этапе декодированное слово $\hat{\boldsymbol{v}}$ переводится в декодированное слово исходного сообщения $\hat{\boldsymbol{u}}$. Очевидно, что (n,k,d)-блоковый код способен обнаруживать до $d-1$ ошибки и исправлять до $[(d-1)/2]$ ошибок.

Линейные коды

Множество $\{0,1\}^n$ с операциями суммы и произведения по модулю 2 образует линейное пространство над конечным полем из двух элементов $\{0,1\}$. Блоковый (n,k,d)-код C называется *линейным*, если множество его кодовых слов образует линейное подпространство размерности k общего линейного пространства $\{0,1\}^n$. Таким образом, для линейного кода произвольная линейная комбинация кодовых слов является кодовым словом. Минимальное кодовое расстояние d для линейного кода определяется как минимальный хэммингов вес (количество ненулевых бит) среди ненулевых кодовых слов. Пусть $\boldsymbol{g}_0, \boldsymbol{g}_1, \ldots, \boldsymbol{g}_{k-1} \in \{0,1\}^n$ – базис C. Тогда $\boldsymbol{v} \in C$ может быть представлено как $\boldsymbol{v} = \sum_{i=0}^{k-1} u_i \boldsymbol{g}_i$, $u_i \in \{0,1\}$ или, эквивалентно, $\boldsymbol{v} = G\boldsymbol{u}$, где $G = [\boldsymbol{g}_0|\boldsymbol{g}_1|\ldots|\boldsymbol{g}_{k-1}] \in \{0,1\}^{n\times k}$ – порождающая матрица кода. Матрица G определена с точностью до эквивалентных преобразований столбцов.

Кодирование. *Несистематическое кодирование* линейного кода, заданного своей порождающей матрицей G, может быть осуществлено как $\boldsymbol{v} = G\boldsymbol{u}$, где $\boldsymbol{u} \in \{0,1\}^k$ – блок исходного сообщения. Очевидно, что с помощью эквивалентных преобразований столбцов матрица G может быть приведена к виду, в котором некоторые k строк образуют единичную подматрицу. Пусть, не ограничивая общности, единичная подматрица образуется в первых k строках матрицы G, т.е. $G = \begin{bmatrix} I_k \\ P \end{bmatrix}$, где I_k – единичная матрица размера $k\times k$, а $P \in \{0,1\}^{m\times k}$. Тогда кодирование по правилу $\boldsymbol{v} = G\boldsymbol{u}$ будет *систематическим*, при котором первые k бит кодового слова $\boldsymbol{v}$ являются битами исходного сообщения $\boldsymbol{u}$. При использовании систематического кодирования этап преобразования из декодированного кодового слова $\hat{\boldsymbol{v}}$ в декодированное сообщение $\hat{\boldsymbol{u}}$ становится тривиальным.

Линейное пространство $\{0,1\}^n$ может быть разложено в прямую сумму линейных подпространств C и $C^\perp$, где $C^\perp$ – ортогональное подпространство для C, $\dim C^\perp = m$. Пусть

$\boldsymbol{h}_0, \ldots, \boldsymbol{h}_{m-1} \in \{0,1\}^m$ – базис $C^\perp$. Составим матрицу

$$H = \begin{bmatrix} \boldsymbol{h}_0^T \\ \boldsymbol{h}_1^T \\ \ddots \\ \boldsymbol{h}_{m-1}^T \end{bmatrix} \in \{0,1\}^{m \times n}.$$

Очевидно, что $\boldsymbol{h}_j^T \boldsymbol{g}_i = 0 \ \forall i, j$. Следовательно, для любого кодового слова $\boldsymbol{v} \in C$ выполнено $H\boldsymbol{v} = 0$. Матрица H называется *проверочной матрицей* кода. Пусть порождающая матрица G имеет вид $\begin{bmatrix} I_k \\ P \end{bmatrix}$. Тогда проверочная матрица H может быть построена как $H = \begin{bmatrix} P & I_m \end{bmatrix} \in \{0,1\}^{m \times n}$, где I_m – единичная матрица размера $m \times m$. Действительно, в этом случае $H\boldsymbol{v} = HG\boldsymbol{u} = (P + P)\boldsymbol{u} = 0$.

Пример 1. Линейный блоковый (6,3)-код задан порождающей матрицей

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

Требуется для данного кода осуществить несистематическое и систематическое кодирование векторов $\boldsymbol{u}_1 = [0\ 1\ 1]^T$ и $\boldsymbol{u}_2 = [1\ 0\ 1]^T$, построить проверочную матрицу кода H, а также определить минимальное кодовое расстояние d.

Несистематическое кодирование находим непосредственно:

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

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

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

В последней матрице в строках (3, 5, 1) стоит единичная подматрица. В результате систематическое кодирование $\boldsymbol{u}_1, \boldsymbol{u}_2$, при котором биты 1, 2, 3 исходного сообщения переходят, соответственно, в биты 3, 5, 1 кодового слова, вычисляется следующим образом

$$[\boldsymbol{v}_1, \boldsymbol{v}_2] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} [\boldsymbol{u}_1, \boldsymbol{u}_2] = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}. \quad (1)$$

С учетом выделенной единичной подматрицы в порождающей матрице G, нетрудно найти проверочную матрицу кода H. Для этого формируем матрицу P из строк G, отличных от строк с

единичной подматрицей, т.е. $P = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. Далее нужно разместить столбцы P, соответственно, в 3-ом, 5-ом и 1-ом столбце H, а во 2-й, 4-ый и 6-ой столбец H поставить единичную подматрицу:

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

Проверим, что полученная матрица действительно является проверочной матрицей кода. Для этого вычислим HG:

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

Проверим также, что в результате систематического кодирования (1) были действительно найдены кодовые слова:

$$H[\boldsymbol{v}_1, \boldsymbol{v}_2] = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Найдем теперь минимальное кодовое расстояние d. Для этого построим матрицу всех $2^3 = 8$ кодовых слов и найдем для них минимальный ненулевой хэммингов вес:

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

Отсюда получаем, что $d = 3$. Следовательно, рассмотренный код способен исправить одну ошибку и обнаружить две ошибки.

Декодирование. Назовём *синдромом* принятого сообщения $\boldsymbol{w}$ вектор $\boldsymbol{s} = H\boldsymbol{w}$, где H – проверочная матрица кода. С учётом представления $\boldsymbol{w} = \boldsymbol{v} + \boldsymbol{e}$, получаем $\boldsymbol{s} = H\boldsymbol{w} = H(\boldsymbol{v} + \boldsymbol{e}) = H\boldsymbol{v} + H\boldsymbol{e} = H\boldsymbol{e}$. Очевидно, что синдром является нулевым вектором тогда и только тогда, когда принятое сообщение является кодовым словом. Вектор ошибок удовлетворяет системе линейных уравнений $H\boldsymbol{e} = \boldsymbol{s}$. Матрица данной системы имеет размер $m \times n$. Следовательно, все решения данной СЛАУ описываются как $\boldsymbol{e} = \hat{\boldsymbol{e}} + G\boldsymbol{u}$, где $\hat{\boldsymbol{e}}$ – произвольное частное решение системы, а $G\boldsymbol{u}$ – решение однородной системы $H\boldsymbol{e} = \boldsymbol{0}$, где $\boldsymbol{u}$ – произвольный вектор длины k. Таким образом, получаем 2^k различных решений для вектора ошибок $\boldsymbol{e}$. Среди них решение с наименьшим хэмминговым весом дает искомый вектор ошибок.

Пример 2. Рассмотрим линейный код из примера 1. Пусть исходный вектор $\boldsymbol{u} = [0\ 1\ 1]^T$. 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 $\boldsymbol{w} = [1\ 0\ 0\ 0\ 1\ 0]^T$. Для декодирования $\boldsymbol{w}$ найдём его синдром

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

Далее необходимо найти все решения системы $H\boldsymbol{e} = \boldsymbol{s}$. Частное решение этой системы легко найти с учётом того, что в столбцах $2, 4, 6$ проверочной матрицы H стоит единичная подматрица. Пусть

$\hat{e}_1 = \hat{e}_3 = \hat{e}_5 = 0$. Тогда $\hat{e}_2 = s_1, \hat{e}_4 = s_2, \hat{e}_6 = s_3$, т.е. $\hat{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$. Решение однородной системы уже было найдено раньше на этапе вычисления кодового расстояния d:

$$G[\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_8] = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Таким образом, все 8 решений системы $H\boldsymbol{e} = \boldsymbol{s}$ могут быть записаны как

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

Выбирая среди них решение с наименьшим весом, находим $\boldsymbol{e} = [0\ 1\ 0\ 0\ 0\ 0]^T$, т.е. $\hat{\boldsymbol{v}} = \boldsymbol{w} + \boldsymbol{e} = [1\ 1\ 0\ 0\ 1\ 0]^T$.

Циклические коды

Линейный блоковый (n, k, d)-код называется *циклическим*, если любой циклический сдвиг кодового слова является кодовым словом. Поставим в соответствие произвольному вектору $\boldsymbol{v} = \{v_0, v_1, \ldots, v_{n-2}, v_{n-1}\} \in \{0, 1\}^n$ полином вида $v(x) = v_0 + v_1 x + \cdots + v_{n-2}x^{n-2} + v_{n-1}x^{n-1}$. Тогда можно показать, что для (n, k, d)-линейного циклического блокового кода найдется полином $g(x)$ степени $m = n - k$ такой, что

1. Все кодовые слова $v(x)$ могут быть представлены как $g(x)q(x)$, где $q(x)$ – некоторый полином степени не выше, чем $k - 1$;
2. Полином $g(x)$ является делителем полинома $x^n + 1$.

Такой полином $g(x)$ называется *порождающим полиномом* циклического кода. Любой полином, являющийся делителем $x^n + 1$, является порождающим для некоторого циклического кода.

Несистематическое кодирование $u(x)$ для циклического кода, заданного своим порождающим полиномом $g(x)$, может быть осуществлено как $v(x) = g(x)u(x)$. Процесс систематического кодирования может быть реализован как

$$v(x) = x^m u(x) + \mathrm{mod}(x^m u(x), g(x)),$$

где m – степень $g(x)$. Здесь биты входного сообщения $u(x)$ воспроизводятся в крайних правых битах кодового слова $v(x)$.

Назовём *синдромом* принятого полинома $w(x)$ полином $s(x) = \mathrm{mod}(w(x), g(x)) = \mathrm{mod}(v(x) + e(x), g(x)) = \mathrm{mod}(e(x), g(x))$. Как и раньше для случая линейных кодов синдром является нулевым многочленом тогда и только тогда, когда $w(x)$ является кодовым словом. Таким образом, для циклических кодов синдром вычисляется без необходимости конструирования проверочной матрицы H. Общий алгоритм декодирования циклического кода принципиально не отличается от общего алгоритма декодирования линейного кода. В нём рассматривается общее решение системы $e(x) = s(x) + g(x)u(x)$ для всех возможных полиномов $u(x)$ степени $k - 1$, а искомый полином ошибок определяется как решение с минимальным числом ненулевых слагаемых.

Пример 3. Пусть длина циклического кода $n = 7$. Для построения циклического кода необходимо сначала найти разложение полинома $x^7 + 1$ на неприводимые множители. Так как $7 = 2^3 - 1$, то все ненулевые элементы поля $\mathbb{F}_2^3$ являются корнями $x^7 + 1$. Известно, что каждый многочлен над $\mathbb{F}_2$ содержит в расширении поля $\mathbb{F}_2^3$ вместе с любым своим корнем β также смежные корни вида

$\beta^2, \beta^{2^2}, \beta^{2^3}, \ldots$. Пусть α – произвольный примитивный элемент поля $\mathbb{F}_2^3$. Тогда с учетом $\alpha^7 = 1$ легко найти разбиение всех элементов поля на смежные классы:

$$(\alpha, \alpha^2, \alpha^4);\ (\alpha^3, \alpha^6, \alpha^5);\ \alpha^7.$$

Таким образом, многочлен x^7+1 имеет один неприводимый делитель степени 1, а также два неприводимых делителя степени 3. В результате получаем разложение

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

В качестве $g(x)$ может выступать произвольный делитель x^7+1. Выберем в качестве $g(x)$ многочлен $x^3 + x + 1$. В результате получаем циклический $(7, 4)$-код.

Пусть входной полином $u(x)$ равен $x^3 + x^2$. Его несистематическое кодирование находим как

$$v(x) = u(x)g(x) = (x^3 + x^2)(x^3 + x + 1) = x^6 + x^5 + x^4 + x^2.$$

В бинарном представлении это соответствует

$$\boldsymbol{u} = [0011],\ \boldsymbol{v} = [0010111].$$

Для осуществления систематического кодирования необходимо найти остаток от деления многочлена $x^3u(x)$ на $g(x)$. В результате находим

$$v(x) = x^3u(x) + \mathrm{mod}(x^3u(x), g(x)) = x^6 + x^5 + \mathrm{mod}(x^6 + x^5, x^3 + x + 1) = x^6 + x^5 + x.$$

В бинарном представлении этот соответствует

$$\boldsymbol{u} = [0011],\ \boldsymbol{v} = [0100011].$$

Таким образом, действительно биты входного сообщения $\boldsymbol{u}$ воспроизводятся в крайних правых битах кодового слова $\boldsymbol{v}$.

Коды БЧХ

Полином $m_\alpha(x) \in \mathbb{F}_2[x]$ называется минимальным полиномом для элемента $\alpha \in \mathbb{F}_2^l$, если он является полиномом минимальной степени, для которого α является корнем. В частности, минимальный полином для примитивного элемента α называется примитивным полиномом. Можно показать, что корнями минимального полинома $m_\alpha(x)$ являются $\{\alpha, \alpha^2, \alpha^4, \ldots, \alpha^{2^q}\}$. Данный набор элементов из поля $\mathbb{F}_2^l$ называется классом смежности для элемента α. Смежные классы, порожденные различными элементами поля, либо совпадают, либо не пересекаются. Можно показать, что полином

$$\prod_{i=1}^{q}(x + \alpha^{2^i}) = x^q + \lambda_{q-1}x^{q-1} + \cdots + \lambda_1 x + \lambda_0$$

имеет коэффициенты из $\mathbb{F}_2$ и является минимальным полиномом для α, а также для всех элементов поля, входящих вместе с α в один смежный класс. Отсюда выводится метод построения минимального полинома для заданного элемента поля α:

1. Построить смежный класс, порождённый элементом α;
2. Найти коэффициенты полинома $m_\alpha(x)$ путем перемножения многочленов $x + \alpha^{2^i}$ для всех $i = 1, \ldots, q$.

Пусть $n = 2^l - 1$, $d = 2t+1 \le n$. Тогда *кодом БЧХ* называется (n, k, d)-линейный циклический код, в котором порождающий многочлен $g(x)$ определяется как минимальный многочлен для элементов $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ из поля $\mathbb{F}_2^l$, где α – произвольный примитивный элемент поля $\mathbb{F}_2^l$, т.е.

$$g(x) = \mathrm{НОК}(m_\alpha(x), m_{\alpha^2}(x), \ldots, m_{\alpha^{d-1}}(x)).$$

Набор элементов $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ называется *нулями БЧХ-кода*. Можно показать, что минимальное кодовое расстояние кода БЧХ не меньше, чем величина d. В результате БЧХ-коды по построению способны исправлять не менее t ошибок, где $t = [(d-1)/2]$.

С учетом того, что все кодовые слова циклического кода делятся на $g(x)$, а $g(x)$ является минимальным полиномом для выбранных нулей кода, то

$$v(x) \in C \;\Leftrightarrow\; v(\alpha^i) = 0 \;\forall i = 1, \ldots, 2t.$$

Назовём синдромами принятого сообщения $w(x)$ значения $w(x)$ в нулях кода: $s_i = w(\alpha^i)$, $i = 1, \ldots, 2t$. Все синдромы равны нулю тогда и только тогда, когда $w(x)$ является кодовым словом.

Пример 4. Рассмотрим БЧХ-коды для случая поля $\mathbb{F}_2^3 = \mathbb{F}_2[x]/(x^3 + x + 1)$. Таким образом, $l = 3$, $n = 7$. Полином $x^3 + x + 1$ является примитивным полиномом над $\mathbb{F}_2$. Обозначим через $\alpha \in \mathbb{F}_2^3$ его произвольный корень.

Построим код БЧХ, исправляющий не менее, чем $t = 1$ ошибку. Его порождающий полином $g(x)$ строится как минимальный многочлен для элементов α, α^2. Эти элементы входят в один смежный класс $(\alpha, \alpha^2, \alpha^4)$. Поэтому $g(x) = m_\alpha(x) = m_{\alpha^2}(x) = x^3 + x + 1$. В результате получаем $(7, 4, 3)$-код, являющийся кодом Хэмминга.

Построим код БЧХ, исправляющий не менее, чем $t = 2$ ошибок. Его порождающий полином $g(x)$ строится как минимальный многочлен для элементов $\alpha, \alpha^2, \alpha^3, \alpha^4$. Эти элементы входят в два смежных класса $(\alpha, \alpha^2, \alpha^4)$ и $(\alpha^3, \alpha^6, \alpha^5)$. Поэтому $g(x) = m_\alpha(x) m_{\alpha^3}(x)$. Найдем минимальный многочлен $m_{\alpha^3}(x)$ по его корням

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

Все коэффициенты многочлена $m_{\alpha^3}(x)$ принадлежат $\mathbb{F}_2$. Вычислим эти коэффициенты, используя свойства $\alpha^7 = 1$ (т.к. α является примитивным элементом) и $\alpha^3 = \alpha + 1$ (т.к. α является корнем $x^3 + x + 1$):

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

Таким образом, $m_{\alpha^3}(x) = x^3 + x^2 + 1$, $g(x) = m_\alpha(x) m_{\alpha^3}(x) = (x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Заметим, что многочлен $g(x)$ имеет корни $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$. Следовательно, построен код БЧХ $(7, 1, 7)$, который исправляет не менее, чем $t = 3$ ошибки. Нетрудно видеть, что данный код содержит всего два кодовых слова $\boldsymbol{v}_1 = [0000000]$, $\boldsymbol{v}_2 = [1111111]$.

Декодирование кода Хэмминга. Код Хэмминга является частным случаем кода БЧХ для $t = 1$. Поэтому нулями кода Хэмминга являются α и α^2, где α – примитивный элемент поля $\mathbb{F}_2^l$. Для декодирования принятого слова $w(x)$ вычислим синдром $s_1 = w(\alpha)$. Синдром s_2 автоматически определяется по s_1 как $s_2 = w(\alpha^2) = (w(\alpha))^2 = s_1^2$. Если $s_1 = 0$, то $w(x)$ уже является кодовым словом и $\hat{v}(x) = w(x)$. Предположим, что при передаче по каналу была совершена одна ошибка. Тогда $w(x) = v(x) + e(x)$, где полином ошибок $e(x) = x^j$ для некоторого j. Для нахождения позиции ошибки вычислим значения полинома ошибок в точке α для всех $j = 1, \ldots, n$. Если $e(\alpha) = \alpha^j = s_1$, то j – искомая позиция ошибки и $\hat{v}(x) = w(x) + x^j$. Если $\alpha^j \neq s_1 \;\forall j$, то при передаче было совершено более одной ошибки, и процедура декодирования выдает отказ.

Пример 5. Рассмотрим код Хэмминга из примера 4. Он имеет порождающий полином $g(x) = x^3 + x + 1$, а все вычисления проводятся в поле $\mathbb{F}_2^3 = \mathbb{F}_2[x]/(x^3 + x + 1)$[1]. Пусть входной полином $u(x) = x^3 + x^2$. Его систематическое кодирование было найдено в примере 3: $v(x) = x^6 + x^5 + x$. Пусть при передаче произошла ошибка в позиции 5, т.е. $w(x) = x^6 + x$, а истинный $e(x) = x^5$. Для декодирования сначала найдем синдром $s_1 = w(\alpha) = \alpha^6 + \alpha = (\alpha^3)^2 + \alpha = (\alpha + 1)^2 + \alpha = \alpha^2 + \alpha + 1$.

[1]Совпадение в данном случае порождающего полинома и полинома, по которому строится поле, является случайностью.

Теперь вычислим α^j для всех $j = 0, \ldots, 6$:

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

Отсюда находим, что $\alpha^5 = s_1$, т.е. ошибка произошла в позиции 5. Таким образом, $\hat{v}(x) = w(x) + x^5 = x^6 + x^5 + 1$.

Декодирование БЧХ кода. Пусть при передаче по каналу произошло ν ошибок, т.е. $e(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_\nu}$, где $j_1, \ldots, j_\nu$ – позиции ошибок. Рассмотрим *полином локаторов ошибок*

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

Корнями данного полинома являются α^{-j_i}. Рассмотрим также *синдромный полином*

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

где $s_i = w(\alpha^i),\ i = 1, \ldots, 2t$ – значения принятого полинома в нулях БЧХ кода. Можно показать, что полином локаторов ошибок может быть найден путем решения уравнения

$$s(x)\sigma(x) + x^{2t+1}a(x) = \Lambda(x) \tag{2}$$

для некоторого многочлена $\Lambda(x)$, степень которого не превосходит t. Данное уравнение может быть решено с помощью расширенного алгоритма Евклида для пары многочленов x^{2t+1} и $s(x)$. Количество фактически совершенных ошибок ν определяется степенью найденного $\sigma(x)$. В результате общая схема декодирования БЧХ кода выглядит следующим образом:

1. Для принятого слова $w(x)$ найти все синдромы $s_i = w(\alpha^i)\ \forall i = 1, \ldots, 2t$;
2. Найти полином локаторов ошибок $\sigma(x)$ путем решения уравнения (2) с помощью расширенного алгоритма Евклида;
3. Найти все корни $\sigma(x)$ полным перебором; пусть найденные корни равны $\alpha^{k_1}, \ldots, \alpha^{k_\nu}$;
4. Найти позиции ошибок $j_i = -k_i \mod n$, где $n = 2^l - 1$ – порядок примитивного элемента α;
5. Исправить ошибки $\hat{v}(x) = w(x) + x^{j_1} + \cdots + x^{j_\nu}$;
6. Найти все синдромы $\hat{v}(x)$; если они не равны нулю, то выдать отказ от декодирования.

Пример 6. Рассмотрим (15,5,7) БЧХ код, исправляющий три ошибки. Он имеет порождающий полином $g(x) = x^{10}+x^8+x^5+x^4+x^2+x+1$, а все вычисления проводятся в поле $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(x^4+x+1)$. Пусть входной полином имеет вид $u(x) = x^4 + x^2 + x$. При систематическом кодировании ему соответствует кодовый полином $v(x) = x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2 + x$. Пусть полином ошибок равен $e(x) = x^{12}+x^6+1$. Следовательно, принятое слово $w(x) = x^{14}+x^{11}+x^8+x^6+x^4+x^3+x^2+x+1$.

Для удобства последующих вычислений построим для всех элементов поля $\mathbb{F}_2^4$ таблицу соответствий между степенным представлением и полиномиальным (см. таблицу 1).

С использованием таблицы 1 найдём синдромы для принятого слова:

$$\begin{aligned}
&s_1 = w(\alpha) = \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha + \alpha^2 + 1 + \alpha^3 + \alpha^2 + \alpha + 1 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha,\\
&s_2 = w(\alpha^2) = (w(\alpha))^2 = \alpha^2,\\
&s_3 = w(\alpha^3) = \alpha^{42} + \alpha^{33} + \alpha^{24} + \alpha^{18} + \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 = \alpha^{12} + \alpha^3 + \alpha^9 + \alpha^3 + \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 =\\
&\qquad = \alpha^6 + \alpha^3 + 1 = \alpha^3 + \alpha^2 + \alpha^3 + 1 = \alpha^2 + 1 = \alpha^8,\\
&s_4 = w(\alpha^4) = (w(\alpha^2))^2 = \alpha^4,\\
&s_5 = w(\alpha^5) = \alpha^{70} + \alpha^{55} + \alpha^{40} + \alpha^{30} + \alpha^{20} + \alpha^{15} + \alpha^{10} + \alpha^5 + 1 = \alpha^{10} + \alpha^{10} + \alpha^{10} + 1 + \alpha^5 + 1 + \alpha^{10} + \alpha^5 + 1 = 1,\\
&s_6 = w(\alpha^6) = (w(\alpha^3))^2 = (\alpha^2+1)^2 = \alpha^4 + 1 = \alpha.
\end{aligned}$$

Таблица 1: Таблица вычислений для поля $\mathbb{F}_2^4 = \mathbb{F}_2[x]/(x^4+x+1)$.

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	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

Таким образом, синдромный полином $s(x) = \alpha x^6 + x^5 + \alpha^4 x^4 + \alpha^8 x^3 + \alpha^2 x^2 + \alpha x + 1$.

Теперь решим уравнение $x^7 a(x) + s(x)\sigma(x) = \Lambda(x)$ расширенным алгоритмом Евклида.

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

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 меньше, чем $t = 3$. Таким образом, $\sigma(x) = y_2(x) = \alpha x^3 + \alpha^5 x^2 + \alpha^{14} x + \alpha^{13}$ и $\nu = \deg\sigma(x) = 3$.

Найдём корни $\sigma(x)$ полным перебором:

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

$$\sigma(\alpha^9) = \alpha^{13} + \alpha^8 + \alpha^8 + \alpha^{13} = 0,$$
$$\sigma(\alpha^{10}) = \alpha + \alpha^{10} + \alpha^9 + \alpha^{13} = \alpha,$$
$$\sigma(\alpha^{11}) = \alpha^4 + \alpha^{12} + \alpha^{10} + \alpha^{13} = \alpha^2 + \alpha,$$
$$\sigma(\alpha^{12}) = \alpha^7 + \alpha^{14} + \alpha^{11} + \alpha^{13} = 1,$$
$$\sigma(\alpha^{13}) = \alpha^{10} + \alpha + \alpha^{12} + \alpha^{13} = \alpha^2 + \alpha + 1,$$
$$\sigma(\alpha^{14}) = \alpha^{13} + \alpha^3 + \alpha^{13} + \alpha^{13} = \alpha^2 + 1,$$
$$\sigma(\alpha^{15}) = \alpha + \alpha^5 + \alpha^{14} + \alpha^{13} = 0.$$

По найденным корням $\alpha^3, \alpha^9, \alpha^{15}$ легко вычислить позиции ошибок: $j_1 = -3 \mod 15 = 12$, $j_2 = -9 \mod 15 = 6$, $j_3 = -15 \mod 15 = 0$. Значит, $e(x) = x^{12} + x^6 + 1$ и $\hat{v}(x) = w(x) + e(x) = x^{14} + x^{12} + x^{11} + x^8 + x^4 + x^3 + x^2 + x$.