1 Коды БЧХ (Боуза - Чоудхури - Хоквингема)

Теорема 1. *(Граница БЧХ)*
Пусть $g(x)$ порождает код C и среди его корней есть

$$\alpha^m, \alpha^{m+j}, \alpha^{m+2j}, \ldots, \alpha^{m+(d-2)j},$$

где α^j – примитивный элемент поля разложения $g(x)$. Тогда минимальное расстояние кода C не менее d.

Доказательство. (от противного) Предположим $d(C) < d$, то есть в C есть кодовое слово расстояние которого меньше d. Выпишем его в виде многочлена

$$f(x) = \beta_1 x^{i_1} + \beta_2 x^{i_2} + \ldots + \beta_{d-1} x^{i_{d-1}},$$

где, возможно, некоторые β_i нулевые, но сам $f(x)$ отличен от нуля.

По определению циклических кодов $g(x)|f(x)$, значит все корни $g(x)$ являются конями $f(x)$.

$$\begin{cases} \beta_1\alpha^{mi_1} + \beta_2\alpha^{mi_2} + \ldots + \beta_{d-1}\alpha^{mi_{d-1}} & = 0 \\ \beta_1\alpha^{(m+j)i_1} + \beta_2\alpha^{(m+j)i_2} + \ldots + \beta_{d-1}\alpha^{(m+j)i_{d-1}} & = 0 \\ \ldots & \\ \beta_1\alpha^{(m+(d-2)j)i_1} + \beta_2\alpha^{(m+(d-2)j)i_2} + \ldots + \beta_{d-1}\alpha^{(m+(d-2)j)i_{d-1}} & = 0 \end{cases}$$

Это система из $d-1$ уравнения с $d-1$ неизвестным $\beta_1, \beta_2, \ldots, \beta_{d-1}$. Определитель системы:

$$\Delta = \alpha^{mi_1}\alpha^{mi_2}\ldots\alpha^{mi_{d-1}} \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha^{ji_1} & \alpha^{ji_2} & \ldots & \alpha^{ji_{d-1}} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha^{(d-2)ji_1} & \alpha^{(d-2)ji_2} & \ldots & \alpha^{(d-2)ji_{d-1}} \end{vmatrix} \neq 0,$$

– отличен от нуля, следовательно имеется единственное решение системы, $\beta_i = 0$, $\forall i$. Противоречие с условием $f(x) \neq 0$. □

Определение 2. *Пусть даны $d, m_0 \in \mathbb{Z}$ и $\alpha \in \mathrm{GF}(2^m)$, α примитивный корень. Код БЧХ – код с порождающим многочленом $g(x) \in \mathrm{GF}(2)[x]$, наименьшей степени среди корней которого есть $\alpha^{m_0}, \alpha^{m_0+1}, \ldots, \alpha^{m_0+d-2}$. Если $m_0 = 1$, тогда это примитивный БЧХ-код.*

Замечание 3. $g(x)|x^{2^m-1} - 1$.
Это верно, так как каждый элемент $\mathrm{GF}(2^m)$ является корнем $x^{2^m} - x$, и $\mathrm{GF}(2^m)$ является поле разложения $g(x)$.

Замечание 4. Длинна БЧХ-кода $n = 2^m - 1$.
Это следует из условия, что $g(x)|x^n - 1$ и n – минимальное с таким своиством.

Теорема 5. *Приминивный БЧХ-код способен исправить $t \leqslant \frac{d-1}{2}$ ошибок.*

Доказательство. Предположим, что при передаче сообщения произошло $\nu \leqslant t$ ошибок:

$$i(x)g(x) \longrightarrow_{+e(x)} f(x) = i(x)g(x) + e(x),$$

где $e(x)$ многочлен ошибок:

$$e(x) = x^{i_1} + x^{i_2} + \ldots + x^{i_\nu}, \text{ где } i_j < 2^m - 1.$$

Корнями многочлена $g(x)$ являются α, α^2, ..., α^{d-1}, таким образом $f(\alpha^j) = i(\alpha^j)\ g(\alpha^j) + e(\alpha^j) = e(\alpha^j)$, при $j \in \{1, 2, \ldots, d-1\}$. Рассмотрим следующие объекты:

$$S_j = f(\alpha^j) = e(\alpha^j),$$

– синдромы.

Задача исправления ошибок ставится следующим образом: имеются $d-1$ синдромов S_j, необходимо востановить многочлен ошибок $e(x)$.

Многочлен $e(x)$ определяется коэффицентами ν и $i_1, i_2, ..., i_\nu$.

Введём дополнительно вспомогательные объекты: $X_1 = \alpha^{i_1}$, $X_2 = \alpha^{i_2}$, ..., $X_\nu = \alpha^{i_\nu}$ – локаторы ошибок.

В таких обозначениях:

$$\begin{array}{rcccl} e(\alpha) & = & X_1 + X_2 + ... + X_\nu & = & S_1 \\ e(\alpha^2) & = & X_1^2 + X_2^2 + ... + X_\nu^2 & = & S_2 \\ & & ... & & \\ e(\alpha^{2t}) & = & X_1^{2t} + X_2^{2t} + ... + X_\nu^{2t} & = & S_{2t} \end{array}$$

Все локаторы различны, так как $X^k = X^l \Leftrightarrow \alpha^{i_k} = \alpha^{i_l} \Leftrightarrow i_k \equiv i_l (\mathrm{mod}\, 2^m - 1)$, но $i_k, i_l < 2^m - 1$; и отличны от нуля.

Рассмотрим матрицу:

$$M = \begin{pmatrix} S_1 & S_2 & ... & S_t \\ S_2 & S_3 & ... & S_{t+1} \\ ... & ... & ... & ... \\ S_t & S_{t+1} & ... & S_{2t-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & ... & 1 \\ X_1 & X_2 & ... & X_\nu \\ ... & ... & ... & ... \\ X_1^{t-1} & X_2^{t-1} & ... & X_\nu^{t-1} \end{pmatrix} \begin{pmatrix} X_1 & X_1^2 & ... & X_1^t \\ X_2 & X_2^2 & ... & X_2^t \\ ... & ... & ... & ... \\ X_\nu & X_\nu^2 & ... & X_\nu^t \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 1 & ... & 1 \\ X_1 & X_2 & ... & X_\nu \\ ... & ... & ... & ... \\ X_1^{t-1} & X_2^{t-1} & ... & X_\nu^{t-1} \end{pmatrix} \begin{pmatrix} X_1 & & & \\ & X_2 & & \\ & & ... & \\ & & & X_\nu \end{pmatrix} \begin{pmatrix} 1 & X_1 & ... & X_1^{t-1} \\ 1 & X_2 & ... & X_2^{t-1} \\ ... & ... & ... & ... \\ 1 & X_\nu & ... & X_\nu^{t-1} \end{pmatrix} = W I W^T.$$

Ранг матриц W и I равен ν, следовательно ранг матрицы M так же равен ν.

Рассмотрим локаторный многочлен:

$$\Lambda(x) = (1 - x\, X_1)(1 - x\, X_2)...(1 - x\, X_\nu) = \Lambda_\nu x^\nu + \Lambda_{\nu-1} x^{\nu-1} + ... + \Lambda_1 x + 1.$$

Его корни обратны локаторам. Подставим вместо x локатор X_i^{-1}, получим:

$$\Lambda_\nu X_i^{-\nu} + \Lambda_{\nu-1} X_i^{1-\nu} + ... + \Lambda_1 X_i^{-1} + 1 = 0, \text{ умножим на } X_i^{j+\nu},$$

$$\Lambda_\nu X_i^j + \Lambda_{\nu-1} X_i^{j+1} + ... + \Lambda_1 X_i^{j+\nu-1} + X_i^{j+\nu} = 0, \text{ сложим по всем } i \in \{1...\nu\}.$$

$$\Lambda_\nu S_j + \Lambda_{\nu-1} S_{j+1} + ... + \Lambda_1 S_{j+\nu-1} + S_{j+\nu} = 0.$$

Получаем систему линейных уравнений с неизвестными Λ_i:

$$\star \left\{ \begin{array}{rcl} \Lambda_\nu S_1 + \Lambda_{\nu-1} S_2 + ... + \Lambda_1 S_\nu & = & -S_{\nu+1} \\ \Lambda_\nu S_2 + \Lambda_{\nu-1} S_3 + ... + \Lambda_1 S_{\nu+1} & = & -S_{\nu+2} \\ ... & & \\ \Lambda_\nu S_\nu + \Lambda_{\nu-1} S_{\nu+1} + ... + \Lambda_1 S_{2\nu-1} & = & -S_{2\nu} \end{array} \right.$$

Матрица этой системы:

$$\begin{pmatrix} S_1 & S_2 & ... & S_\nu \\ S_2 & S_3 & ... & S_{\nu+1} \\ ... & ... & ... & ... \\ S_\nu & S_{\nu+1} & ... & S_{2\nu-1} \end{pmatrix}$$

– является подматрицией матрицы M и имеет размер $\nu \times \nu$, следовательно является линейно независимой. Система Крамеровская и $\Lambda_1, \Lambda_2, ..., \Lambda_\nu$ находятся. □

Замечание 6. Система $\star$ в общем виде выглядит иначе:

$$\left\{ \begin{array}{rcl} \Lambda_\nu S_1 + \Lambda_{\nu-1} S_2 + ... + \Lambda_1 S_\nu & = & -S_{\nu+1} \\ \Lambda_\nu S_2 + \Lambda_{\nu-1} S_3 + ... + \Lambda_1 S_{\nu+1} & = & -S_{\nu+2} \\ ... & & \\ \Lambda_\nu S_t + \Lambda_{\nu-1} S_{t+1} + ... + \Lambda_1 S_{2t-1} & = & -S_{2t} \end{array} \right.$$

но, находясь в рамках условия теоремы, решение сокращённой системы является решением общей.

В общем случае, вообще говоря это не верно.

Предложение 7. *Алгоритм исправления ошибок:*

1. *(предварительные вычисления) Вычисляем* $S_1, S_2, \ldots, S_{2t}$.
2. *(инициализация)* $\nu = t$.
3. *(шаг цикла) Считаем* $\Delta = \begin{vmatrix} S_1 & \ldots & S_\nu \\ \ldots & \ldots & \ldots \\ S_\nu & \ldots & S_{2\nu-1} \end{vmatrix}$.
4. *(условие цикла) Если* $\Delta = 0$, *то* $\nu = \nu - 1$ *и повторяем шаг 3.*
5. *(вычисляем коэффиценты* $\Lambda(x)$*) Решаем систему, находим* $\Lambda_1, \Lambda_2, \ldots, \Lambda_\nu$.
6. *(поиск локаторов) Подбираем корни* $\Lambda(x)$, *находим* $X_1, X_2, \ldots, X_\nu$.
7. *(востанавливаем* $e(x)$*) Находим* $i_1, i_2, \ldots, i_\nu$.

2 Алгоритм Берлекэмпа

Постановка задачи. Даны $S_1, S_2, \ldots, S_{2t} \in \mathrm{GF}(2^m)$ и система

$$\left\{\begin{array}{lcl} \Lambda_\nu S_1 + \Lambda_{\nu-1} S_2 + \ldots + \Lambda_1 S_\nu & = & -S_{\nu+1} \\ \Lambda_\nu S_2 + \Lambda_{\nu-1} S_3 + \ldots + \Lambda_1 S_{\nu+1} & = & -S_{\nu+2} \\ \ldots & & \\ \Lambda_\nu S_t + \Lambda_{\nu-1} S_{t+1} + \ldots + \Lambda_1 S_{2t-1} & = & -S_{2t} \end{array}\right., \nu \leqslant t.$$

Необходимо найти решение, состоящее из: наименьшего ν и $\Lambda_1, \Lambda_2, \ldots, \Lambda_\nu \in \mathrm{GF}(2^m)$.

Пусть $\Lambda(x)$ – многочлено степени L со свободным члено 1 ($\Lambda_0 = 1$).

Определение 8. $\Lambda(x)$ *порождает* $S_1, S_2, \ldots, S_r$, *если* $\forall \rho \in \{L+1, \ldots, r\}$ *выполняется*

$$\Sigma_{j=0}^{L} \Lambda_j S_{p-j} = 0.$$

Теперь задачу можно сформулировать иначе: необходимо найти многочлен наименьшей степени порождающий все $S_1, S_2, \ldots, S_{2t}$.

Будем действовать интерационно, подгоняя $\Lambda(x)$ под синдромы.

Предложение 9. *Алгоритм Берлекэмпа:*

1. *(инициализация)* $\Lambda^{(0)}(x) = 1$ *– многочлен который мы строим,* $B^{(0)}(x) = 1$, $L(0) = 0$, $r = 1$ *– вспомогательные элементы.*
2. *(строим неувязку)* $\Delta_r = \Sigma_{j=0}^{L(r-1)} \Lambda_j^{(r-1)} S_{r-j}$.
3. *(*$\Delta_r = 0$*) Если* $\Delta_r = 0$, *то* $\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x)$, $L(r) = L(r-1)$.
4. *(*$\Delta_r \neq 0$*) Если* $\Delta_r \neq 0$, *то* $\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) - \Delta_r x\, B^{(r-1)}(x)$, $L(r) = \max\{L(r-1), r - L(r-1)\}$.
5. *(пересчитываем* $B^{(r)}$*)*

$$B^{(r)}(x) = \left\{\begin{array}{l} B^{(r-1)}(x) x, \text{ если } L(r) = L(r-1) \\ \Delta_r^{-1} \Lambda^{(r-1)}(x), \text{ если } L(r) > L(r-1). \end{array}\right.$$

6. *(шаг) Если* $r < 2t$, *то продолжить выполнение с шага 2 при* $r = r+1$.

Докажем корректность.

Лемма 10. *Пусть* $\Lambda^{(r-1)}(x)$ *и* $\Lambda^{(r)}(x)$ *многочлены наименьших степеней порождающие синдромы* S_1, S_2, ..., S_{r-1} *и* S_1, S_2, ..., S_r *соответственно;* $L(r-1)=\deg\Lambda^{(r-1)}(x)$, $L(r)=\deg\Lambda^{(r)}(x)$ *и* $\Lambda^{(r-1)}(x)\neq\Lambda^{(r)}(x)$, *тогда* $L(r)\geqslant\max\{L(r-1), r-L(r-1)\}$.

Доказательство. Из минимальности $\Lambda^{(r-1)}$ следует, что $L^{(r-1)}\leqslant L^{(r)}$, остаётся доказать, что $r-L(r-1)\leqslant L(r)$. Предположим обратное:

$$r-L(r-1)>L(r) \text{ или, что тоже самое, } r-L(r)>L(r-1).$$

Из условия теоремы, мы имеем:

$$\forall\rho\in\{L(r-1)+1, r-1\} \text{ имеем } \Sigma_{j=0}^{L(r-1)}\Lambda_j^{(r-1)}S_{\rho-j}=0\Rightarrow S_\rho=-\Sigma_{j=1}^{L(r-1)}\Lambda_j^{(r-1)}S_{\rho-j};$$

$$\forall\rho\in\{L(r)+1, r\} \text{ имеем } \Sigma_{j=0}^{L(r)}\Lambda_j^{(r)}S_{\rho-j}=0\Rightarrow S_\rho=-\Sigma_{j=1}^{L(r)}\Lambda_j^{(r)}S_{\rho-j}.$$

При этом получаем:

$$S_r\neq-\Sigma_{j=1}^{L(r-1)}\Lambda_j^{(r-1)}S_{r-j} \text{ , где } r-j \text{ пробегает от } r-1 \text{ до } r-L(r-1)\text{, что больше } L(r);$$

$$S_r=-\Sigma_{j=1}^{L(r)}\Lambda_j^{(r)}S_{r-j} \text{ , где } r-j \text{ пробегает от } r-1 \text{ до } r-L(r)\text{, что больше } L(r-1).$$

Таким образом подставляя первые уравнения во вторые (что допустимо из оценок на интервалы по которым пробегают параметры) получаем:

$$S_r\neq-\Sigma_{j=1}^{L(r-1)}\Lambda_j^{(r-1)}(-\Sigma_{i=1}^{L(r)}\Lambda_i^{(r)}S_{r-j-i}),$$

$$S_r=-\Sigma_{j=1}^{L(r)}\Lambda_j^{(r)}(-\Sigma_{i=1}^{L(r-1)}\Lambda_i^{(r-1)}S_{r-j-i})$$

– противоречие, так как одна сумма получается из другой переименованием переменных. □

Лемма 11. *Пусть* $\forall i\in\{1, ..., r-1\}$ $\Lambda^{(i)}(x)$ *наименьший многочлен порождающий* S_1, S_2, ..., S_i; $L(i)=\deg\Lambda^{(i)}(x)$; *и* $\Lambda^{(r-1)}(x)$ *не порождает* S_r. *Тогда* $\star$ $\Lambda^{(r)}(x)=\Lambda^{(r-1)}(x)-\Delta_r\Delta_m^{-1}x^{r-m}\Lambda^{(m-1)}(x)$, *где* m *– последний номер, где произошло увеличение* ($L(m-1)<L(m)$), *порождает* $S_1, S_2, ..., S_r$, *имеет наименьшую степень, и* $\deg\Lambda^{(r)}(x)=\max\{L(r-1), r-L(r-1)\}$.

Доказательство. По из условия на m мы имеем $L(r-1)=L(m)>L(m-1)$;

$$\Sigma_{j=0}^{L(r-1)}\Lambda_j^{(r-1)}S_{p-j}=\begin{cases}0\text{ , если } p\in\{L(r-1)+1, ..., r-1\}\\ \Delta_r\text{ , если } p=r.\end{cases}$$

Можно считать, что

$$\Sigma_{j=0}^{L(m-1)}\Lambda_j^{(m-1)}S_{p-j}=\begin{cases}0\text{ , если } p\in\{L(m-1)+1, ..., m-1\}\\ \Delta_r\neq0\text{ , если } p=m,\end{cases}$$

при этом $L(m)=m-L(m-1)$.

Найдём степень $\Lambda^{(r)}(x)$ из формулы $\star$:

$$\begin{array}{rcll}\deg\Lambda^{(r)}(x) & \leqslant & \max\{L(r-1), L(m-1)+r-m\} & =\\ & = & \max\{L(r-1), r-L(m)\} & =\\ & = & \max\{L(r-1), r-L(r-1)\}. & \end{array}$$

Покажем, что $\Lambda^{(r)}(x)$ порождает $S_1, S_2, ..., S_r$, тогда по Лемме 10: $\deg\Lambda^{(r)}(x)\geqslant\max\{L(r-1), r-L(r-1)\}$, таким образом, учитывая предыдущее, степень $\Lambda^{(r)}(x)$ будет точно

$$\deg\Lambda^{(r)}(x)\geqslant\max\{L(r-1), r-L(r-1)\},$$

то есть $\Lambda^{(r)}(x)$ – многочлен наименьшей степени порождающий $S_1, S_2, ..., S_r$.

Считаем j-й коэффицент в $\Lambda^{(r)}(x)$:

$$\Lambda_j^{(r)} = \Lambda_j^{(r-1)} - \Delta_r \Delta_m^{-1} \Lambda_{j-r+m}^{(m-1)}\text{ , где } \Lambda_i^{(m-1)} = 0,\text{ для } i < 0.$$

$$\begin{aligned}
\Sigma_{j=0}^{L(r)} \Lambda_j^{(r)} S_{p-j} &= \Sigma_{j=0}^{L(r-1)} \Lambda_j^{(r-1)} S_{p-j} - \Delta_r \Delta_m^{-1} \Sigma_{j=0}^{L(m-1)} \Lambda_j^{(m-1)} S_{p-r+m-j} &&= \\
&= [p \in \{L(r)+1, ..., r\} \Rightarrow p - r + m \leqslant m] &&= \\
&= [\Sigma_{j=0}^{L(m-1)} \Lambda_j^{(m-1)} S_t = \begin{cases} 0 \text{ , при } t < m \\ \Delta_m \text{ , при } t = m \end{cases}] &&= \\
&= \begin{cases} 0 + 0 = 0 \text{ , при } p \leqslant r - 1 \\ \Delta_r - \Delta_r \Delta_m^{-1} \Delta_m = 0 \text{ , при } p = m. \end{cases}
\end{aligned}$$

□

$\|GF(2^m)\|$	$g(x)$	n	k	$d_{\text{БЧХ}}$	корни
2^3	x^3+x+1	7	4	3	α, α^2
2^4	x^4+x+1	15	11	3	α, α^2
	$(x^4+x+1)(x^4+x^3+x^2+x+1)$	15	7	5	$\alpha, \alpha^2, \alpha^3, \alpha^4$
	$(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$	15	5	7	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$
2^5	x^5+x^2+1	31	26	3	α, α^2
	$(x^5+x^2+1)(x^5+x^4+x^3+x^2+1)$	31	21	5	$\alpha, \alpha^2, \alpha^3, \alpha^4$
	$(x^5+x^2+1)(x^5+x^4+x^2+x+1)(x^5+x^4+x^3+x^2+1)$	31	16	7	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$
	$(x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1)$				
	$(x^5+x^4+x^3+x^2+1)$	31	11	11	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \ldots$
	$(x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^2+x+1)$				
	$(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)$	31	6	15	$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \ldots$
2^6		63	57	3	
		63	51	5	
		63	45	7	
		63	39	9	
		63	36	11	
		63	30	13	
		63	24	15	
		63	18	21	