Теория кодирования

МФТИ, осень 2013

Александр Дайняк

www.dainiak.com

Циклический код

Циклический код — это линейный код, такой, что для любого кодового слова $(a_0, a_1 \dots, a_{n-1})$
слово $(a_{n-1}, a_0 \dots, a_{n-2})$ также является кодовым.

Т.е. циклический сдвиг кодового слова также является кодовым словом.

Циклический код

Например, $[7,4,3]$-код Хемминга эквивалентен циклическому коду с проверочной матрицей

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

Алгебраическое определение циклических кодов

Сопоставим слову

$$(a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$$

многочлен

$$f \coloneqq a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x]$$

Тогда слову $(a_{n-1}, a_0 \ldots, a_{n-2})$ отвечает многочлен

$$a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} = x \cdot f - a_{n-1}(x^n - 1)$$

Алгебраическое определение циклических кодов

Перейдём в кольцо $\mathbb{F}_q[x]/(x^n - 1)$.

Слову $(a_0, \dots, a_{n-1})$ отвечает элемент кольца

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1},$$

а слову $(a_{n-1}, a_0 \dots, a_{n-2})$ отвечает элемент

$$x \cdot f - a_{n-1}(x^n - 1) \overset{\text{в кольце}}{=} x \cdot f$$

Вывод: циклический сдвиг слова эквивалентен умножению соответствующего многочлена на x в кольце $\mathbb{F}_q[x]/(x^n - 1)$.

Алгебраическое определение циклических кодов

Циклический код — это подмножество C кольца $\mathbb{F}_q[x]/(x^n - 1)$, такое, что

- $f_1, f_2 \in C \quad \Rightarrow \quad \forall \alpha, \beta \in \mathbb{F}_q \quad \alpha f_1 + \beta f_2 \in C$
- $f \in C \quad \Rightarrow \quad x \cdot f \in C$

Циклический код — идеал кольца

Утверждение.
Для любого ц.к. $C \subseteq \mathbb{F}[x]/(x^n - 1)$ выполнено
$$f \in C \quad \Rightarrow \quad \forall g \in \mathbb{F}[x]/(x^n - 1) \quad f \cdot g \in C$$

Доказательство: утверждение непосредственно следует из алгебраического определения ц.к.

Циклический код — идеал кольца

Утверждение.
Любой циклический код $C \subseteq \mathbb{F}[x]/(x^n - 1)$ может быть представлен в виде

$$\{f \cdot g \quad | \quad f \in \mathbb{F}[x]/(x^n - 1)\}$$

для некоторого фиксированного многочлена g.

Циклический код — идеал кольца

Доказательство:

Пусть C — ц.к. Рассмотрим $g_0 \in C$, такой, что

$$\deg g_0 = \min_{\substack{g \in C \\ g \not\equiv 0}} \deg g$$

Тогда любой многочлен $f \in C$ кратен g_0. Действительно, поделим f на g_0 с остатком:

$$f(x) = g_0(x) \cdot \tilde{f}(x) + r(x)$$

где $\deg r < \deg g_0$.

Но $r = f - \tilde{f} \cdot g_0 \in C$, а значит $r \equiv 0$.

Единственность порождающего многочлена

Нормированный многочлен — это многочлен с коэффициентом 1 при мономе старшей степени.

Утверждение.
В любом ц.к. ненулевой нормированный многочлен минимальной степени единственен.

Этот многочлен называется *порождающим многочленом* циклического кода.

Единственность порождающего многочлена

Доказательство:

Допустим, что в коде C нашлись два разных нормногочлена минимальной степени:

$$g_1(x) = x^l + \cdots$$
$$g_2(x) = x^l + \cdots$$

Но тогда $(g_1 - g_2) \in C$ и $\deg(g_1 - g_2) < l$ — это противоречит минимальности l.

Критерий существования циклического кода

Теорема.
Нормногочлен $g \in \mathbb{F}[x]/(x^n - 1)$ может быть порождающим многочленом циклического кода т. и т.т., когда он является делителем многочлена $(x^n - 1)$ в кольце $\mathbb{F}[x]$.

Критерий существования циклического кода: достаточность

Доказательство $g|(x^n - 1) \quad \Rightarrow \quad \exists\text{ц. к.}$

Пусть $g(x) \mid (x^n - 1)$.

Положим

$$C \coloneqq \{fg, \quad \text{где } f \in \mathbb{F}[x]/(x^n - 1)\}$$

Очевидно, C — циклический код.

Осталось доказать, что g — порождающий многочлен кода C, то есть что в C любой ненулевой многочлен имеет степень $> \deg g$, либо равен $\mathrm{const} \cdot g$.

Критерий существования циклического кода: достаточность

Рассмотрим произвольный многочлен $\tilde{g} \in C$.

Имеем $\tilde{g} = fg$ для некоторого $\mathbb{F}[x]/(x^n - 1)$.

Тогда в кольце $\mathbb{F}[x]$ для тех же самых f и $\tilde{g}$ и некоторого s выполнено равенство

$$\tilde{g} = f \cdot g + s \cdot (x^n - 1)$$

По условию, $(x^n - 1) = r \cdot g$ для некоторого $r \in \mathbb{F}[x]$, следовательно

$$\tilde{g} = f \cdot g + sr \cdot g = (f + sr) \cdot g$$

Критерий существования циклического кода: достаточность

Итак, в кольце $\mathbb{F}[x]$ для некоторых f, r, s имеем

$$\tilde{g} = (f + sr) \cdot g$$

Возможны случаи:

- $(f + sr) \equiv 0$ — тогда $\tilde{g} \equiv 0$
- $(f + sr) \equiv \mathrm{const} \neq 0$ — тогда $\tilde{g} = \mathrm{const} \cdot g$
- $\deg(f + sr) \geq 1$ — тогда $\deg \tilde{g} > \deg g$

Критерий существования циклического кода: необходимость

Доказательство $\exists\text{ц.к.} \Rightarrow g|(x^n - 1)$

Пусть C — циклический код в $\mathbb{F}[x]/(x^n - 1)$ с порождающим многочленом g.

Поделим в кольце $\mathbb{F}[x]$ с остатком $(x^n - 1)$ на g:

$$x^n - 1 = f \cdot g + r$$

где $\deg r < \deg g$.

Тогда в кольце $\mathbb{F}[x]/(x^n - 1)$ имеем

$$r = (-f) \cdot g \in C$$

Отсюда $r \equiv 0$, то есть $g|(x^n - 1)$.

Размерность и порождающая матрица циклического кода

Утверждение.
Пусть порождающий многочлен циклического кода $C \subseteq \mathbb{F}_q[x]/(x^n - 1)$ имеет вид

$$c_0 + c_1 x + \cdots + c_{\alpha-1} x^{\alpha-1} + x^{\alpha}$$

Тогда, если рассматривать C как подпространство $\mathbb{F}_q^n$, то $\dim C = n - \alpha$ и порождающая матрица кода имеет вид

$$\begin{pmatrix} c_0 & c_1 & \dots & c_{\alpha-1} & 1 & 0 & \dots & \dots & 0 \\ 0 & c_0 & c_1 & \dots & c_{\alpha-1} & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & c_0 & c_1 & \dots & c_{\alpha-1} & 1 \end{pmatrix}$$

Размерность и порождающая матрица циклического кода

Доказательство:

Очевидно, что строки матрицы

$$\begin{pmatrix} c_0 & c_1 & \dots & c_{\alpha-1} & 1 & 0 & \dots & \dots & 0 \\ 0 & c_0 & c_1 & \dots & c_{\alpha-1} & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & c_0 & c_1 & \dots & c_{\alpha-1} & 1 \end{pmatrix}$$

линейно независимы и её ранг равен $(n-\alpha)$.

Остаётся доказать равенство $\dim C = n - \alpha$.

Размерность и порождающая матрица циклического кода

Для произвольного $f \in \mathbb{F}_q[x]/(x^n - 1)$ положим

$$C_f := \{f + h \mid h \in C\}.$$

Докажем, что если $f_1 \neq f_2$ и $\deg f_i < \alpha$, то

$$C_{f_1} \cap C_{f_2} = \emptyset$$

Допустим, что $C_{f_1} \cap C_{f_2} \neq \emptyset$. Это означает, что $f_1 + h_1 = f_2 + h_2$ для некоторых $h_1, h_2 \in C$.

Тогда $f_1 - f_2 = h_2 - h_1 \in C$.

Но тогда из условия $\deg(f_1 - f_2) < \alpha$ вытекает, что $f_1 - f_2 \equiv 0$ — противоречие.

Размерность и порождающая матрица циклического кода

Пусть

$$f_1, \dots, f_{q^\alpha} \in \mathbb{F}_q[x]/(x^n - 1)$$

— всевозможные многочлены степени $< \alpha$.

Так как $C_{f_i} \cap C_{f_j} = \emptyset$ при $i \neq j$, то

$$\left|C_{f_1}\right| + \cdots + \left|C_{f_{q^\alpha}}\right| \leq \left|\mathbb{F}_q[x]/(x^n - 1)\right| = q^n$$

Очевидно, $\left|C_{f_i}\right| = |C|$ для каждого i, а значит

$$|C| \leq \frac{q^n}{q^\alpha} = q^{n-\alpha}$$

Следовательно, $\dim C \leq n - \alpha$.

Размерность и порождающая матрица циклического кода

Доказанное утверждение:

Если код C имеет порождающий многочлен

$$c_0 + c_1 x + \cdots + c_{\alpha-1} x^{\alpha-1} + x^{\alpha}$$

то порождающая матрица кода C имеет вид

$$\begin{pmatrix} c_0 & c_1 & \dots & c_{\alpha-1} & 1 & 0 & \dots & \dots & 0 \\ 0 & c_0 & c_1 & \dots & c_{\alpha-1} & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & c_0 & c_1 & \dots & c_{\alpha-1} & 1 \end{pmatrix}$$

Следствие.

Код C можно представить в виде

$$\{f \cdot g \quad | \quad f \in \mathbb{F}[x]/(x^n - 1)\,, \quad \deg f < n - \alpha\}$$

Систематическое кодирование циклических кодов

Утверждение.
У любого циклического кода существует порождающая матрица канонического вида.
(Т.е. любой ц.к. допускает систематическое кодирование.)

Замечание.
Важно, что *сам* код допускает систематическое кодирование.
Не нужно переходить к эквивалентному коду.

Систематическое кодирование циклических кодов

Доказательство:

Пусть g — порождающий многочлен, $\deg g = \alpha$.

Поделим многочлены $x^{\alpha}, x^{\alpha+1}, \dots, x^{n-1}$ с остатком на g:

$$\begin{array}{ccc} x^{\alpha} & = & h_0 \cdot g + r_0 \\ & \vdots & \\ x^{n-1} & = & h_{n-\alpha-1} \cdot g + r_{n-\alpha-1} \end{array}$$

Перепишем:

$$\begin{array}{ccc} h_0 \cdot g & = & x^{\alpha} - r_0 \\ & \vdots & \\ h_{n-\alpha-1} \cdot g & = & x^{n-1} - r_{n-\alpha-1} \end{array}$$

Систематическое кодирование циклических кодов

Имеем

$$\begin{array}{rcl} h_0 \cdot g & = & x^{\alpha} - r_0 \\ & \vdots & \\ h_{n-\alpha-1} \cdot g & = & x^{n-1} - r_{n-\alpha-1} \end{array}$$

Каждый из многочленов $h_i \cdot g$ принадлежит C и имеет вид

$$x^{\alpha+i} + c_{i,\alpha-1}x^{\alpha-1} + c_{i,\alpha-2}x^{\alpha-2} + \cdots + c_{i,0}$$

где $c_{i,j}$ — некоторые коэффициенты.

Систематическое кодирование циклических кодов

Многочлены $h_i \cdot g$ принадлежат C и имеют вид

$$x^{\alpha+i} + c_{i,\alpha-1}x^{\alpha-1} + c_{i,\alpha-2}x^{\alpha-2} + \cdots + c_{i,0}.$$

Составим из их коэффициентов порождающую матрицу кода C, она будет иметь вид

$$\begin{pmatrix} c_{0,0} & \dots & c_{0,\alpha-1} & 1 & 0 & \dots & 0 \\ c_{1,0} & \dots & c_{1,\alpha-1} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & & & \ddots & \\ c_{n-\alpha-1,0} & \dots & c_{n-\alpha-1,\alpha-1} & 0 & 0 & \dots & 1 \end{pmatrix}$$

Систематическое кодирование циклических кодов

Итак, у кода C есть порождающая матрица вида

$$\begin{pmatrix} c_{0,0} & \cdots & c_{0,\alpha-1} & 1 & 0 & \cdots & 0 \\ c_{1,0} & \cdots & c_{1,\alpha-1} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & & \ddots & \\ c_{n-\alpha-1,0} & \cdots & c_{n-\alpha-1,\alpha-1} & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Т.к. код C циклический, то можно циклически переставить столбцы в этой матрице, и получится искомая матрица вида $\left(I|\tilde{G}\right)$, где I — единичная матрица порядка $(n-\alpha)$.

Проверочный многочлен

Пусть g — порождающий многочлен кода C.

Так как $g|(x^n - 1)$, то в кольце $\mathbb{F}[x]$ имеем

$$x^n - 1 = g \cdot h$$

для некоторого $h \in \mathbb{F}[x]$.

Многочлен $h(x)$ называется *проверочным многочленом* кода C.

Для любого $f \in C$ в кольце $\mathbb{F}[x]/(x^n - 1)$ выполнено равенство

$$f \cdot h = 0.$$

Проверочная матрица циклического кода

Утверждение.
Пусть проверочный многочлен циклического кода $C \subseteq \mathbb{F}[x]/(x^n - 1)$ имеет вид

$$h_0 + h_1 x + \cdots + h_{n-\alpha} x^{n-\alpha}$$

Тогда, если рассматривать C как обычный линейный код, то его проверочная матрица будет иметь вид

$$\begin{pmatrix} h_{n-\alpha} & \dots & h_1 & h_0 & 0 & \dots & \dots & 0 \\ 0 & h_{n-\alpha} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & h_{n-\alpha} & \dots & h_1 & h_0 \end{pmatrix}$$

Проверочная матрица циклического кода

Доказательство:

Пусть проверочный многочлен циклического кода $C \subseteq \mathbb{F}[x]/(x^n - 1)$ имеет вид

$$h_0 + h_1 x + \cdots + h_{n-\alpha} x^{n-\alpha}$$

Для любого многочлена

$$c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in C$$

в кольце $\mathbb{F}[x]/(x^n - 1)$ выполнено равенство

$$(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \cdot (h_0 + h_1 x + \cdots + h_{n-\alpha} x^{n-\alpha}) = 0$$

Проверочная матрица циклического кода

Для удобства формально введём $h_{n-\alpha+1} = h_{n-\alpha+2} = \cdots = 0.$

В кольце $\mathbb{F}[x]/(x^n - 1)$ выполнено равенство

$$0 = (c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) \cdot (h_0 + h_1 x + \cdots + h_{n-1} x^{n-1})$$

$$= \sum_{m=0}^{2n-2} x^m \sum_{i=0}^{m} c_i h_{m-i}$$

В $\mathbb{F}[x]/(x^n - 1)$ выполнено $x^{n+t} = x^t$, отсюда

$$\sum_{m=0}^{2n-2} x^m \sum_{i=0}^{m} c_i h_{m-i} = \sum_{m=0}^{n-1} x^m \sum_{i=0}^{m} c_i h_{m-i} + \sum_{m=0}^{n-1} x^m \sum_{i=m+1}^{n-1} c_i h_{m+n-i}$$

Проверочная матрица циклического кода

В кольце $\mathbb{F}[x]/(x^n - 1)$ выполнены равенства

$$0 = \sum_{m=0}^{n-1} x^m \sum_{i=0}^{m} c_i h_{m-i} + \sum_{m=0}^{n-1} x^m \sum_{i=m+1}^{n-1} c_i h_{m+n-i}$$

Отсюда при каждом $m \in \{0, \dots, n-1\}$ должно быть выполнено

$$\sum_{i=0}^{m} c_i h_{m-i} + \sum_{i=m+1}^{n-1} c_i h_{m+n-i} = 0$$

Проверочная матрица циклического кода

При каждом $m \in \{0, \dots, n-1\}$ должно быть выполнено

$$\sum_{i=0}^{m} c_i h_{m-i} + \sum_{i=m+1}^{n-1} c_i h_{m+n-i} = \sum_{i=0}^{n-1} c_i h_{(m-i) \bmod n} = 0$$

При $m \in \{n-\alpha, \dots, n-1\}$ уравнения

$$\sum_{i=0}^{n-1} c_i h_{(m-i) \bmod n} = 0$$

как раз и задаются матрицей

$$\begin{pmatrix} h_{n-\alpha} & \dots & h_1 & h_0 & 0 & \dots & \dots & 0 \\ 0 & h_{n-\alpha} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & h_{n-\alpha} & \dots & h_1 & h_0 \end{pmatrix}$$

Проверочная матрица циклического кода

Доказали, что кодовые слова удовлетворяют системе, задаваемой матрицей

$$\begin{pmatrix} h_{n-\alpha} & \dots & h_1 & h_0 & 0 & \dots & \dots & 0 \\ 0 & h_{n-\alpha} & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & 0 & h_{n-\alpha} & \dots & h_1 & h_0 \end{pmatrix}$$

То, что эта матрица проверочная (т.е. никакие «лишние» слова не удовлетворяют системе), следует из того, что её ранг равен α, а размерность кода равна $(n-\alpha)$.

Лемма Вандермонда (A.—T. Vandermonde)

Имеет место *формула Вандермонда*:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_r \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_1^{r-1} & \lambda_2^{r-1} & \cdots & \lambda_r^{r-1} \end{vmatrix} = \prod_{1 \le i < j \le r} (\lambda_j - \lambda_i)$$

Из неё следует, что матрица невырождена при $\lambda_j \neq \lambda_i$.

Доказательство индукцией по r.

База: $r = 1$. Очевидно: $\begin{vmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{vmatrix} = \lambda_2 - \lambda_1$.

Лемма Вандермонда

Индуктивный переход:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_1 & \lambda_2 & \cdots & \lambda_r \\ \vdots & \vdots & \cdots & \vdots \\ \lambda_1^{r-1} & \lambda_2^{r-1} & \cdots & \lambda_r^{r-1} \end{vmatrix} = \begin{vmatrix} 1 & 0 & \cdots & 0 \\ \lambda_1 & \lambda_2 - \lambda_1 & \cdots & \lambda_r - \lambda_1 \\ \vdots & \vdots & \cdots & \vdots \\ \lambda_1^{r-1} & \lambda_2^{r-1} - \lambda_1^{r-1} & \cdots & \lambda_r^{r-1} - \lambda_1^{r-1} \end{vmatrix} =$$

$$= \begin{vmatrix} \lambda_2 - \lambda_1 & \cdots & \lambda_r - \lambda_1 \\ \lambda_2^2 - \lambda_1^2 & \cdots & \lambda_r^2 - \lambda_1^2 \\ \vdots & \cdots & \vdots \\ \lambda_2^{r-2} - \lambda_1^{r-2} & \cdots & \lambda_r^{r-2} - \lambda_1^{r-2} \\ \lambda_2^{r-1} - \lambda_1^{r-1} & \cdots & \lambda_r^{r-1} - \lambda_1^{r-1} \end{vmatrix} = \begin{vmatrix} \lambda_2 - \lambda_1 & \cdots & \lambda_r - \lambda_1 \\ \lambda_2^2 - \lambda_1\lambda_2 & \cdots & \lambda_r^2 - \lambda_1\lambda_r \\ \vdots & \cdots & \vdots \\ \lambda_2^{r-2} - \lambda_1\lambda_2^{r-3} & \cdots & \lambda_r^{r-2} - \lambda_1\lambda_r^{r-3} \\ \lambda_2^{r-1} - \lambda_1\lambda_2^{r-2} & \cdots & \lambda_r^{r-1} - \lambda_1\lambda_r^{r-2} \end{vmatrix} =$$

$$= \left(\prod_{i=2}^{r}(\lambda_i - \lambda_1)\right) \cdot \det \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_2 & \lambda_3 & \cdots & \lambda_r \\ \vdots & \vdots & \cdots & \vdots \\ \lambda_2^{r-2} & \lambda_3^{r-2} & \cdots & \lambda_r^{r-2} \end{vmatrix} = \prod_{1 \le i < j \le r} (\lambda_j - \lambda_i)$$

Примитивный элемент

Рассмотрим поле $\mathbb{F}_q$, где $q = p^m$, p простое.

Известно, что множество $\mathbb{F}_q \setminus \{0\}$ образует циклическую группу по умножению.

Каждый образующий элемент этой группы (порядок которого равен $(q-1)$) называется *примитивным элементом поля*.

Иными словами, примитивный элемент — это такой $\lambda \in \mathbb{F}_q$, что $\{1, \lambda, \lambda^2, \dots, \lambda^{q-2}\} = \mathbb{F}_q \setminus \{0\}$.

Граница Боуза—Чоудхури—Хоквингема

Теорема. (A.Hocquenghem’1959,
R.C. Bose and D.K. Ray-Chaudhuri’1960)

Пусть λ — примитивный элемент $\mathbb{F}_q$, и $\delta \leq q$.

Пусть порождающий многочлен g кода $C \subseteq \mathbb{F}_q^n$ таков, что в $\mathbb{F}_q$ среди его корней есть числа

$$\lambda^b, \lambda^{b+1}, \ldots, \lambda^{b+\delta-2}$$

Тогда $d(C) \geq \delta$.

Граница Боуза—Чоудхури—Хоквингема

Доказательство:

Рассмотрим произвольный $f(x) \in C$.

Найдётся многочлен $s(x) \in \mathbb{F}_q[x]/(x^n - 1)$, такой, что $\deg s < n - \deg g$ и в кольце $\mathbb{F}_q[x]/(x^n - 1)$ выполнено равенство

$$f(x) = s(x) \cdot g(x)$$

Так как $\deg s + \deg g < n$, то это равенство выполнено и в кольце $\mathbb{F}_q[x]$.

Граница Боуза—Чоудхури—Хоквингема

В кольце $\mathbb{F}_q[x]$ справедливо равенство

$$f(x) = s(x) \cdot g(x)$$

Пусть $\lambda^b, \dots, \lambda^{b+\delta-2}$ — различные корни $g(x)$.

Они же будут корнями f.

Пусть $f = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$.

Вектор $(c_0, \dots, c_{n-1})$ удовлетворяет системе линейных уравнений с матрицей

$$\begin{pmatrix} 1 & \lambda^b & \cdots & \lambda^{b(n-1)} \\ 1 & \lambda^{b+1} & \cdots & \lambda^{(b+1)(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda^{b+\delta-2} & \cdots & \lambda^{(b+\delta-2)(n-1)} \end{pmatrix}$$

Граница Боуза—Чоудхури—Хоквингема

Любой кодовый вектор удовлетворяет системе с матрицей

$$\widetilde{H} = \begin{pmatrix} 1 & \lambda^{b} & \cdots & \lambda^{b(n-1)} \\ 1 & \lambda^{b+1} & \cdots & \lambda^{(b+1)(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda^{b+\delta-2} & \cdots & \lambda^{(b+\delta-2)(n-1)} \end{pmatrix}$$

(Это не обязательно проверочная матрица кода, но её можно дополнить до проверочной.)

Достаточно доказать, что любые $(\delta-1)$ столбцов матрицы $\widetilde{H}$ линейно независимы.

Граница Боуза—Чоудхури—Хоквингема

$$\widetilde{H} = \begin{pmatrix} 1 & \lambda^{b} & \cdots & \lambda^{b(n-1)} \\ 1 & \lambda^{b+1} & \cdots & \lambda^{(b+1)(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \lambda^{b+\delta-2} & \cdots & \lambda^{(b+\delta-2)(n-1)} \end{pmatrix}$$

Выберем в $\widetilde{H}$ произвольные столбцы $i_1, \ldots, i_{\delta-1}$. Получим матрицу

$$\begin{pmatrix} \lambda^{b\cdot i_1} & \lambda^{b\cdot i_2} & \cdots & \lambda^{b\cdot i_{\delta-1}} \\ \lambda^{(b+1)\cdot i_1} & \lambda^{(b+1)\cdot i_2} & \cdots & \lambda^{(b+1)\cdot i_{\delta-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda^{(b+\delta-2)\cdot i_1} & \lambda^{(b+\delta-2)\cdot i_2} & \cdots & \lambda^{(b+\delta-2)\cdot i_{\delta-1}} \end{pmatrix}$$

Граница Боуза—Чоудхури—Хоквингема

Докажем, что матрица $\widetilde{H}_{i_1,\dots,i_{\delta-1}}$ невырождена. Имеем

$$\begin{vmatrix} \lambda^{b\cdot i_1} & \lambda^{b\cdot i_2} & \cdots & \lambda^{b\cdot i_{\delta-1}} \\ \lambda^{(b+1)\cdot i_1} & \lambda^{(b+1)\cdot i_2} & \cdots & \lambda^{(b+1)\cdot i_{\delta-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda^{(b+\delta-2)\cdot i_1} & \lambda^{(b+\delta-2)\cdot i_2} & \cdots & \lambda^{(b+\delta-2)\cdot i_{\delta-1}} \end{vmatrix} =$$

$$= \lambda^{b\cdot(i_1+\cdots+i_{\delta-1})} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda^{i_1} & \lambda^{i_2} & \cdots & \lambda^{i_{\delta-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda^{(\delta-2)\cdot i_1} & \lambda^{(b-2)\cdot i_2} & \cdots & \lambda^{(\delta-2)\cdot i_{\delta-1}} \end{vmatrix}$$

По лемме Вандермонда, определитель последней матрицы не равен нулю.