Notes on Golay Codes

1. Sphere Packing Bound

$e = \left\lfloor \frac{d-1}{2} \right\rfloor$ $\quad C$ code in $\mathbb{F}_q^N$

$$|C| \left(\sum_{i=0}^{e} \binom{N}{i} (q-i)^i \right) \leq q^N$$

Perfect codes are those that meet this bound.

Def. $A_i(c) = \left| \{ c' \in C \mid d(c,c') = i \} \right|$

Thm. If C is perfect e-error correcting code, that it is distance invariant ($A_i(c) = A_i(c'), \forall c, c' \in C$) Weight distribution depends only on N and.

Pf (Special case $N=23$, $e=3$)

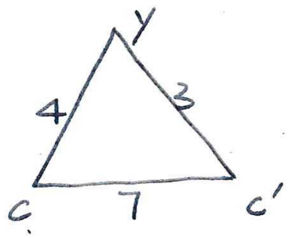
Fix c. Count pairs (c', y).

$d(y,c) = j$, $d(y,c') \leq 3$

$\forall$ for each j.

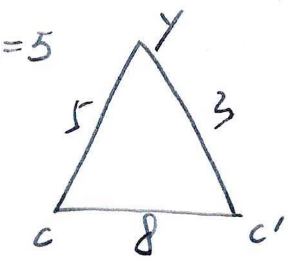
$A_1(c) = \cdots = A_6(c) = 0$ by assumption

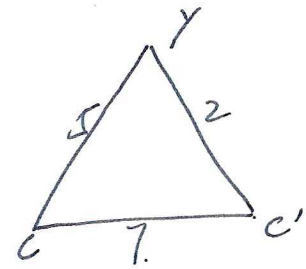
$j=4$



$$\binom{7}{3} A_7(c) = \binom{23}{4} \Rightarrow A_7 = 253$$

$j=5$





$$\binom{7}{2} A_7(c) + \binom{8}{3} A_8(c) = \binom{23}{5}$$

$\Rightarrow A_8 = 506$

continue this process one eventually gets

$A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$

$A_{11} = A_{12} = 1288$

2. Golay Codes

2.1. Hexacodes C_6 (in $\mathbb{F}_4^6$)

$(ab\ cd\ ef) \in C_6$

if $\quad a+b = c+d = e+f = s$

$a+c+e = \omega s$

we can easily compute $C^{\perp}$:

$$C^{\perp} = \begin{bmatrix} 1 & 1 & +1 & +1 & 0 & 0 \\ 0 & 0 & 1 & 1 & +1 & +1 \\ \bar{\omega} & \omega & 1 & 0 & 1 & 0 \end{bmatrix}$$

symmetry group of C_6:

(i) $\cdot\,\omega$

(ii) interchange two entries in any two couples

(iii) permutation of 3 couples

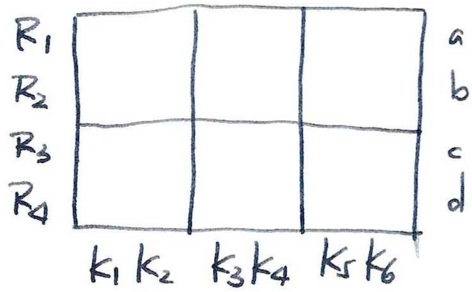
orbits:

	# image
$(01 \quad 01 \quad \omega\bar{\omega})$	$\to 36$
$(\omega\bar{\omega} \quad \omega\bar{\omega} \quad \omega\bar{\omega})$	$\to 12$
$(00 \quad 11 \quad 11)$	$\to 9$
$(11 \quad \omega\omega \quad \bar{\omega}\bar{\omega})$	$\to 6$
$(00 \quad 00 \quad 00)$	$\to 1$

Observation: $d(C_6) = 4$

Any 3 entries uniquely determine a codeword.

3. The miracle Octad generator



scoring map φ

$\varphi: (a\ b\ c\ d) \to a\cdot 0 + b\cdot 1 + c\cdot\omega + d\cdot\bar{\omega}$

φ gives a map: $\mathbb{F}_2^{24} \to \mathbb{F}_4^{6}$

def^{n} $v \in \mathbb{F}_2^{24}$ balanced if

$\langle v, R_1\rangle = \langle v, K_i\rangle \quad 1 \le i \le 6$

Golay Code C_{24}: all balanced vector v with $\varphi(v) \in C_6$.

Thm. Golay code C_{24} is a self-dual $[24, 12, 8]$ binary code. #

$4 \mid wt(v) \quad v \in C_{24}$.

$(v, R_1) = \text{even}$

Pf Let $E =$ even subcode of C_{24}

If $e \in E$, $wt(\varphi(e)) = 0/4/6$

~~wt(e)~~ a nonzero entry in $\varphi(e)$ is a binary 4-tuple with wt 2 a zero entry has wt 0 or 4

In either case, $4 \mid wt(e)$

If $x, y \in E$, then

$wt(x+y) = wt(x) + wt(y) - 2wt(x \cap y)$

Since $4 \mid wt(x+y), wt(x), wt(y)$

$\Rightarrow 2 \mid wt(x \cap y)$

$\Rightarrow \langle x, y \rangle = 0$

$\Rightarrow E$ is self-dual.

$C_{24} = \langle E, k_1 + R_1 \rangle$

$e \in C_{24} \Rightarrow \langle e, k_1 \rangle = \langle e, R_1 \rangle$

$\Rightarrow \langle e, k_1 + R_1 \rangle = 0$

Since $\langle k_1 + R_1, k_1 + R_1 \rangle = 0$; together we have.

$\langle E, k_1 + R_1 \rangle$ is self-dual.

$wt(k_1 + R_1 + e) = wt(k_1 + R_1) + wt(e) - 2wt((k_1 + R_1) \cap e)$.

$\Rightarrow 4 \mid wt(k_1 + R_1 + e)$.

$\Rightarrow 4 \mid v, \ \forall v \in C_{24}$.

Now we show $d = 8$.

If $\exists c \in C_{24}$, $wt(c) = 4$

Odd parity $\Rightarrow wt(c) \geq 6$.

$wt(\varphi(c)) \leq 2 \Rightarrow$ impossible.

Puncturing out one coord gives a $[23, 12, 7]$ code, perfect.

$\Rightarrow A_0 = A_{24} = 1 \quad A_8 = A_{16} = 759$

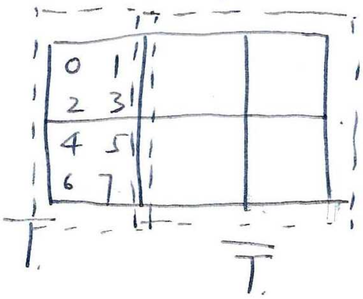
$A_{12} = 2576$.

Rmk: Weight 16 vectors are just complements of weight 8 vectors.

Thm. Every set of 5 points uniquely determines an octad.

Pf. $759 \binom{8}{5} = \binom{24}{5}$.

4. Notes on Nordstrom Robinson Code. (c.f. V.P.)



Let $C^{\overline{T}}$ be punctured code on $\overline{T}$.

$C_{\overline{T}}$ be shortened code on $\overline{T}$.

Let c_i be the codeword s.t.

$\mathrm{supp}(c_i) \cap T = \{0, i\}$, $1 \le i \le 7$.

Note that $C^{\overline{T}}$ is a $[8, 7, 2]$ code in T.

$$\sum_{i=0}^{4} \binom{8}{2i} = 2^7$$

$\Rightarrow$ $C^{\overline{T}}$ is the set of all vectors of even weight.

$\Rightarrow$ singleton bound gives

$d(C^{\overline{T}}) \le 2$, we know that

$d(C^{\overline{T}}) \neq 1 \Rightarrow d(C^{\overline{T}}) = 0$

$\Rightarrow$ Those c_i's exist.

Let $c_0 = \bar{0}$.

Nordstrom Robinson code is.

$\bigcup_{i=0}^{7} c_i + \cancel{C(T)}\, C_{\overline{T}}$ punctured on $\overline{T}$.

Since $\dim C^{\overline{T}} = 7$,

$\dim C_{\overline{T}} = 5$

$\Rightarrow |C_{\overline{T}}| = 32$.

$\Rightarrow$ NR is a $[16, 256]$ code.

$d(NR) \geq 6$. since, $c_1 \neq c_2 \in C_{24}$

disagree on at most 2 points.

Turyn Construction

Let H = extended $[8, 4, 4]$ Hamming Code, Let H' be a column permutation s.t.

$$\begin{array}{ccc} & \mathbb{F}_2^8 & \\ & | & \\ & \langle 1 \rangle^{\perp} = H + H' & \\ / & & \backslash \\ H & & H' \\ \backslash & & / \\ & H \cap H' = \langle 1 \rangle & \\ & | & \\ & \{0\} & \end{array}$$

G_{24} Let a code C

$=(c_1+c', c_1+c_2+c', c_2+c')$ $c_1, c_2 \in H$ $c' \in H'$

Check: self-dual.

Every codeword has wt disible by 4: $S=\{(c_1,c_1,0), (0,c_2,c_2), (c',c',c')\}$ is a spanning set.

Induction: $\left[v_k \cap \left(\sum_{i=1}^{k-1} v_i\right)\right]$

$$wt\left(v_k+\sum_{i=1}^{k-1} v_i\right) = wt(v_k) + wt\left(\sum_{i=1}^{k-1} v_i\right) - 2wt$$

$4 \mid$ every term on RHS.

Now prove $\dim C = 12$.

$(c_1,c_1,0)+(0,c_2,c_2)+(c',c',c')=(0,0,0)$

$\Rightarrow c_1 = c' = c_2 = 0$ since $H \cap H' = \langle 1 \rangle$

Each of c_1, c_2, c' gives 4 binary degree of freedom

$\Rightarrow \dim C = 12$.

Suppose

$\exists\, x=(c_1+c', c_1+c_2+c', c_2+c') \in C$, $wt(x) \le 4$.

Since $H+H' = \langle 1 \rangle^{\perp}$, a non-zero vector has even weight.

$\Rightarrow$ one of c_1+c', c_1+c_2+c', c_2+c' is zero.

$\Rightarrow c' = \bar{0}$ or $\bar{1}$.

$\Rightarrow$ ~~$x=(0, c_2, c_2+c')$~~ / ~~$x=(c_1$~~

In any case, $x=0$.

Rmk. By uniqueness of Golay Code ~~&~~ C must be the Golay Code.

Explicit Construction of H, H'

$$H' = \{c' ; \text{ s.t } (c',c',c') \in G_{24}\}.$$

$\varphi(c',c',c')$ must be in the orbit of $\omega\bar{\omega}$ $\omega\bar{\omega}$ $\omega\bar{\omega}$.

i.e. ~~$\emptyset$~~

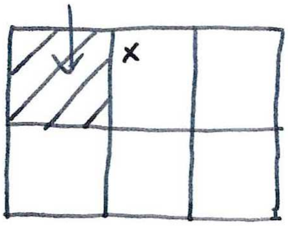
$$H' = \varphi^{-1}(\langle \omega\bar{\omega} \rangle).$$

Similarly

$$H = \varphi^{-1}(\langle 1 1 \rangle).$$

Rmk: The subcode of Golay Code, whose projection onto T. lies in $[8,4,4]$ extended Hamming code, is essentially just two copies of H.

Puncture out 4-coords.



(20, 12, 4).

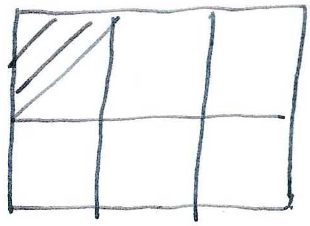
1. pick any point in the remaining 20 coords
2. with 4 points deleted uniquely determines an octad
3. all codewords with 4 are obtained by puncturing out the 4 points from an octad.
4. $A_4(C') = \frac{\binom{20}{1}}{\binom{4}{1}} = 5$

1 point $\longrightarrow$ octad.

4 points. determine the same octad/the same codeword of wt 4 in C'

$A_4(C') = 5$ covers 20 points.

$\Rightarrow$ has to be 1-avail-4-LRC.



(21, 12, 5).

Any pair lies in exactly one.

c, $wt(c) = 5$ $\Rightarrow$ two codewords with weight 5 intersect at at most 1 point.

$A_5(C') = \frac{\binom{21}{2}}{\binom{5}{2}} = \frac{21\times 20}{5\times 4} = 21$

· is ~~Ae~~ actually a 2-(21, 5, 1) Design.

$\lambda_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} = 1 \cdot \frac{\binom{20}{4}}{\binom{4}{1}} = 5$

$\Rightarrow$ Induces a 1-(21, 5, 5) Design

$\Rightarrow$ 5-avail-4-LRC.