Лекция 01.12.2020

Коды Голея G_{23} и G_{24}.

В самом начале курса мы построили совершенный бинарный код Хэмминга $H_4^{(7)}$ типа $[7,4;3]$ и самодвойственный код $H_4^{(8)}$ типа $[8,4;4]$: $\left(H_4^{(8)}\right)^{\perp} = H_4^{(8)}$.

В этой лекции мы построим второй совершенный код G_{23} типа $[23,12;7]$ и самодвойственный код $G_{24} = \overline{G_{23}}$ типа $[24,12;8]$ (G_{24} - чётное расширение G_{23}).

Замечание. Если код G типа $[23,12;7]$ существует, то он совершенный!
$7 = 2\cdot 3 + 1$, поэтому такой код исправляет 3 ошибки. Число элементов в шаре $B_3(0) \subset \mathbb{F}_2^{23}$ равно

$$|B_3(0)| = 1 + C_{23}^1 + C_{23}^2 + C_{23}^2 =$$

$$= 1 + 23 + 253 + 1771 = 2048 \overset{!}{=} 2^{11}$$

Следовательно,

$$\left| \bigsqcup_{m \in C} B_3(m) \right| = |C| \cdot |B_3(0)| = 2^{12} \cdot 2^{11} = 2^{23}$$

и

$$|F_2^{23}| = \left| \bigsqcup_{m \in C} B_3(m) \right| !$$

Мы построим код C как циклический код длины 23. Для этого надо найти разложение кругового многочлена $\Phi_{23}(x)$ над полем F_2:

$$x^{23} - 1 \overset{\mathbb{Z}}{=} (x-1)\,\Phi_{23}(x) \overset{F_2}{=} ???$$

Для исследования $\Phi_{23}(x)$ над F_2 необходимо найти порядок $p = 2$ в $(\mathbb{Z}/23\mathbb{Z})^\times$.

Напоминание: $(n, p) = 1$, $\Phi_n(x)$ раскладется над полем F_p в произведение неприводимых множителей степени d, где $d = \operatorname{ord}_{(\mathbb{Z}/n\mathbb{Z})^\times} p$.

n	1	2	3	4	5	6	7	8	9	10	11	
2^n	2	4	8	16	9	18	13	3	6	12	1	$\bmod 23$

$$\operatorname{ord}_{(\mathbb{Z}/23\mathbb{Z})^\times} 2 = 11 \Rightarrow$$

$$\Phi_{23}(x) = f(x)\cdot g(x), \quad \deg f = \deg g, \quad f, g \in \mathbb{F}_2[x].$$

Замечание. Любой корень f или g является корнем $\Phi_{23}(x)$, т.е. примитивным корнем степени 23 из 1. Эти корни лежат в поле $\mathbb{F}_{2^{11}}$ из 2048 элементов.

Это следствие доказанной теоремы о поведении Φ_n в конечных полях характеристики p.

Как это увидеть в данном конкретном случае?

$\mathbb{F}_{2^{11}}^\times$ — циклическая группа порядка $2^{11}-1$.

Выше мы показали, что $2^{11}-1 \equiv 0 \bmod 23$. Следовательно, группа $\mathbb{F}_{2^{11}}^\times$ содержит элемент порядка 23.

Построение кода длины 23.

Мы установили, что $\Phi_{23}(x) = f(x) \cdot g(x)$.

Определим циклический код по $f(x)$:

$$C_f = \{ a(x) f(x) \bmod x^{23} - 1,\ a(x) \in \mathbb{F}_2[x] \}$$

Имеем $$\boxed{\dim C_f = 23 - \deg f = 12.}$$

Как оценить минимальную дистанцию C_f

$$d(C_f) = \min_{0 \neq m \in C_f} w(m) \quad ?$$

Пусть α корень $f(x)$. (Все эти корни есть корни степени 23 и лежат в поле $\mathbb{F}_{2048} \cong \mathbb{F}_2[x]/(f)$, т.е. за α можно взять $x \bmod f(x)$.)

По α можно найти все корни $f(x)$.

(См. док-во теоремы о многочленах Φ_n.)

$$(f(x))^2 = f(x^2) \Rightarrow f(\alpha^2) = f(\alpha)^2 = 0 \Rightarrow$$

$$\alpha, \alpha^2, \alpha^4, \alpha^8, \dots, \alpha^{2^k}, \dots, \alpha^{2^{10}} =$$

$\alpha^{(1)}, \alpha^{(2)}, \alpha^{(4)}, \alpha^{8}, \alpha^{16}, \alpha^{9}, \alpha^{18}, \alpha^{13}, \alpha^{(3)}, \alpha^{6}, \alpha^{12}$

все 11 корней многочлена $f(x)$:

$$f(x) = \prod_{k=0}^{10} (x - \alpha^{2^k}).$$

Среди степеней корней имеется ровно четыре последовательные степени:

$$\| \; 1, 2, 3, 4. \; \|$$

По теореме об оценке $d(C_f)$ получаем

$$\boxed{d(C_f) \geq 5.}$$

Отметим, что выражения для $f(x)$ нам пока не известно. Как можно найти $f(x)$ явно?

Интересный метод для нахождения разложения $\Phi_{23}(x)$ над $\mathbb{F}_2$.

Попробуем найти многочлен $h(x)$ над $\mathbb{F}_2$ такой, что $h(\alpha) = 0$ для корня степени 23 из 1.

Тогда $f(x) \cdot g(x) = 0$, f и g неприводимые, поэтому $h(x)$ делится на $f(x)$ или $g(x)$. Следовательно, мы можем определить один из них, взяв

$$\text{НОД}\left(x^{23}-1,\ h(x)\right).$$

Рассмотрим разбиение $\left(\mathbb{Z}/23\mathbb{Z}\right)^*$ на два подмножества (т.е. две циклотомические орбиты):

$$R_+ = \{ 2^k \bmod 23 \mid 0 \le k \le 10 \} =$$

$$= \{ 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \},$$

$$R_- = \{ 5 \cdot 2^k \bmod 23 \mid 0 \le k \le 10 \} =$$

$$= \{ 23 - \ell,\ \ell \in R_+ \}.$$

Положим

$$\ell_\pm(x) = \sum_{m \in R_\pm} x^m \in \mathbb{F}_2[x].$$

Степени m образуют две орбиты, инва-

рисентные при умножении на 2 по модулю 23. Это даёт следующее с-во:

$$\ell_\pm(x)^2 \underset{\mathbb{F}_2}{=} \sum_{m\in R_\pm} x^{2m} \equiv \sum_{m\in R_\pm} x^m \bmod (x^{23}-1).$$

Следовательно,

$$\ell_\pm(x)^2 \equiv \ell_\pm(x) \bmod (x^{23}-1), \text{ т.е.}$$

$\ell_\pm(x)$ – два идемпотента в факторкольце $\mathbb{F}_2[x]/(x^{23}-1)$.

(Многочлен $x^{23}-1$ приводимый, поэтому в этом кольце есть делители нуля и идемпотенты ≠1.)

Для любого корня α степени 23 из 1 над полем $\mathbb{F}_2$ имеем

$$\ell_\pm(\alpha)^2 = \ell_\pm(\alpha), \text{ т.к. } \alpha^{23}-1=0.$$

Следовательно, $\ell_\pm(\alpha) = 0 \vee 1$.

Кроме того

$$1 + \ell_+(x) + \ell_-(x) = \frac{x^{23}-1}{x-1}.$$

Следовательно,

$$\ell_+(\alpha) + \ell_-(\alpha) = 1.$$

ИТОГ: мы имеем два варианта

$$\begin{cases} \ell_+(\alpha) = 0 \\ \ell_-(\alpha) = 1 \end{cases} \quad \text{или} \quad \begin{cases} \ell_+(\alpha) = 1 \\ \ell_-(\alpha) = 0 \end{cases}.$$

В любом случае мы можем найти множитель $\Phi_{23}(x)$, вычислив

$$\text{НОД}\left(x^{23}-1,\ \ell_\pm(x)\right) \quad !$$

Алгоритм Евклида даёт

$$\text{НОД}\left(x^{23}-1,\ \ell_+(x)\right) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} = f(x),$$

$$\text{НОД}\left(x^{23}-1,\ \ell_-(x)\right) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11} = g(x).$$

Отметим, что множители взаимны

$$\widetilde{f}(x) = x^{11} f\left(\frac{1}{x}\right) = g(x),$$

что видно и без вычислений явных формул для $f(x)$ и $g(x)$. (Достаточно посмотреть на последовательности степеней корней по модулю 23.)

Основная Теорема лекции

1) $C_f \cong C_g$ изоморфные коды. (Определите соотв. перестановку!)

2) C_f – совершенный код типа $[23, 12; 7]$.

3) Его тётное расширение $\overline{C}_f$ есть автодуальный код типа $[24, 12; 8]$:

$$\overline{C}_f^{\perp} = \overline{C}_f .$$

Д-во. Мы уже доказали, что если C_f имеет тип $[23, 12; 7]$, то он совершенный. Более того, мы установили, что $d(C_f) \geq 5$. Результат $d = 7$ будет следовать из автодуальности. Чтобы это доказать, надо исследовать $\overline{C}^{\perp}$ – ортогональное дополнение тётного расширения любого нетётного кода.

Определение. Пусть C — линейный код в $\mathbb{F}_2^n$. Чётным подкодом

$$C_0 = \{ m \in C \mid w(m) = 0 \bmod 2 \}$$

есть пересечение $C < \mathbb{F}_2^n$ с гиперплоскостью $x_1 + x_2 + \dots + x_n = 0$ в $\mathbb{F}_2^n$.

Следовательно, C_0 — подпространство кода C коразмерности 1.

Лемма 1. Пусть C — линейный код, $\overline{C} = \{ (m, \underbrace{w(m) \bmod 2}_{\overline{w(m)}}) \in \mathbb{F}_2^{n+1} \}$ его чётное расширение. Тогда

$$\overline{C}^{\perp} = (C^{\perp}, 0) \sqcup (C_0^{\perp} \setminus C^{\perp}, 1).$$

Д-во. $C \supset C_0 \Rightarrow C^{\perp} \subset C_0^{\perp}$.

1) Пусть $(a,0) \in \overline{C}^{\perp}$. Тогда линейное скалярное дай'т

$$\big((a,0), (m, \overline{w(m)}) \big) = (a, m) + 0 \cdot \overline{w(m)} = (a, m) = 0,$$

т.е. $a \in C^{\perp}$.

2) $(a,1) \in \overline{C}^{\perp}$, тогда

$\left((a,1), (m, \overline{w}(m))\right) = (a,m) + \overline{w}(m)$.

Если $m \in C_0$, то $\overline{w}(m) = 0$. $\Rightarrow$ $a \in C_0^{\perp}$.

3) Если $b \in C^{\perp}$ и $\exists (\delta, 1) \in C$, то

$$\left((b,1), (\delta,1)\right) = (b,\delta) + 1 = 1.$$

4) Если $a \in C_0^{\perp} \setminus C^{\perp}$, то

$(a, \underbrace{\delta + C_0}) = (a,\delta) = 1$, т.к. $a \notin C^{\perp}$

все нечётные слова C.

5) $\left((a,1), (\delta + C_0, 1)\right) = (a,\delta) + 1 = 0$. ▨

Следствие (Критерий автодуальности).

$$\overline{C}^{\perp} = \overline{C} \Leftrightarrow C^{\perp} = C_0.$$

Д-во.

$$\overline{C} = (C_0, 0) \sqcup (C \setminus C_0, 1)$$

$$\overline{C}^{\perp} = (C^{\perp}, 0) \sqcup (C_0^{\perp} \setminus C^{\perp}, 1)$$

$\overline{C} = \overline{C}^{\perp} \Leftrightarrow$ (равенство первых компонент) $\Leftrightarrow C_0 = C^{\perp}$. ▨

Лемма 2. Для любого многочлена $h(x) \in \mathbb{F}_2[x]$ такого, что $h(1) = 1$ и любого циклического кода $C_{h(x)}$ его чётный подкод циклический и

$$(C_{h(x)})_0 = C_{(x-1)h(x)}.$$

Д-во.

$$C_h = \{ a(x)h(x) \bmod x^n - 1,\ a(x) \in \mathbb{F}_2[x] \}$$

$$(C_h)_0 = \{ a(x)h(x) \bmod x^n - 1,\ a(1)h(1) = 0 \} =$$

$$a(x) = (x-1)b(x)$$

$$= \{ b(x)(x-1)h(x) \bmod (x^n - 1) \} =$$

$$= C_{(x-1)h(x)}. \qquad \blacksquare$$

Д-во автодуальности кода C_f.

$$x^{23} - 1 = f(x)\left((x-1)g(x)\right).$$

Напоминание: $x^n - 1 = a(x)b(x)$, тогда

$$C^{\perp}_{a(x)} = C_{\widetilde{b(x)}}$$

$\widetilde{b(x)}$ – возвратный многочлен.

Вывод.

$$C_f^{\perp} \Rightarrow C_{\widetilde{(x-1)}\,\widetilde{g(x)}} = C_{(x-1)\,f(x)} = (C_f)_0.$$

Автодуальность $\overline{C}_f$ получается из Следствия из Леммы 1. ☞

Докажем теперь, что $d(C_f) = 7$.

1) $\overline{C}_f = \overline{C}_f^{\perp} \Rightarrow \forall\, m, l \in \overline{C}_f \;\; (m, l) = 0$,

следовательно $\underbrace{\#\, m \wedge l}_{\text{число общих единиц}}$ – чётное.

2) $w(m+l) = w(m) + w(l) - 2\#\, m \wedge l$.

3) C_f порождён циклическими перестановками вектора $f(x)$:

$$f \longmapsto (\overset{1+x}{1}, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, \underbrace{0, \dots, 0}_{\text{11 нулей}}) \in \mathbb{F}_2^{23}$$

Следовательно, $\overline{C}_f$ порождён 12 векторами длины 8.

4) Из 2 следует, что

Если $w(u) \equiv w(l) \equiv 0 \mod 4$, то

$$w(u+l) \equiv 0 \mod 4.$$

Для всех базисных векторов $\overline{C}_f$ их вес равен $8 \equiv 0 \mod 4$. Следовательно

$$\forall\ u \in \overline{C}_f \qquad \boxed{w(u) \equiv 0 \mod 4}.$$

Заключаем, что $\overline{C}_f$ не содержит векторов веса 6. Следовательно

$$d(\overline{C}_f) = 8 \quad \text{и} \quad d(C_f) = 7.$$

Основная теорема доказана.