On a class of binary codes from superimposed codes

Tefjol Pllaha (Joint with T. Hussain)

Department of Mathematics & Statistics
University of South Florida

email: tpllaha@usf.edu
website: pllahat.github.io

Notations

Let $\mathbb{F}_q$ be a finite field with q elements.
If $f(x) = \sum_{i=0}^{m-1} f_i x^i + x^m \in \mathbb{F}_p[x]$ is an irreducible monic polynomial and $\alpha \in \mathbb{F}_q$ is a root of $f(x)$ then $\mathbb{F}_q \cong \mathbb{F}_p[\alpha]$, and we have an isomorphism

$$\psi : x = \sum_{i=0}^{m-1} x_i \alpha^i \in \mathbb{F}_q \longmapsto \mathbf{x} = (x_0, x_1, \ldots, x_{m-1}) \in \mathbb{F}_p^m.$$

Order $\mathbb{F}_q[\alpha]$ lexicographically and define the bijection

$$\phi : \beta_i \in \mathbb{F}_q \to \mathbf{e}_i \in \mathbb{F}_2^q$$

that sends the ith element of $\mathbb{F}_q$ to the ith standard basis vector $\mathbf{e}_i$ of $\mathbb{F}_2^q$.

Defining the codes in questions

Let $\mathcal{C}$ be an $[n, k]_q$ code. Let $M_{\mathcal{C}}$ be the $n \times q^k$ matrix where its columns are the codewords of $\mathcal{C}$ ordered lexicographically.
Let $H_{\mathcal{C}}$ be the $nq \times q^k$ matrix where each entry β of $M_{\mathcal{C}}$ is replaced with the (column) vector $\phi(\beta)^\top$.
We will discuss the codes $\mathcal{C}_\phi = \mathrm{null}(H_{\mathcal{C}})$ and their duals $\mathcal{C}_\phi^\perp = \mathrm{rs}(H_{\mathcal{C}})$ introduced by Haymaker and McMillon[1].

[1] K. Haymaker and E. McMillon. A class of quasi-cyclic binary parity-check codes from Reed-Solomon codes. In 2025 13th International Symposium on Topics in Coding (ISTC), pages 1–5, 2025.

What do we do?

Question: What is their dimension and their distance?

Trivial bound: $\dim(\mathcal{C}_\phi) \geq q^k - (nq - (n-1))$

Distance bounds from folklore:

(a) Let $\mathcal{C}$ be an $[n, k, d]_q$ code. Then,
$d(\mathcal{C}_\phi) \geq \lfloor (n-1)/(d-1) \rfloor + 2$.

(b) Let $\mathcal{C}$ be an $[n, 2]$ code. Then $H_\mathcal{C}$ satisfies the **row-column constraint** and thus $d(\mathcal{C}_\phi) \geq n + 1$.

Improved dimension bound

Theorem [Hussain, P., 26] Let $q = 2^m$ and let $\mathcal{C}$ be an $[n, k]_q$ code. Then

$$\dim(\mathcal{C}_\phi) \geq q^k - [nq - (n-1) - (n-k)m] \, .$$

Proof: It would suffice to show that

$$\mathrm{rank}(H_{\mathcal{C}}) \leq nq - [(n-1) + (n-k)m] \, . \tag{1}$$

We will show this by explicitly constructing $(n-1) + (n-k)m$ linearly independent vectors in the space

$$\mathrm{null}(H_{\mathcal{C}}^\top) = \{\mathbf{x} \in \mathbb{F}_2^{nq} \mid \mathbf{x} H_{\mathcal{C}} = \mathbf{0}\}$$

.

Proof continued

For the monic polynomial $f(x) = \sum_{i=0}^{m-1} f_i x^i + x^m$, consider the companion matrix A , which is the matrix representation of multiplication by α in $\mathbb{F}_q$, namely, $\psi(\alpha x) = \psi(x)A$ for all $x \in \mathbb{F}_q$. We will make use of the following field isomorphism:

$$\chi : x = \sum_{i=0}^{m-1} x_i \alpha^i \in \mathbb{F}_q \cong \mathbb{F}_p[\alpha] \longmapsto \sum_{i=0}^{m-1} x_i A^i \in \mathbb{F}_p[A] \subset \mathbb{F}_p^{m \times m}. \tag{2}$$

Additionally, let $F = [\psi(\beta)^\top \mid \beta \in \mathbb{F}_q] \in \mathbb{F}_p^{m \times q}$ and $\widehat{F} = \mathrm{diag}(F, F, \ldots, F)$.

Main insights: (a) $\mathrm{rank}(\bar{\chi}(H_{\mathcal{C}})\widehat{F}) = m(n-k)$,
(b) $\left(\bar{\chi}(H_{\mathcal{C}})\widehat{F}\right) H_{\mathcal{C}} = \mathbf{0}$.

The special case of $\mathcal{C} = \mathbb{F}_q^n$

Theorem [Hussain, P., 26] Let $\mathcal{C} = \mathbb{F}_q^n$. Then $\mathcal{C}_\phi$ is an $[q^n, q^n - nq + (n-1), 4]_2$ code.

Remark (a) This generalizes a result of Haymaker-McMillon for $\mathcal{C} = \mathbb{F}_q^2$.
(b) This case attains the previous lower bound.
(c) **It appears that**, if $\dim(\mathcal{C}) > k/2$, then the previous lower bound is also attained.

On the dual code $\mathcal{C}_\phi^\perp$

Let $\mathcal{C} = \mathrm{null}(H)$. Then $\mathcal{C}_\phi^\perp = \mathrm{rs}(H_\mathcal{C})$

A typical dual codeword looks like $\mathbf{d_x} = \mathbf{x}H_\mathcal{C} \in \mathcal{C}_\phi^\perp, \quad \mathbf{x} \in \mathbb{F}_2^{nq}$.

Define functions $h_i : \mathbb{F}_q \to \mathbb{F}_2, \beta \mapsto x_{i,\beta}$. With this notation, for $\mathbf{c} \in \mathcal{C}$ we have

$$\mathbf{d_x}(\mathbf{c}) = \sum_{i=1}^{n} h_i(c_i),$$

and furthermore, we can compute the weight of $\mathbf{d_x}$ as

$$\begin{aligned}\mathrm{wt}(\mathbf{d_x}) &= \sum_{\mathbf{c}\in\mathcal{C}} \frac{1-(-1)^{\mathbf{d_x}(\mathbf{c})}}{2} \\ &= \frac{q^k}{2}\left(1 - \frac{1}{q^k}\sum_{\mathbf{c}\in\mathcal{C}}(-1)^{\mathbf{d_x}(\mathbf{c})}\right).\end{aligned}$$

On the weight of dual codewords

Denote $A_i = \{\beta \in \mathbb{F}_q \mid h_i(\beta) = 1\}$ and $a_i = |A_i|$.

Theorem [Hussain, P., 26] Let $\mathcal{C} = \mathrm{rs}(G)$ be an $[n, k]_q$ code and consider $\mathcal{C}_\phi$. For $\mathbf{d_x} = \mathbf{x}H_{\mathcal{C}} \in \mathrm{rs}(H_{\mathcal{C}}) = \mathcal{C}_\phi^\perp$, we have

$$\mathrm{wt}(\mathbf{d_x}) = \frac{q^k}{2}\left[1 - \sum_{T\subseteq[n]} (-2)^{|T|} \cdot N_T\right],$$

where $r_T = \mathrm{rank}(G_T)$ and $N_T = |\pi_T(\mathcal{C}) \cap (\prod_{i\in T} A_i)| \cdot q^{-r_T}$.

Two special cases

Corollary Let $S = \{i \in [n] \mid a_i > 0\}$. If $\operatorname{rank}(G_S) = |S|$ then

$$\operatorname{wt}(\mathbf{d}_{\mathbf{x}}) = \frac{q^k}{2}\left[1 - \prod_{i \in S}\left(1 - \frac{2a_i}{q}\right)\right].$$

Theorem [Hussain, P., 26] Let $\mathcal{C}$ be an $[n,k]_q$ Reed-Solomon code and let $\mathbf{d}_{\mathbf{x}} \in \operatorname{rs}(H_{\mathcal{C}}) = \mathcal{C}_{\phi}^{\perp}$. Then

$$\operatorname{wt}(\mathbf{d}_{\mathbf{x}}) = \frac{q^k}{2}\left[1 - \sum_{\boldsymbol{\beta} \in \mathcal{C}^{\perp}} \prod_{i=1}^{n} \hat{h}_i(\beta_i)\right].$$

More on duality (CSS & CSS-T codes)

Theorem [Hussain, P., 26] Let $\mathcal{C}$ be an $[n, k > 2]_{2^m}$ non degenerate code. Then $\mathcal{C}_\phi^\perp \subset \mathcal{C}_\phi$.

Theorem [Hussain, P., 26] Let $\mathcal{C} = \mathrm{rs}(G)$ be an $[n, k > 3]_{2^m}$ code, and assume that any three columns of G are linearly independent. Then $H_\mathcal{C}$ is triorthogonal ($\mathrm{wt}(\mathbf{x} \star \mathbf{y} \star \mathbf{z})$ is even for any three rows).

Future research

(1) Prove that the for $k > n/2$ the improved lower bound is attained.
(2) Compute the weight enumerator of $\mathcal{C}_{\phi}^{\perp}$ if $\mathcal{C}$ is a Reed-Solomon code, with the ultimate goal of understanding the distance of $\mathcal{C}_{\phi}$.
(3) The resulting CSS and CSS-T codes have high rate but (really) low distance. Can anything be modified and obtain higher distance?

Thank You!

email: tpllaha@usf.edu
website: pllahat.github.io