2022-12-05 Week 11 Review Session

The Golay codes. Classification of perfect codes up to parameter equivalence.

The two Golay codes:

* ① The Binary Golay code G_{23}
* ② The ternary Golay code G_{11}

Reminder: $\mathrm{Ham}(r, q) \subseteq \mathbb{F}_q^n$ is not one code but a class of linearly equivalent codes.
Same for the Golay codes.

G_{23} is an equivalence class of codes in $\mathbb{F}_2^{23}$ ($n=23$)

G_{11} " " " in $\mathbb{F}_3^{11}$ ($n=11$)

Def. given in the course:

G_{23} Cyclic code: $x^{23}-1$

factorise in $\mathbb{F}_2[x]$

$$x^{23}-1 = (x+1)\, g(x)\, \overleftarrow{g}(x)$$

$(x-1)$ is always a factor of x^n-1.

where $g(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$

$\overleftarrow{g}(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$

There is a cyclic code $C \subseteq \mathbb{F}_2^{23}$ with $g(x)$ as the generator polynomial. [also, C' with $\overleftarrow{g}(x)$]

$\dim C = n - \deg g = 23-11=12$

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

g

$\overleftarrow{g} = 11000111010100000000000$

The cyclic codes generated by $g(x)$ and by $\overleftarrow{g}(x)$ are lin. equivalent

(*) Parameters of $G_{23} = C : [23, 12, 7]_2$

$\deg g(x) = 11$

$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$

$\underline{g} = 1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,1\,1\;\;0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0$

$w(\underline{g}) = 7 \Rightarrow \underline{g} \in C$

$\boxed{w(C) \le 7}$

In fact, $d(C) = 7$ (*)

G_{23} attains the Hamming bound:

$d = 7 \qquad t = \left[\frac{d-1}{2}\right] = 3$ (*)

log. H.B.: $k \le n - \log_q \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$

$\binom{23}{0} = 1$

$\binom{23}{1} = 23$

$\binom{23}{2} = \frac{23 \times 22}{1 \times 2} = 253$

$253 \times 7 = 1771$

$RHS = 23 - \log_2 [1 + 23 + 253 + 1771] = 23 - \log_2(2048) = 23 - 11 = 12$

$\binom{23}{3} = \frac{23 \times 22 \times 21}{1 \times 2 \times 3} =$

$$\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3} = 2048$$

$12 \leq 23 - \log_2 2048 = 23-11$ so G_{23} is perfect.

$G_{11} \subseteq \mathbb{F}_3^{11}$ $\quad [11, 6, 5]_3$ $\quad (*)$

$x^{11}-1 = (x-1)\, g(x)\, \overleftarrow{g}(x)$ $\quad \deg g = \deg \overleftarrow{g} = 5$

Need to be able to show: perfect.

CLASSIFICATION OF PERFECT CODES

In 1949:

- trivial codes $\mathbb{F}_q^n$
- $\mathrm{Rep}(2t+1, \mathbb{F}_2)$
- $\mathrm{Ham}(r,q)$ } perfect.
- G_{23} } perfect.
- G_{11} } perfect.

Tietäväinen-van Lint thm (1973)

If q is a prime power, every perfect q-ary code is parameter equivalent to one of the above.

Reed-Muller codes $R(r,m)$

- Binary
- Constructed using "Boolean functions"

$V^m = \{000\ldots00, 00\ldots01, \ldots, \underbrace{11\ldots1}_{m}\}$

$= \{$all binary words of length $m\}$

$\{f: V^m \to \{0,1\} = \mathbb{F}_2\} \longmapsto [00100\ldots0]$ (2^m positions)

$\{$subset of functions on $V^m\} \longmapsto$ code of length 2^m

$V^3 =$	000	001	010	011	100	101	110	111	
1	1	1	1	1	1	1	1	1	Rep $(8,\mathbb{F}_2)$
v_1	0	0	0	0	1	1	1	1	$R(1,3)$ $r=1$ $m=3$
v_2	0	0	1	1	0	0	1	1	
v_3	0	1	0	1	0	1	0	1	
coordinate functions									
~~v_1^2~~	~~$v_1^2=0$~~							~~$v_1^2=1$~~	
v_1v_2	0	0	0	0	0	0	1	1	
v_2v_3									$R(2,3)$
v_1v_3									
$v_1v_2v_3$	0	0	0	0	0	0	0	1	$R(3,3)$

$R(r,m)$ is $\left[2^m, \binom{m}{0}+\binom{m}{1}+\ldots+\binom{m}{r}, 2^{m-r}\right]$