THE DUAL AND THE HULL CODE IN THE FRAMEWORK OF THE TWO GENERIC CONSTRUCTIONS

Virginio Fratianni
University of Paris VIII
University Sorbonne Paris Nord, LAGA, UMR 7539

Journées C2 2023
Najac, France

17th October 2023

INDEX

NOTATIONS

- Let $\mathbb{F}_q$ be the finite field of order q, where $q = p^m$.
- Let $x, y \in \mathbb{F}_q^n$, then the Hamming distance and weight are defined as follows:
$$d(x, y) := |\{i : x_i \neq y_i\}|, \quad w(x) := |\{i : x_i \neq 0\}.$$
- An $[n, k, d]_q$ linear code $\mathcal{C}$ is a linear subspace of the vector space $\mathbb{F}_q^n$ with dimension k and distance d, where
$$d = \min_{x,y \in \mathcal{C}, x \neq y} d(x, y) = \min_{x \in \mathcal{C}, x \neq 0} w(x).$$
- We denote by G a generator matrix and by H a check matrix of the linear code $\mathcal{C}$.

THE HULL OF A LINEAR CODE

DEFINITION

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$, then its *Euclidean Hull* is defined as

$$\mathrm{Hull}_E(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^{\perp}.$$

THE HULL OF A LINEAR CODE

DEFINITION

Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$, then its *Euclidean Hull* is defined as

$$\text{Hull}_E(\mathcal{C}) := \mathcal{C} \cap \mathcal{C}^{\perp}.$$

It can be algebraically characterized in the following way

$$\text{Hull}(\mathcal{C}) = \left\{ I \in \mathbb{F}_q^n : \begin{bmatrix} G \\ H \end{bmatrix} I^T = \mathbf{0} \right\},$$

where G is a generator matrix and H is a parity-check matrix.
It was initially introduced in 1990 by Assmus and Key to classify finite projective planes.

LINEAR COMPLEMENTARY DUAL CODES

DEFINITION

A linear code $\mathcal{C}$ is said to be linear complementary dual (LCD) if

$$\mathrm{Hull}_E(\mathcal{C}) = 0.$$

THEOREM (JAMES L. MASSEY, 1992)

Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_q$ and let G be its generating matrix. Then $\mathcal{C}$ is a LCD code if and only if the matrix GG^T is nonsingular.

LINEAR COMPLEMENTARY DUAL CODES

DEFINITION

A linear code $\mathcal{C}$ is said to be linear complementary dual (LCD) if

$$\text{Hull}_E(\mathcal{C}) = 0.$$

THEOREM (JAMES L. MASSEY, 1992)

Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_q$ and let G be its generating matrix. Then $\mathcal{C}$ is a LCD code if and only if the matrix GG^T is nonsingular.

The importance of LCD has been highlighted by Carlet and Guilley, then they have been widely studied from 2015 in the european project SECODE, headed by Mesnager at the LAGA lab, and later all over the world.

LOW DIMENSIONAL HULL CODES

Great importance of low dimensional Hull codes, for example:

1. determining the complexity of algorithms for checking permutation equivalence of two linear codes;
2. computing the automorphism group of a linear code;
3. building good quantum codes via entanglement

are very effective in general when the hull dimension is small.

There is a considerable **gap** between the interest in linear codes with a low dimensional hull and our knowledge of them.

THE FIRST GENERIC CONSTRUCTIONS

DEFINITION

The first generic construction is obtained by considering a code $\mathcal{C}(f)$ over $\mathbb{F}_p$ involving a polynomial f from $\mathbb{F}_q$ to $\mathbb{F}_q$ (where $q = p^m$). Such a code is defined by

$$\mathcal{C}(f) = \{\mathbf{c} = (Tr_{q/p}(af(x) + bx))_{x \in \mathbb{F}_q} \mid a \in \mathbb{F}_q, b \in \mathbb{F}_q\}.$$

The resulting code $\mathcal{C}(f)$ from f is a linear code over $\mathbb{F}_p$ of length q and its dimension is upper bounded by $2m$ which is reached when the nonlinearity of the vectorial function f is larger than 0, which happens in many cases.

LINK WITH THE WALSH TRANSFORM

Consider a function $f : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^m$, which we will use the define the code in the first generic construction, with p odd, and define the following function

$$\begin{aligned} g : \mathbb{F}_q &\longrightarrow \mathbb{F}_p \\ x &\longmapsto \mathrm{Tr}_{q/p}(f(x) - x). \end{aligned}$$

If we suppose that g is weakly regular bent, then there exists another function $g^* : \mathbb{F}_q \to \mathbb{F}_p$ such that, for $b \in \mathbb{F}_q$:

$$\hat{\chi}_g(b) = \epsilon \sqrt{p^*}^m \zeta^{g^*(b)}$$

and

$$\hat{\chi}_{g^*}(b) = \frac{\epsilon p^m}{\sqrt{p^*}^m} \zeta^{g(b)},$$

where $\epsilon = \pm 1$ is the sign of the Walsh transform of $f(x)$, $p^* = (\frac{-1}{p})p$ and $\zeta = e^{\frac{2\pi i}{p}}$ is the primitive p-th root of unity.

LINK WITH THE WALSH TRANSFORM

By fixing an enumeration $(x_i)_{i=1,\dots,q}$ of the elements in $\mathbb{F}_q$, we have the following necessary condition.

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that the previously defined function g is weakly regular bent and consider $(c_1, \dots, c_q) \in \mathcal{C}(f)^\perp$. Then

1. *if f respects the scalar multiplication, i.e. for every $\alpha \in \mathbb{F}_p$ and $x \in \mathbb{F}_q$, $f(\alpha x) = \alpha f(x)$:*

$$\prod_{i=1}^{q} \hat{\chi}_{g^*}(c_i x_i) = \left(\frac{\epsilon p^m}{\sqrt{p^*}^m}\right)^q,$$

2. *for a generic f:*

$$\prod_{i=1}^{q} \left(\hat{\chi}_{g^*}(x_i)\right)^{c_i} = \prod_{i=1}^{q} \left(\frac{\epsilon p^m}{\sqrt{p^*}^m}\right)^{c_i}.$$

WEIGHT ENUMERATOR IN THE EVEN CHARACTERISTIC

Let $\mathbb{F}_q$ be a finite field of even characteristic.

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that the previously defined function g is (weakly regular) bent and consider $\boldsymbol{c} = (c_1, \ldots, c_q) \in \mathcal{C}(f)^{\perp}$. Then, if

$$\alpha := \prod_{i=1}^{q} \left(\hat{\chi}_{g^*}(x_i)\right)^{c_i}$$

we have

$$wt(\boldsymbol{c}) = \frac{\log_2(\alpha^2)}{m}.$$

THE GENERAL CASE

Consider a function $f : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^m$, which we will use to define the code in the first generic construction, and for every $i = 1, \ldots, q$ define the functions $g_i : \mathbb{F}_q \to \mathbb{F}_p$ such that $g_i(x_i) = \mathrm{Tr}_{q/p}(f(x_i))$ and $g_i(x) = \mathrm{Tr}_{q/p}(x)$ for $x \neq x_i$.

THE GENERAL CASE

Consider a function $f : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^m$, which we will use to define the code in the first generic construction, and for every $i = 1, \ldots, q$ define the functions $g_i : \mathbb{F}_q \to \mathbb{F}_p$ such that $g_i(x_i) = \mathrm{Tr}_{q/p}(f(x_i))$ and $g_i(x) = \mathrm{Tr}_{q/p}(x)$ for $x \neq x_i$.

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function, $g_i : \mathbb{F}_q \to \mathbb{F}_p$ be the previously defined functions and consider $(c_1, \ldots, c_q) \in \mathcal{C}(f)^{\perp}$. Then

$$\prod_{i=1}^{q} \left(\hat{\chi}_{g_i}(1) + 1 - q\right)^{c_i} = 1.$$

AN EXAMPLE

1

(Weakly regular) bent function	m	p
$\sum_{i=0}^{[m/2]} Tr_1^m\left(c_1 x^{p^x+1}\right)$	any	any
$\sum_{i=0}^{p^k-1} \mathrm{Tr}_1^m\left(c_i x^{i\left(p^k-1\right)}\right) + \mathrm{Tr}_1^l\left(\epsilon x^{\frac{p^m-1}{\epsilon}}\right)$	$m=2k$	any
$\mathrm{Tr}_1^m\left(cx^{\frac{3m-1}{4}}+3^k+1\right)$	$m=2k$	$p=3$
$\mathrm{Tr}_1^m\left(x^{p^{3k}+p^{2k}-p^k+1}+x^2\right)$	$m=4k$	any
$\mathrm{Tr}_1^m\left(cx^{\frac{3^i+1}{2}}\right)$, i odd $\gcd(i,m)=1$	any	$p=3$

[1] X. Du, W. Jin, S. Mesnager: Several classes of new weakly regular bent functions outside RF, their duals and some related (minimal) codes with few weights, Springer, 2023

AN EXAMPLE

Let $p = 3, m = 2, c = 1$ and $i = 3$; then we get the function

$$\mathrm{Tr}_1^2(x^6).$$

We could study the dual code of the linear code obtained via the first generic construction with the function

$$f(x) = x^6.$$

With the software MAGMA we conclude that the dual code is contained in the linear code described by the following parity check equation

$$X_2 + 2X_4 + X_6 + 2X_8 = 0.$$

THE HULL CODE

PROPOSITION (F., 2023+)

Let f be a function from $\mathbb{F}_q$ to $\mathbb{F}_q$ and $\mathcal{C}(f)$ be the code built with the first generic construction. Define

$$\boldsymbol{c}_{\alpha,\beta} := (Tr_{q/p}(\alpha f(x) + \beta x))_{x \in \mathbb{F}_q}$$

and consider the following linear mapping

$$\varphi : C(f) \longrightarrow \mathbb{F}_q^2$$

$$\boldsymbol{c}_{\alpha,\beta} \longmapsto (\sum_{i=1}^{q} Tr_{q/p}(\alpha f(x_i) + \beta x_i)x_i, \sum_{i=1}^{q} Tr_{q/p}(\alpha f(x_i) + \beta x_i)f(x_i)).$$

Then

$$Hull(C(f)) = ker(\varphi)$$

and in particular

$$dim(Hull(C(f))) = l \iff rk(\varphi) = dim(C(f)) - l.$$

THE HULL CODE

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that the previously defined function g is weakly regular bent and consider $\mathbf{c}_{\alpha,\beta} \in \mathcal{C}(f)$. If $\mathbf{c}_{\alpha,\beta} \in Hull(C(f))$ then

1. *if f respects the scalar multiplication:*

$$\prod_{i=1}^{q} \hat{\chi}_{g^*}(Tr_{q/p}(\alpha f(x_i) + \beta x_i)x_i) = \left(\frac{p^m}{\epsilon\sqrt{p^*}^m}\right)^q,$$

2. *for a generic f:*

$$\prod_{i=1}^{q} \left(\hat{\chi}_{g^*}(x_i)\right)^{Tr_{q/p}(\alpha f(x_i)+\beta x_i)} = \prod_{i=1}^{q} \left(\frac{p^m}{\epsilon\sqrt{p^*}^m}\right)^{Tr_{q/p}(\alpha f(x_i)+\beta x_i)}.$$

THE SECOND GENERIC CONSTRUCTION

DEFINITION

The second generic construction of linear codes from functions is obtained by fixing a set $D = \{d_1, d_2, \cdots, d_n\}$ in $\mathbb{F}_q$ (where $q = p^k$) and by defining a linear code involving D as follows:

$$\mathcal{C}_D = \{(Tr_{q/p}(xd_1), Tr_{q/p}(xd_2), \cdots, Tr_{q/p}(xd_n)) \mid x \in \mathbb{F}_q\}.$$

The set D is usually called the *defining-set* of the code $\mathcal{C}_D$. The resulting code $\mathcal{C}_D$ is linear over $\mathbb{F}_p$ of length n with dimension at most k.

LINK WITH THE WALSH TRANSFORM

Consider a function $f : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^m$, which we will use the define the code in the second generic construction, with p odd, using the deining set

$$D(f) = \{f(x) \,|\, x \in \mathbb{F}_q\} \setminus \{0\} = \{f(x_1), \ldots, f(x_n)\}.$$

Now we define the following function

$$\begin{aligned} g : \mathbb{F}_q &\longrightarrow \mathbb{F}_p \\ x &\longmapsto \mathrm{Tr}_{q/p}(f(x)). \end{aligned}$$

If we suppose that g is weakly regular bent, as we already saw then there exists another function $g^* : \mathbb{F}_q \to \mathbb{F}_p$ such that, for $b \in \mathbb{F}_q$:

$$\hat{\chi}_g(b) = \epsilon \sqrt{p^*}^m \zeta^{g^*(b)}$$

and

$$\hat{\chi}_{g^*}(b) = \frac{\epsilon p^m}{\sqrt{p^*}^m} \zeta^{g(b)},$$

where $\epsilon = \pm 1$ is the sign of the Walsh transform of $f(x)$, $p^* = (\frac{-1}{p})p$ and $\zeta = e^{\frac{2\pi i}{p}}$ is the primitive p-th root of unity.

LINK WITH THE WALSH TRANSFORM

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that the previously defined function g is weakly regular bent and consider $(c_1, \ldots, c_n) \in \mathcal{C}^{\perp}_{D(f)}$. Then

1. *if f respects the scalar multiplication:*

$$\prod_{i=1}^{n} \hat{\chi}_{g^*}(c_i x_i) = \left(\frac{\epsilon p^m}{\sqrt{p^*}^m}\right)^n,$$

2. *for a generic f:*

$$\prod_{i=1}^{n} \left(\hat{\chi}_{g^*}(x_i)\right)^{c_i} = \prod_{i=1}^{n} \left(\frac{\epsilon p^m}{\sqrt{p^*}^m}\right)^{c_i}.$$

WEIGHT ENUMERATOR IN THE EVEN CHARACTERISTIC

Let $\mathbb{F}_q$ be a finite field of even characteristic.

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that the previously defined function g is (weakly regular) bent and consider $\boldsymbol{c} = (c_1, \ldots, c_q) \in \mathcal{C}^{\perp}_{D(f)}$. Then, if

$$\alpha := \prod_{i=1}^{n} \left(\hat{\chi}_{g^*}(x_i)\right)^{c_i}$$

we have

$$wt(\boldsymbol{c}) = \frac{\log_2(\alpha^2)}{m}.$$

The general case

Consider a function $f : \mathbb{F}_q \to \mathbb{F}_q$, $q = p^m$, which we will use to define the code in the second generic construction, and for every $i = 1, \ldots, n$ define the functions $g_i : \mathbb{F}_q \to \mathbb{F}_p$ such that $g_i(x_i) = \mathrm{Tr}_{q/p}(f(x_i) + x_i)$ and $g_i(x) = \mathrm{Tr}_{q/p}(x)$ for $x \neq x_i$. Then we have the following necessary condition.

Proposition (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function, $g_i : \mathbb{F}_q \to \mathbb{F}_p$ be the previously defined functions and consider $(c_1, \ldots, c_n) \in \mathcal{C}_{D(f)}^{\perp}$. Then

$$\prod_{i=1}^{n} \left(\hat{\chi}_{g_i}(1) + 1 - q\right)^{c_i} = 1.$$

THE HULL CODE

PROPOSITION (F., 2023+)

Let $D = \{d_1, \ldots, d_n\} \subseteq \mathbb{F}_q$ be a defining set for a code in the second generic construction. Define $\boldsymbol{c}_x := (Tr_{q_p}(xd))_{d \in D}$ and consider the following linear mapping

$$\begin{aligned} \varphi : \mathcal{C}_D &\longrightarrow \mathbb{F}_q \\ \boldsymbol{c}_x &\longmapsto \sum_{d \in D} Tr(xd)d. \end{aligned}$$

Then

$$Hull(\mathcal{C}_D) = ker(\varphi)$$

and in particular, if $dim(\mathcal{C}_D) = k$ then

$$dim(Hull(\mathcal{C}_D)) = l \iff rk(\varphi) = k - l.$$

THE HULL CODE

PROPOSITION (F., 2023+)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be a function such that the previously defined function g is weakly regular bent and consider $\boldsymbol{c}_x \in \mathcal{C}_{D(f)}$. If $\boldsymbol{c}_x \in Hull(\mathcal{C}_{D(f)})$ then

1. *if f respects the scalar multiplication:*

$$\prod_{i=1}^{n} \hat{\chi}_{g^*}(Tr(xf(x_i))x_i) = \left(\frac{\epsilon p^m}{\sqrt{p^*}^m}\right)^n,$$

2. *for a generic f:*

$$\prod_{i=1}^{n} \left(\hat{\chi}_{g^*}(x_i)\right)^{Tr(xf(x_i))} = \prod_{i=1}^{n} \left(\frac{\epsilon p^m}{\sqrt{p^*}^m}\right)^{Tr(xf(x_i))}.$$

CONSTRUCTION OF FIXED HULL DIMENSION

Let $\mathbb{F}_p$ be a finite field in which -1 is a quadratic residue (for example $p = 5$) and in particular let $\alpha \in \mathbb{F}_p$ be a root of the polynomial $x^2 + 1$. Also consider $\beta \in \mathbb{F}_p$ such that $\beta^2 \neq -1$ and take $d_1, \ldots, d_k \in \mathbb{F}_q$, $q = p^m$, which are linear independent over $\mathbb{F}_p$ and $0 \leq l \leq k$.
Now we consider the following defining set

$$D = \{d_1, \ldots, d_k, \alpha d_1, \ldots, \alpha d_l, \beta d_{l+1}, \ldots, \beta_{d_k}\}.$$

CONSTRUCTION OF FIXED HULL DIMENSION

Let $\mathbb{F}_p$ be a finite field in which -1 is a quadratic residue (for example $p = 5$) and in particular let $\alpha \in \mathbb{F}_p$ be a root of the polynomial $x^2 + 1$. Also consider $\beta \in \mathbb{F}_p$ such that $\beta^2 \neq -1$ and take $d_1, \ldots, d_k \in \mathbb{F}_q$, $q = p^m$, which are linear independent over $\mathbb{F}_p$ and $0 \leq l \leq k$.
Now we consider the following defining set

$$D = \{d_1, \ldots, d_k, \alpha d_1, \ldots, \alpha d_l, \beta d_{l+1}, \ldots, \beta_{d_k}\}.$$

The code $\mathcal{C}_D$ built with the second generic construction is a linear code over $\mathbb{F}_p$ of Hull dimension l.

Construction of fixed Hull dimension

$$\begin{cases} \mathrm{Tr}(xd_1)d_1 + \mathrm{Tr}(x\alpha d_1)\alpha d_1 = 0 \\ \mathrm{Tr}(xd_2)d_2 + \mathrm{Tr}(x\alpha d_2)\alpha d_2 = 0 \\ \dots \\ \mathrm{Tr}(xd_l)d_l + \mathrm{Tr}(x\alpha d_l)\alpha d_l = 0 \\ \mathrm{Tr}(xd_{l+1})d_{l+1} + \mathrm{Tr}(x\beta d_{l+1})\beta d_{l+1} = 0 \\ \dots \\ \mathrm{Tr}(xd_k)d_k + \mathrm{Tr}(x\beta d_k)\beta d_k = 0 \end{cases} \iff \begin{cases} (\alpha^2+1)\mathrm{Tr}(xd_1)d_1 = 0 \\ (\alpha^2+1)\mathrm{Tr}(xd_2)d_2 = 0 \\ \dots \\ (\alpha^2+1)\mathrm{Tr}(xd_l)d_l = 0 \\ (\beta^2+1)\mathrm{Tr}(xd_{l+1})d_{l+1} = 0 \\ \dots \\ (\beta^2+1)\mathrm{Tr}(xd_k)d_k = 0. \end{cases}$$

CONSTRUCTION OF FIXED HULL DIMENSION

$$\begin{cases} \mathrm{Tr}(xd_1)d_1 + \mathrm{Tr}(x\alpha d_1)\alpha d_1 = 0 \\ \mathrm{Tr}(xd_2)d_2 + \mathrm{Tr}(x\alpha d_2)\alpha d_2 = 0 \\ \dots \\ \mathrm{Tr}(xd_l)d_l + \mathrm{Tr}(x\alpha d_l)\alpha d_l = 0 \\ \mathrm{Tr}(xd_{l+1})d_{l+1} + \mathrm{Tr}(x\beta d_{l+1})\beta d_{l+1} = 0 \\ \dots \\ \mathrm{Tr}(xd_k)d_k + \mathrm{Tr}(x\beta d_k)\beta d_k = 0 \end{cases} \iff \begin{cases} (\alpha^2+1)\mathrm{Tr}(xd_1)d_1 = 0 \\ (\alpha^2+1)\mathrm{Tr}(xd_2)d_2 = 0 \\ \dots \\ (\alpha^2+1)\mathrm{Tr}(xd_l)d_l = 0 \\ (\beta^2+1)\mathrm{Tr}(xd_{l+1})d_{l+1} = 0 \\ \dots \\ (\beta^2+1)\mathrm{Tr}(xd_k)d_k = 0. \end{cases}$$

$$\mathrm{Hull}(\mathcal{C}_D) \cong \frac{\bigcap_{i=l+1}^{k} d_i^{-1}\ker(\mathrm{Tr}_{q/p})}{\bigcap_{d\in D} d_i^{-1}\ker(\mathrm{Tr}_{q/p})}.$$

Also, $\dim(\bigcap_{i=l+1}^{k} d_i^{-1}\ker(\mathrm{Tr}_{q/p})) = m+k-l$. Hence $\dim_{\mathbb{F}_p}(\mathrm{Hull}(\mathcal{C}_D)) = m+l-k-(m-k) = l$, as we wanted to show.

The work is available as a preprint at:

arXiv:2307.14300 (submitted)

The work is available as a preprint at:

arXiv:2307.14300 (submitted)

Thank you for your attention!