

Additive Cyclic Codes

Funda Özdemir

Faculty of Engineering and Natural Sciences
Sabancı University, Istanbul

SP Coding School, January 19-30, 2015

- J. Bierbrauer generalized the theory of cyclic codes from the category of linear codes to the category of additive codes in 2002.
- We will state Bierbrauer's BCH bound on the minimum distance of additive cyclic codes.
- Our goal is to improve the bound on the minimum distance of these codes.

Setting

- Consider \mathbb{F}_q with $q = p^e$. Let $n \mid q^r - 1$ and $W = \langle \alpha \rangle$ be a multiplicative subgroup of $\mathbb{F}_{q^r}^*$.
- Fix $A = \{i_1, \dots, i_s\} \subseteq \mathbb{Z}/n\mathbb{Z}$.
- Define the \mathbb{F}_q -linear space of polynomials

$$\mathcal{P}(A) := \{a_1x^{i_1} + \dots + a_sx^{i_s} : a_1, \dots, a_s \in \mathbb{F}_{q^r}\}$$

- Set

$$\mathcal{B}(A) := \{(f(\alpha^0), \dots, f(\alpha^{n-1})) : f(x) \in \mathcal{P}(A)\}$$

- Define a surjective \mathbb{F}_q -linear mapping

$$\begin{aligned} \phi : \mathbb{F}_{q^r} &\rightarrow \mathbb{F}_q^m \\ x &\mapsto (Tr(\gamma_1x), \dots, Tr(\gamma_mx)) \end{aligned}$$

for some subset $\{\gamma_1, \dots, \gamma_m\} \subset \mathbb{F}_{q^r}$, where Tr denotes the **trace function** from \mathbb{F}_{q^r} to \mathbb{F}_q .

- The set $\{\gamma_1, \dots, \gamma_m\}$ is linearly independent over \mathbb{F}_q since ϕ is onto.
- Extend ϕ to a mapping : $\mathbb{F}_{q^r}^n \rightarrow (\mathbb{F}_q^m)^n$ in the usual way.

Additive Cyclic Codes

Definition

Define the **additive cyclic code** over the alphabet \mathbb{F}_q^m with length n as

$$\begin{aligned}\mathcal{C}(A) &:= (\phi(\mathcal{B}(A)))^\perp \\ &= \{(\phi(f(\alpha^0)), \dots, \phi(f(\alpha^{n-1}))) : f(x) \in \mathcal{P}(A)\}^\perp \subseteq (\mathbb{F}_q^m)^n \\ &= \{(Tr(\gamma_1 f(\alpha^0)), \dots, Tr(\gamma_m f(\alpha^0)); \dots; Tr(\gamma_1 f(\alpha^{n-1})), \dots, Tr(\gamma_m f(\alpha^{n-1}))) : f(x) \in \mathcal{P}(A)\}^\perp \\ &\subseteq \mathbb{F}_q^{mn}\end{aligned}$$

- The code $\mathcal{C}(A)$ is not linear over its alphabet \mathbb{F}_q^m . If we view \mathcal{C} in \mathbb{F}_q^{mn} as above, then it is \mathbb{F}_q -linear.
- $\mathcal{C}(A)$ is **cyclic**: Since the dual code of a cyclic code is also cyclic, it is enough to show that $\mathcal{C}(A)^\perp$ is cyclic. Consider the codeword

$$c_f = (\phi(f(\alpha^0)), \dots, \phi(f(\alpha^{n-1})))$$

determined by $f(x) = \sum_{j=1}^s \lambda_j x^j \in \mathcal{P}(A)$.

For $g(x) = \sum_{j=1}^s \lambda_j \alpha^{-ij} x^j \in \mathcal{P}(A)$, we have:

$$(\phi(f(\alpha^{n-1})), \phi(f(\alpha^0)), \dots, \phi(f(\alpha^{n-2}))) = (\phi(g(\alpha^0)), \phi(g(\alpha)), \dots, \phi(g(\alpha^{n-1})))$$

- Linear cyclic codes correspond to the special case when $m = 1$ and $\phi(x) = Tr(x)$.

Definition

$A \subseteq \mathbb{Z}/n\mathbb{Z}$ is an **interval** if there is a generator (an integer j , coprime with n) of $\mathbb{Z}/n\mathbb{Z}$ such that $A = \{jl, j(l+1), \dots, j(l+i-1)\}$, for some $l \pmod{n}$. In the special case $A = \{i, i+1, \dots, j\}$, the short notation $A = [i, j]$ is used.

Theorem (Bierbrauer's BCH bound)

If A contains an interval of size $t \pmod{n}$, then the minimum distance of $C(A)$ is $\geq t + 1$.

Goal: Improve the minimum distance bound for additive cyclic codes!