Ternary Golay Code

Hongyu Zhu

· Preliminaries

Recall · Hamming distance $\partial(\vec{u},\vec{v})$

· $\Sigma_e(\vec{x}) = \{\vec{y} \mid \partial(\vec{x},\vec{y}) \le e\}$

Def $[n,k,d]_q$ code: A subspace $C \subseteq \mathbb{F}_q^n$, with $\dim C = k$, minimum distance d.

i.e. $\min\{\partial(u,v) \mid u \neq v,\ u,v \in C\} = d$.

Def A perfect e-code is a code C s.t. $\{\Sigma_e(\vec{x}) \mid \vec{x} \in C\}$ partitions $\mathbb{F}_q^n$ (without repeat).

Recall Standard inner product $\vec{x}\cdot\vec{y}$

Def A code C is self-dual if $C = C^{\perp}$.

Def The weight of $\vec{v}$ is the number of its nonzero entries, denoted $w(\vec{v})$.

Rk ① By linearity, $\partial(\vec{u},\vec{v}) = \partial(\vec{u}-\vec{v},\vec{0})$, so

$$d = \min\{w(\vec{u}) \mid \vec{u} \in C \setminus \{0\}\}.$$

② When $q = 2, 3$, we have

$$w(\vec{v}) = \vec{v}\cdot\vec{v}.$$

In particular, if $\vec{v}$ belongs to some self-dual code, then $w(\vec{v}) \equiv 0 \pmod q$.

Def The weight enumerator of a code C is

$$\sum_{\vec{v}\in C} x^{n-w(\vec{v})} y^{w(\vec{v})}$$

· Ternary Golay Code

Def (Ternary Golay Code) The subspace $C \subseteq \mathbb{F}_3^{11}$ spanned by the row vectors of the following matrix:

$$\left[\begin{array}{cccccc|ccccc}
1 &&&&&& 1 & 1 & 1 & 1 & 1 \\
& 1 &&&&& 0 & 1 & -1 & -1 & 1 \\
&& 1 &&&& 1 & 0 & 1 & -1 & -1 \\
&&& 1 &&& -1 & 1 & 0 & 1 & -1 \\
&&&& 1 && -1 & -1 & 1 & 0 & 1 \\
&&&&& 1 & 1 & -1 & -1 & 1 & 0
\end{array}\right]$$

Identity

cyclic permutations of $(0,1,-1,-1,1)$

We will show that it is an $[11,6,5]_3$ code.

Thm C has minimum distance $d_C = 5$.

Pf To be done in the last 2 sections.

As a result,

Thm C is a perfect 2-code.

Pf · $\{\Sigma_2(\vec{x}) \mid \vec{x} \in C\}$ are pairwise disjoint ($d_C = 5$).

· For any $\vec{x} \in \mathbb{F}_3^{11}$,

$$\Sigma_2(\vec{x}) = 1 + 2\cdot\binom{11}{1} + 2^2\cdot\binom{11}{2} = 243 = 3^5$$

Whereas $|C| = 3^6$, so by disjointness

$$|\cup\{\Sigma_2(\vec{x}) \mid \vec{x}\in C\}| = 3^5\cdot 3^6 = |\mathbb{F}_3^{11}|$$

So it indeed partitions the whole space. ∎

Rk We also know that:

· Its weight enumerator is

$$x^{11} + 132x^6y^5 + 132x^5y^6 + 330x^3y^8 + 110x^2y^9 + 24y^{11}.$$

· Its group of (permutation) automorphism is the Mathieu group M_{11}.

· Extended Ternary Golay Code.

Def (extended ternary golay code) $\tilde{C}$ is obtained by: extend C to $\mathbb{F}_3^{12}$ by adding a column making each row sum to 0:

$$\begin{bmatrix}
1 &&&&&& 1 & 1 & 1 & 1 & 1 & 0 \\
& 1 &&&&& 0 & 1 & -1 & -1 & 1 & -1 \\
&& 1 &&&& 1 & 0 & 1 & -1 & -1 & -1 \\
&&& 1 &&& -1 & 1 & 0 & 1 & -1 & -1 \\
&&&& 1 && -1 & -1 & 1 & 0 & 1 & -1 \\
&&&&& 1 & 1 & -1 & -1 & 1 & 0 & -1
\end{bmatrix}$$

This will be a $[12,6,6]_3$ code.

Thm $\tilde{C}$ has minimum distance $d_{\tilde{C}} = 6$.

Pf To be done in the last 2 sections

Thm $\tilde{C}$ is self dual.

Pf Any of the 6 basis vector is orthogonal to all 6 of them. ∎

Rk · Weight enumerator:

$$x^{12} + 264x^6y^6 + 440x^9y^3 + 24y^{12}$$

· Permutation automorphism group: the Mathieu group M_{12}.

· Minimum Distances

Thm $d_C = 5$ and $d_{\tilde{C}} = 6$.

Pf · It is easy to see $d_C \le 5$, $d_{\tilde{C}} \le 6$.

· By definition,

$$d_{\tilde{C}} \geq d_C \geq d_{\tilde{C}} - 1.$$

· Since $\tilde{C}$ is self-dual,

$$d_{\tilde{C}} = \min_{\vec{v}\in\tilde{C}\setminus\{0\}} \vec{v}\cdot\vec{v} \equiv 0 \pmod 3$$

So it suffices to show that

$$\boxed{d_C \geq 4}$$

(Then $d_{\tilde{C}} \geq 6$, so $d_C \geq 5$, which implies the result.)

To prove $d_C \geq 4$, we need to use the "BCH bound".

· Polynomial Code

From now on, we view $(a_i)_{i<11}$ as the polynomial $\sum_{i<11} a_i z^i$.

Prop A codeword is in C $\iff$ it is divisible by

$$g(z) = z^5 + z^4 - z^3 + z^2 - 1.$$

Pf Clearly the RHS is a subspace with basis $\{g(z)\cdot z^i\}_{i<6}$

So it suffices to check this is another basis for C. ∎

Rk $g(z)$ has interesting number theoretic properties:

· It is irreducible (over $\mathbb{F}_3$).

· It is a factor of $x^{11} - 1$.

· Let α be a root of g (thus a primitive 11-th root of unity), then

$$g(z) = (z-\alpha)\underline{(z-\alpha^3)(z-\alpha^4)(z-\alpha^5)}(z-\alpha^9).$$

Clearly, $d_C \le 4$ is equivalent to the following:

Thm If $p \in C$ has at most 3 nonzero terms, then $p = 0$.

Pf · Write $p(z) = b_1x^{k_1} + b_2x^{k_2} + b_3x^{k_3}$. $(0 \le k_1 < k_2 < k_3 < 11)$.

· Since $p \in C$, $g \mid p$, in particular

$$\underline{p(\alpha^3) = p(\alpha^4) = p(\alpha^5) = 0}$$

$$\Rightarrow \underbrace{\begin{bmatrix} \alpha^{3k_1} & \alpha^{3k_2} & \alpha^{3k_3} \\ \alpha^{4k_1} & \alpha^{4k_2} & \alpha^{4k_3} \\ \alpha^{5k_1} & \alpha^{5k_2} & \alpha^{5k_3} \end{bmatrix}}_{A} \cdot \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}}_{\vec{b}} = \underbrace{\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}}_{\vec{0}}$$

· Now $\det(A) = \alpha^{3k_1+3k_2+3k_3}\cdot\det(B)$

where $B = \begin{bmatrix} 1 & 1 & 1 \\ \alpha^{k_1} & \alpha^{k_2} & \alpha^{k_3} \\ \alpha^{2k_1} & \alpha^{2k_2} & \alpha^{2k_3} \end{bmatrix}$

So $\det(B) = (\alpha^{k_1} - \alpha^{k_2})(\alpha^{k_1} - \alpha^{k_3})(\alpha^{k_2} - \alpha^{k_3})$

As $0 \le k_1 < k_2 < k_3 < 11$, $\alpha^{k_1}, \alpha^{k_2}, \alpha^{k_3}$ are distinct

$\Rightarrow \det(A) \neq 0 \quad \Rightarrow \vec{b} = \vec{0} \Rightarrow p = 0.$ ∎

Rk More general statements hold for "BCH codes".

Ternary Golay code $\in$ (generalized) BCH codes $\subsetneq$ cyclic codes $\subsetneq$ polynomial codes.