# 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

Young Research Algebra Conference 2023
L'Aquila, Italy

27th July 2023

# Index

# Coding theory

**Coding theory** is the study of the properties of codes and their fitness for specific application, like data compression for cloud storage, wireless data transmission and especially **cryptography**.
It involves various scientific disciplines, for example mathematics, information theory, computer science, artificial intelligence and linguistics.

It is based on mathematical methods, especially algebraic ones in the linear codes case.

# Linear codes

**Definition**

A **linear codes** of length $n$ and rank $k$ is a linear subspace $\mathcal{C}$ with dimension $k$ of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with $q$ elements.

# LINEAR CODES

### DEFINITION

A **linear codes** of length $n$ and rank $k$ is a linear subspace $\mathcal{C}$ with dimension $k$ of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite field with $q$ elements.

The vectors in $\mathcal{C}$ are called *codewords* and the **size** of a code is the number of codewords and equals $q^k$.

# WEIGHT OF A LINEAR CODE

The **Hamming weight** of a codeword is the number of its elements that are nonzero and the **Hamming distance** between two codewords is the Hamming distance between them, that is, the number of elements in which they differ. The distance $d$ of the linear code is the minimum weight of its nonzero codewords, or equivalently, the minimum distance between distinct codewords.

A linear code of length $n$, dimension $k$, and distance $d$ is called an $[n, k, d]$-code.

## Generator and parity check matrices

Let $\mathcal{C}$ be a $q$-ary $[n, k, d]$-code.

# GENERATOR AND PARITY CHECK MATRICES

Let $\mathcal{C}$ be a $q$-ary $[n, k, d]$-code.

### GENERATOR MATRIX

A **generator matrix** $G$ for $\mathcal{C}$ is a matrix whose rows form a basis for $\mathcal{C}$, hence it is a $k \times n$ matrix.

# Generator and parity check matrices

Let $\mathcal{C}$ be a $q$-ary $[n, k, d]$-code.

### Generator matrix

A **generator matrix** $G$ for $\mathcal{C}$ is a matrix whose rows form a basis for $\mathcal{C}$, hence it is a $k \times n$ matrix.

### Parity check matrix

A **parity check matrix** for $\mathcal{C}$ is a matrix $H$ representing a linear function $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^{n-k}$ whose kernel coincides with $\mathcal{C}$, hence it is a $(n-k) \times n$ matrix.

# THE DUAL CODE

## SCALAR PRODUCT

Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_q$, so $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$ with dimension $k$ and minimum Hamming distance $d$. We observe that the vector space $\mathbb{F}_q^n$ has a natural inner product: let $x = (x_0, \ldots, x_{n-1})$ and $y = (y_1, \ldots, y_{n-1})$ be two vectors in $\mathbb{F}_q^n$. Then we define the *scalar product* of $x$ and $y$ in the following way:

$$\langle x, y \rangle = \sum_{i=0}^{n-1} x_i y_i.$$

# The dual code

## Definition

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$, then its *Euclidean dual code* is denoted by $\mathcal{C}^\perp$ and it is defined in the following way:

$$\mathcal{C}^\perp := \{l \in \mathbb{F}_q^n \,:\, \langle l, c\rangle = 0 \text{ for all } c \in \mathcal{C}\}.$$

In other words:

$$\mathcal{C}^\perp := \{(l_0, \dots, l_{n-1}) \in \mathbb{F}_q^n \,:\, \sum_{i=0}^{n-1} l_i c_i = 0 \text{ for all } (c_0, \dots, c_{n-1}) \in \mathcal{C}\}.$$

# 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

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

Effectively, the Hull code can be characterized algebraically in the following way

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

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 (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

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

## Theorem (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.

# The dual code

**Proposition (F.)**

*Let $f$ be a polynomial from $\mathbb{F}_q$ to $\mathbb{F}_q$, $\mathcal{C}(f)$ be the code built with the first generic construction, $l_1 = (x_1, \ldots, x_q)$, $l_2 = (f(x_1), \ldots, f(x_q))$, $\mathcal{L}_1$ be the code generated by $l_1$ and $\mathcal{L}_2$ the code generated by $l_2$ over $\mathbb{F}_q$. Then*

$$\mathcal{C}(f)^{\perp} = \mathcal{L}_1^{\perp} \cap \mathcal{L}_2^{\perp} \cap \mathbb{F}_p^q.$$

## The dual code

### Proposition (F.)

*Let $f$ be a polynomial from $\mathbb{F}_q$ to $\mathbb{F}_q$, $\mathcal{C}(f)$ be the code built with the first generic construction, $l_1 = (x_1, \ldots, x_q)$, $l_2 = (f(x_1), \ldots, f(x_q))$, $\mathcal{L}_1$ be the code generated by $l_1$ and $\mathcal{L}_2$ the code generated by $l_2$ over $\mathbb{F}_q$. Then*

$$\mathcal{C}(f)^\perp = \mathcal{L}_1^\perp \cap \mathcal{L}_2^\perp \cap \mathbb{F}_p^q.$$

Hence, we have reduced the computation of the dual code to an orthogonality problem for which it is possible to use the Gram-Schmidt algorithm; we recall that in this case the complexity is $\mathcal{O}(q^3)$.

# 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

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

where $\epsilon = \pm 1$ is the sign of the Walsh tranform of $f(x)$, $p^* = (\frac{-1}{p})p$ and $\zeta = e^{\frac{2\pi i}{p}}$ is the primitive $p$-th root of unity. In this case, with the same notation, fixing an enumeration $(x_i)_{i=1,\dots,q}$ in $\mathbb{F}_q$, we have the following necessary condition.

# Link with the Walsh transform

## Proposition (F.)

*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 $x \in \mathbb{F}_q$, $f(\alpha x) = \alpha f(x)$:*
$$\prod_{i=1}^{q} \hat{\chi}_{g^*}(c_i x_i) = \Big(\frac{p^m}{\epsilon\sqrt{p^*}^m}\Big)^q,$$
2. *for a generic $f$:*
$$\prod_{i=1}^{q} \big(\hat{\chi}_{g^*}(x_i)\big)^{c_i} = \prod_{i=1}^{q} \Big(\frac{p^m}{\epsilon\sqrt{p^*}^m}\Big)^{c_i}.$$

# 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 $x \neq x_i$.

## 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.)**

*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 |
| $\sum_{i=0}^{p^k-1} \mathrm{Tr}_1^m\left(c_i x^{i(p^k-1)}\right) + \mathrm{Tr}_1^l\left(\epsilon x^{\frac{p^m-1}{\epsilon}}\right)$ | $m = 2k$ | 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.)

*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*

$$\begin{aligned}\varphi : C(f) &\longrightarrow \mathbb{F}_q^2\\ \boldsymbol{c}_{\alpha,\beta} &\longmapsto \Big(\sum_{i=1}^{q} Tr_{q/p}(\alpha x_i + \beta x_i)x_i, \sum_{i=1}^{q} Tr_{q/p}(\alpha x_i + \beta x_i)f(x_i)\Big).\end{aligned}$$

*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.)

*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 $k$.

# The dual code

**Proposition (F.)**

*Let $D = \{d_1, \ldots, d_n\} \subseteq \mathbb{F}_q$ be a defining set for a code in the second generic construction, and let $\mathcal{L}$ be the linear code over $\mathbb{F}_q$ generated by the codeword $l = (d_1, \ldots, d_n)$. Then*

$$\mathcal{C}_D^{\perp} = \mathcal{L}^{\perp} \cap \mathbb{F}_p^n.$$

# THE DIMENSION

**LEMMA (CUNSHENG DING, HARALD NIEDERREITER, 2007)**

*Let $D = \{d_1, \dots, d_n\} \subseteq \mathbb{F}_q$ be a defining set for a code in the second generic construction, then*

$$dim(\mathcal{C}_D) = dim_{\mathbb{F}_p}\langle d_1, \dots, d_n\rangle.$$

# The dimension

**Proof.**

After having chosen a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, we write the elements $d_i$ as vectors in this basis, then

$$M := (d_1, \ldots, d_n)$$

is a $m \times n$ matrix with entrances in $\mathbb{F}_p$ such that

$$\mathcal{C}_D^{\perp} = \ker(M).$$

Hence, we have our dimensions:

$$\dim(\mathcal{C}_D^{\perp}) = n - \dim_{\mathbb{F}_p}\langle d_1, \ldots, d_n\rangle.$$

And finally

$$\dim(\mathcal{C}_D) = \dim_{\mathbb{F}_p}\langle d_1, \ldots, d_n\rangle.$$

$\square$

# The inverse problem

**Proposition**

*Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_p$ and let $m \in \mathbb{N}$. Then there exists a defining set $D \in \mathbb{F}_q^n$, $q = p^m$, such that*

$$\mathcal{C} = \mathcal{C}_D$$

*if and only if $m \geq k$.*

[1] Can Xiang, It is indeed a fundamental construction of all linear codes, arXiv:1610.06355, 2016
Cunsheng Ding, The construction and weight distributions of all projective binary linear codes, arXiv:2010.03184, 2020

## The inverse problem

### Proposition

*Let $\mathcal{C}$ be a $[n, k, d]$ linear code over $\mathbb{F}_p$ and let $m \in \mathbb{N}$. Then there exists a defining set $D \in \mathbb{F}_q^n$, $q = p^m$, such that*

$$\mathcal{C} = \mathcal{C}_D$$

*if and only if $m \geq k$.*

$$\begin{aligned} \varphi : \mathbb{F}_q^n &\longrightarrow \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_q, \mathbb{F}_p^n) \\ D &\longmapsto \varphi_D, \end{aligned}$$

where $\varphi_D(x) := \mathbf{c}_x = (\mathrm{Tr}_{q/p}(xd_i))_{i=1,\dots,n}$, a codeword of the linear code $\mathcal{C}_D$.

[1] Can Xiang, It is indeed a fundamental construction of all linear codes, arXiv:1610.06355, 2016
Cunsheng Ding, The construction and weight distributions of all projective binary linear codes, arXiv:2010.03184, 2020

# 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

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

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

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

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.)

*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 $(c_1, \dots, c_n) \in \mathcal{C}^{\perp}_{D(f)}$. Then*

1. *if $f$ respects the scalar multiplication:*

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

2. *for a generic $f$:*

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

# 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 second generic construction, and for every $i = 1, \dots, n$ 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.)**

*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 $(c_1, \dots, c_n) \in \mathcal{C}^{\perp}_{D(f)}$. Then*

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

## The Hull code

**Proposition (F.)**

*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.)

*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 $\mathbf{c}_x \in \mathcal{C}_{D(f)}$. If $\mathbf{c}_x \in Hull(\mathcal{C}_{D(f)})$ then*

1. *if $f$ respects the scalar multiplication:*

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

2. *for a generic $f$:*

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

# 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 $d_1, \dots, d_k \in \mathbb{F}_q$, $q = p^m$, which are linear independent over $\mathbb{F}_p$ and $0 \leq l \leq k$.
Now we consider the following defining set

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

# 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 $d_1, \dots, d_k \in \mathbb{F}_q$, $q = p^m$, which are linear independent over $\mathbb{F}_p$ and $0 \leq l \leq k$.
Now we consider the following defining set

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

The linear code $\mathcal{C}_D$ built with the second generic construction is a $[2k, k, 2]$ 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.

# Example of LCD code

Let $q = 2^a$ and $r = q^b$ with $a, b \in \mathbb{N}^*$; fix $k$ linearly independent elements $d_1, \dots, d_k$ of $\mathbb{F}_r$ over $\mathbb{F}_q$, with $k$ even and define the set $D_1 = \{d_1, \dots, d_k\}$. Let $D_2$ be the set of elements in $D_1$, for example

$$D_2 = \{d_1 + d_2, d_3 + d_4, \dots, d_{k-1} + d_k\}.$$

We consider the defining set $D = D_1 \cup D_2$ and we define the code

$$\mathcal{C}_D = \{(\mathrm{Tr}_{r/q}(xd)_{d \in D}) \mid x \in \mathbb{F}_r\}.$$

# Example of LCD code

Let $q = 2^a$ and $r = q^b$ with $a, b \in \mathbb{N}^*$; fix $k$ linearly independent elements $d_1, \ldots, d_k$ of $\mathbb{F}_r$ over $\mathbb{F}_q$, with $k$ even and define the set $D_1 = \{d_1, \ldots, d_k\}$. Let $D_2$ be the set of elements in $D_1$, for example

$$D_2 = \{d_1 + d_2, d_3 + d_4, \ldots, d_{k-1} + d_k\}.$$

We consider the defining set $D = D_1 \cup D_2$ and we define the code

$$\mathcal{C}_D = \{(\mathrm{Tr}_{r/q}(xd)_{d \in D}) \mid x \in \mathbb{F}_r\}.$$

The obtain code $\mathcal{C}_D$ is LCD of length $\frac{3k}{2}$ and dimension $k$.

The work is available as a preprint at:

*arXiv:2307.14300*

The work is available as a preprint at:

*arXiv:2307.14300*

Thank you for your attention!