# Constructions of linear codes from vectorial almost bent functions and their subfield codes

Virginio Fratianni
Université Paris VIII, LAGA, UMR 7539
PhD student under the supervision of Sihem Mesnager

Journées C2 2025
Pornichet - Baie de La Baule

April 3rd, 2025

# Index

1. Preliminaries on cryptographic functions
2. First generic construction of linear codes
3. Linear codes from functions and their subfield codes

# 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 parity-check matrix of the linear code $\mathcal{C}$.

# The trace function

The trace function $\mathrm{Tr}_{p^n/p} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as

$$\mathrm{Tr}_{p^n/p}(x) := \sum_{i=0}^{n-1} x^{p^i} = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}.$$

If we identify the vector space $\mathbb{F}_p^n$ with the finite field $\mathbb{F}_{p^n}$, we use the trace bilinear form $\mathrm{Tr}_{p^n/p}(\lambda x)$ instead of the dot product, that is,

$$\lambda \cdot x = \mathrm{Tr}_{p^n/p}(\lambda x),$$

where $\lambda, x \in \mathbb{F}_{p^n}$.

# THE WALSH TRANSFORM

### DEFINITION

Let $q = p^r$ where $p$ is a prime. A vectorial function $\mathbb{F}_q^n \to \mathbb{F}_q^m$ (or $\mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$) is called an $(n, m)$*-q-ary function*. When $q = 2$, an $(n, m)$-2-ary function will be simply denoted an $(n, m)$*-function*. A *Boolean function* is an $(n, 1)$-function, that is, a function $\mathbb{F}_2^n \to \mathbb{F}_2$ (or $\mathbb{F}_{2^n} \to \mathbb{F}_2$).

# The Walsh transform

## Definition

Let $q = p^r$ where $p$ is a prime. A vectorial function $\mathbb{F}_q^n \to \mathbb{F}_q^m$ (or $\mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$) is called an $(n, m)$*-$q$-ary function*. When $q = 2$, an $(n, m)$-2-ary function will be simply denoted an $(n, m)$*-function*. A *Boolean function* is an $(n, 1)$-function, that is, a function $\mathbb{F}_2^n \to \mathbb{F}_2$ (or $\mathbb{F}_{2^n} \to \mathbb{F}_2$).

Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a $p$-ary function, then the Walsh transform of $f$ is given by:

$$\hat{\chi}_f(\lambda) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{f(x) - \mathrm{Tr}_{p^m/p}(\lambda x)},$$

for $\lambda \in \mathbb{F}_{p^m}$; where $\zeta = e^{\frac{2\pi i}{p}}$ is a complex primitive $p$-th root of the unity.

## BENT FUNCTIONS

- A $p$-ary function $f : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_p$ is called **bent** if all its Walsh-Hadamard coefficients satisfy

$$|\hat{\chi}_f(b)|^2 = p^m.$$

- A bent function $f$ is called **regular bent** if, for every $b \in \mathbb{F}_{p^m}$,

$$p^{-\frac{m}{2}} \hat{\chi}_f(b) = \zeta_p^{f^*(b)}$$

  for some $p$-ary function $f^* : \mathbb{F}_{p^m} \to \mathbb{F}_p$.

- The bent function $f$ is called **weakly regular bent** if there exists a complex number $u$ with $|u| = 1$ and a $p$-ary function $f^*$ such that

$$up^{-\frac{m}{2}} \widehat{\chi}_f(b) = \zeta_p^{f^*(b)}$$

  for all $b \in \mathbb{F}_{p^m}$. This function $f^*(x)$ is called the dual of $f(x)$.

# 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

$$\mathcal{C}(f) = \{\mathbf{c}_{\alpha,\beta} = (\mathrm{Tr}_{q/p}(\alpha f(x) + \beta x))_{x \in \mathbb{F}_q} \mid \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q\}.$$

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.

One can also define a code $\mathcal{C}^\star(f)$ over $\mathbb{F}_p$ involving a polynomial $f$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ (where $q = p^m$) which vanishes at 0 defined by

$$\mathcal{C}^\star(f) = \{\mathbf{c}_{\alpha,\beta} = (\mathrm{Tr}_{q/p}(\alpha f(x) + \beta x))_{x \in \mathbb{F}_q^*} \mid \alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q\}.$$

The resulting code $\mathcal{C}^\star(f)$ from $f$ is a linear code of length $q - 1$, and its dimension is also upper bounded by $2m$.

# The first generic construction

The first generic construction has a long history concerning the application of $p$-ary functions in coding theory and cryptography, as presented by Ding [1]. In particular, its importance is supported by Delsarte's theorem in the paper [2] about modified Reed-Solomon codes and, in the binary case, it gives a coding theory characterization of APN monomials and almost bent functions.

[1] C. Ding. A construction of binary linear codes from Boolean functions. Discrete Mathematics, Vol 339, Issue 9, pp. 2288-2303, 2016

[2] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. IEEE Trans. Inf. Theory, 21(5), (1975), 575– 576

# THE FIRST GENERIC CONSTRUCTION

The first generic construction has a long history concerning the application of *p*-ary functions in coding theory and cryptography, as presented by Ding [1]. In particular, its importance is supported by Delsarte's theorem in the paper [2] about modified Reed-Solomon codes and, in the binary case, it gives a coding theory characterization of APN monomials and almost bent functions.

## PROPOSITION (MESNAGER, 2017)

*For $a \in \mathbb{F}_{p^m}$, let us denote by $f_a$ a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ defined as:*

$$f_a(x) := Tr_{p^m/p}(af(x))$$

*For $\mathbf{c}_{\alpha,\beta} \in \mathcal{C}(f)$, we have*

$$wt\left(\mathbf{c}_{\alpha,\beta}\right) = p^m - \frac{1}{q} \sum_{\omega \in \mathbb{F}_q} \widehat{\chi_{f_{\omega\alpha}}}(\omega\beta).$$

[1] C. Ding. A construction of binary linear codes from Boolean functions. Discrete Mathematics, Vol 339, Issue 9, pp. 2288-2303, 2016

[2] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. IEEE Trans. Inf. Theory, 21(5), (1975), 575– 576

# Subfield codes

Generally, given an $[n, k]$ linear code $\mathcal{C}$ with a generator matrix $G$ over $\mathbb{F}_{q^m}$, a new $[n, k']$ linear code $\mathcal{C}^{(q)}$ over $\mathbb{F}_q$ can be constructed as follows.

Take a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Represent each entry of $G$ as an $m \times 1$ column vector of $\mathbb{F}_{q^m}$ with respect to this basis, and replace each entry of $G$ with the corresponding $m \times 1$ column vector of $\mathbb{F}_{q^m}$. In this way, $G$ is modified into a $km \times n$ matrix over $\mathbb{F}_q$, which generates the new subfield code $\mathcal{C}^{(q)}$ over $\mathbb{F}_q$ with length $n$.

Obviously, the dimension $k'$ of $\mathcal{C}^{(q)}$ satisfies $k' \leq mk$. It was proved by Ding and Heng[3] that the subfield code is independent of the choice of both $G$ and the basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

[3] C. Ding and Z. Heng, *The subfield codes of ovoid codes*, IEEE Trans. Inf. Theory, vol. 65, no. 8, pp. 4715–4729, Aug. 2019.

# TRACE REPRESENTATION

### LEMMA (DING, HENG)

*Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_{q^m}$, with a generator matrix $G = [g_{ij}]_{1\leq i\leq k, 1\leq j\leq n}$. Then the trace representation of the subfield code $\mathcal{C}^{(q)}$ is given by $\mathcal{C}^{(q)} =$*

$$\left\{ \left( \mathrm{Tr}_{q^m/q}\left(\sum_{i=1}^{k} a_i g_{i1}\right), \cdots, \mathrm{Tr}_{q^m/q}\left(\sum_{i=1}^{k} a_i g_{in}\right) \right) : a_1, \ldots, a_k \in \mathbb{F}_{q^m} \right\},$$

*where $\mathrm{Tr}_{q^m/q}(x) = \sum_{i=0}^{m-1} x^{q^i}$ denotes the trace function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$.*

The subfield codes of some optimal codes or very good codes over $\mathbb{F}_{q^m}$ have been studied in several references, for example ovoid codes, hyperoval codes, conic codes, arc codes, some cyclic codes and maximum distance separable (MDS) codes. Most of the resultant subfield codes have good parameters and few weights.

Recently, Xu et al.[4] proposed a construction method of linear codes from two functions and studied their subfield codes. Let $f$ and $g$ be two functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Define a subset $\mathcal{D}$ of $\mathbb{F}_{q^m}^2$ as

$$\mathcal{D} = \left\{(x, y) \in \mathbb{F}_{q^m}^2 : f(x) + g(y) = 0\right\}$$

and a $3 \times (\#\mathcal{D})$ matrix $G_{f,g}^*$ over $\mathbb{F}_{q^m}$ as

$$G_{f,g}^* = \begin{pmatrix} 1 \\ x \\ y \end{pmatrix}_{(x,y)\in\mathcal{D}} .$$

Then a $[\#\mathcal{D} + 1, 3]$ linear code $\mathcal{C}_{f,g}$ over $\mathbb{F}_{q^m}$ can be obtained with the generator matrix

$$G_{f,g} = \begin{pmatrix} 0 & \\ 1 & G_{f,g}^* \\ 0 & \end{pmatrix} .$$

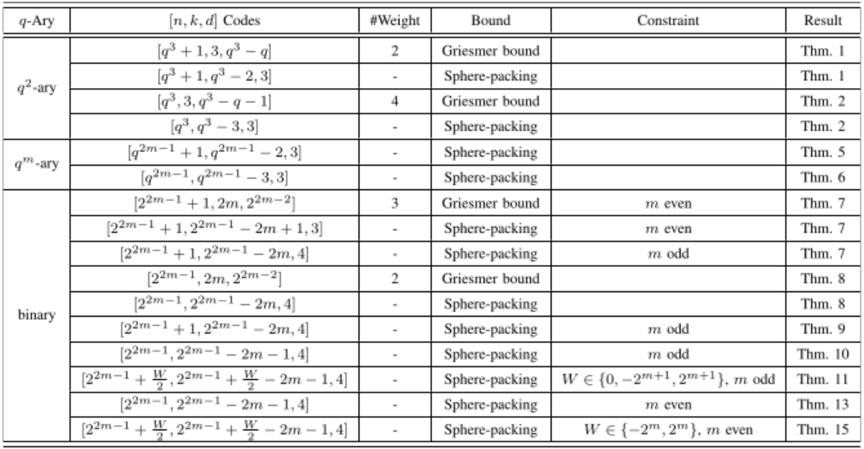
[4] L. Xu, C. Fan, S. Mesnager, R. Luo and H. Yan, *Subfield Codes of Several Few-Weight Linear Codes Parameterized by Functions and Their Consequences*, in IEEE Transactions on Information Theory, vol. 70, no. 6, pp. 3941-3964, June 2024

# The considered cases

The authors studied the linear codes obtained from the following functions and the respective subfield codes.

- $f_1(x) = \mathrm{Tr}_{q^2/q}(x)$ and $g_1(x) = \mathrm{Norm}_{q^2/q}(y)$;
- $f_2(x) = \mathrm{Tr}_{q^m/q}(x)$ and $g_2(x) = \mathrm{Tr}_{q^m/q}(y^2)$;
- $f_3(x) = \mathrm{Tr}_{2^m/2}(x)$ and $g_3(y) = \mathrm{Tr}_{2^m/2}(A(y))$, where $m$ is odd and $A(y)$ is an almost bent function from $\mathbb{F}_{2^m}$ to itself;
- $f_4(x) = \mathrm{Tr}_{2^m/2}(A_1(x))$ and $g_4(y) = \mathrm{Tr}_{2^m/2}(A_2(y))$, where $m$ is odd and $A_1$ and $A_2$ are two almost bent functions from $\mathbb{F}_{2^m}$ to itself;
- $f_5(x) = \mathrm{Tr}_{2^m/2}(x)$ and $g_5(y) = B(y)$, where $m$ is even and $B(y)$ is a bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$;
- $f_6(x) = B_1(x)$ and $g_6(y) = B_2(y)$, where $B_1(x)$ and $B_2(y)$ are two bent functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, with $m$ even.

# Optimal linear codes presented in the paper



| $q$-Ary | $[n, k, d]$ Codes | #Weight | Bound | Constraint | Result |
|---|---|---|---|---|---|
| $q^2$-ary | $[q^3+1, 3, q^3-q]$ | 2 | Griesmer bound | | Thm. 1 |
| | $[q^3+1, q^3-2, 3]$ | - | Sphere-packing | | Thm. 1 |
| | $[q^3, 3, q^3-q-1]$ | 4 | Griesmer bound | | Thm. 2 |
| | $[q^3, q^3-3, 3]$ | - | Sphere-packing | | Thm. 2 |
| $q^m$-ary | $[q^{2m-1}+1, q^{2m-1}-2, 3]$ | - | Sphere-packing | | Thm. 5 |
| | $[q^{2m-1}, q^{2m-1}-3, 3]$ | - | Sphere-packing | | Thm. 6 |
| binary | $[2^{2m-1}+1, 2m, 2^{2m-2}]$ | 3 | Griesmer bound | $m$ even | Thm. 7 |
| | $[2^{2m-1}+1, 2^{2m-1}-2m+1, 3]$ | - | Sphere-packing | $m$ even | Thm. 7 |
| | $[2^{2m-1}+1, 2^{2m-1}-2m, 4]$ | - | Sphere-packing | $m$ odd | Thm. 7 |
| | $[2^{2m-1}, 2m, 2^{2m-2}]$ | 2 | Griesmer bound | | Thm. 8 |
| | $[2^{2m-1}, 2^{2m-1}-2m, 4]$ | - | Sphere-packing | | Thm. 8 |
| | $[2^{2m-1}+1, 2^{2m-1}-2m, 4]$ | - | Sphere-packing | $m$ odd | Thm. 9 |
| | $[2^{2m-1}, 2^{2m-1}-2m-1, 4]$ | - | Sphere-packing | $m$ odd | Thm. 10 |
| | $[2^{2m-1}+\frac{W}{2}, 2^{2m-1}+\frac{W}{2}-2m-1, 4]$ | - | Sphere-packing | $W \in \{0, -2^{m+1}, 2^{m+1}\}$, $m$ odd | Thm. 11 |
| | $[2^{2m-1}, 2^{2m-1}-2m-1, 4]$ | - | Sphere-packing | $m$ even | Thm. 13 |
| | $[2^{2m-1}+\frac{W}{2}, 2^{2m-1}+\frac{W}{2}-2m-1, 4]$ | - | Sphere-packing | $W \in \{-2^m, 2^m\}$, $m$ even | Thm. 15 |

# APPLICATION TO THREE FUNCTIONS

Let $f$, $g$ and $h$ be three functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. Define a subset $\mathcal{D}$ of $\mathbb{F}_{q^m}^3$ as

$$\mathcal{D} = \left\{(x, y, z) \in \mathbb{F}_{q^m}^3 : f(x) + g(y) + h(z) = 0\right\}$$

and a $4 \times (\#\mathcal{D})$ matrix $G^*_{f,g,h}$ over $\mathbb{F}_{q^m}$ as

$$G^*_{f,g,h} = \begin{pmatrix} 1 \\ x \\ y \\ z \end{pmatrix}_{(x,y,z)\in\mathcal{D}} .$$

Then a $[\#\mathcal{D} + 1, 4]$ linear code $\mathcal{C}_{f,g,h}$ over $\mathbb{F}_{q^m}$ can be obtained with the generator matrix

$$G_{f,g,h} = \begin{pmatrix} 0 & \\ 1 & G^*_{f,g,h} \\ 0 & \\ 0 & \end{pmatrix} .$$

# The subfield code

In this context, the trace representation of the subfield code $\mathcal{C}_{f,g,h}^{(q)}$ is given by

$$\mathcal{C}_{f,g,h}^{(q)} = \{\mathbf{c}_{a,b,c,d} : a \in \mathbb{F}_q, b, c, d \in \mathbb{F}_{q^m}\},$$

where

$$\mathbf{c}_{a,b,c,d} = \left(\mathrm{Tr}_{q^m/q}(b), \left(a + \mathrm{Tr}_{q^m/q}(bx + cy + dz)\right)_{(x,y,z)\in\mathcal{D}}\right).$$

Let $\chi$ and $\chi'$ be the canonical additive character of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively. We define the following two character sums

$$\Phi_{f,g,h} = \sum_{s\in\mathbb{F}_q^*} \sum_{x\in\mathbb{F}_{q^m}} \chi(sf(x)) \sum_{y\in\mathbb{F}_{q^m}} \chi(sg(y)) \sum_{z\in\mathbb{F}_{q^m}} \chi(sh(z))$$

and

$$\Lambda_{a,b,c,d}^{f,g,h} = \sum_{s\in\mathbb{F}_q^*} \chi(sa) \sum_{\omega\in\mathbb{F}_q^*} \sum_{(x,y,z)\in\mathbb{F}_{q^m}^3} \chi(\omega f(x) + \omega g(y) + \omega h(z))\chi'(sbx + scy + sdz),$$

for any $(a, b, c, d) \in \mathbb{F}_q \times \mathbb{F}_{q^m}^3$.

# The parameters of the codes

Let $\delta : \mathbb{F}_{q^m} \to \{0,1\}$ be a function such that $\delta(x) = 0$ if $\mathrm{Tr}_{q^m/q}(x) = 0$ and $\delta(x) = 1$ otherwise.

## Proposition (F.)

*The length of the code $\mathcal{C}_{f,g,h}^{(q)}$ is $n = 1 + q^{3m-1} + \frac{1}{q}\Phi_{f,g,h}$. Also, for any $(a,b,c,d) \in \mathbb{F}_q \times \mathbb{F}_{q^m}^3$, the weight of the codeword $\mathbf{c}_{a,b,c,d}$ is given by*

$$wt(\mathbf{c}_{a,b,c,d}) = \begin{cases} 0 & \text{if } a=b=c=d=0, \\ q^{3m-1} + \frac{1}{q}\Phi_{f,g,h} & \text{if } a \neq 0 \text{ and } b=c=d=0 \\ \delta(b) + q^{3m-2}(q-1) + \frac{1}{q^2}\left[(q-1)\Phi_{f,g,h} - \Lambda_{a,b,c,d}^{f,g,h}\right] & \text{otherwise.} \end{cases}$$

## The parameters of the codes

Let $\delta : \mathbb{F}_{q^m} \to \{0, 1\}$ be a function such that $\delta(x) = 0$ if $\mathrm{Tr}_{q^m/q}(x) = 0$ and $\delta(x) = 1$ otherwise.

### Proposition (F.)

*The length of the code $\mathcal{C}_{f,g,h}^{(q)}$ is $n = 1 + q^{3m-1} + \frac{1}{q}\Phi_{f,g,h}$. Also, for any $(a, b, c, d) \in \mathbb{F}_q \times \mathbb{F}_{q^m}^3$, the weight of the codeword $\mathbf{c}_{a,b,c,d}$ is given by*

$$wt(\mathbf{c}_{a,b,c,d}) = \begin{cases} 0 & \text{if } a = b = c = d = 0, \\ q^{3m-1} + \frac{1}{q}\Phi_{f,g,h} & \text{if } a \neq 0 \text{ and } b = c = d = 0 \\ \delta(b) + q^{3m-2}(q-1) + \frac{1}{q^2}\left[(q-1)\Phi_{f,g,h} - \Lambda_{a,b,c,d}^{f,g,h}\right] & \text{otherwise.} \end{cases}$$

Hence, the length of the punctured code $\mathcal{C}_{f,g,h}^{*(q)}$ is equal to $q^{3m-1} + \frac{1}{q}\Phi_{f,g,h}$ and $\mathrm{wt}(\mathbf{c}^*_{a,b,c,d}) = \mathrm{wt}(\mathbf{c}_{a,b,c,d}) - \delta(b)$.

# Application to specific functions

We choose the functions $f(x) = \mathrm{Tr}_{q^m/q}(x)$, $g(y) = \mathrm{Tr}_{q^m/q}(y^2)$ and $h(z) = \mathrm{Norm}_{q^m/q}(z)$.

### Lemma (F.)

*The code $\mathcal{C}_{f,g,h}$ is of length $1 + q^{3m-1}$ and dimension $4$. In addition, for an even $q$, the values of the sum $\Lambda^{f,g,h}_{a,b,c,d}$ are the following.*

$$\Lambda^{f,g,h}_{a,b,c,d} = \begin{cases} 0 & \text{if } b \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q^* \text{ or } c \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q^* \\ q^{2m} \sum_{z \in \mathbb{F}_{q^m}} \chi\left(\frac{b}{c^2}(a + Tr_{q^m/q}(dz) - bNorm_{q^m/q}(z))\right) & \text{otherwise.} \end{cases}$$

# Application to specific functions

We choose the functions $f(x) = \mathrm{Tr}_{q^m/q}(x)$, $g(y) = \mathrm{Tr}_{q^m/q}(y^2)$ and $h(z) = \mathrm{Norm}_{q^m/q}(z)$.

## Lemma (F.)

*The code $\mathcal{C}_{f,g,h}$ is of length $1 + q^{3m-1}$ and dimension $4$. In addition, for an even $q$, the values of the sum $\Lambda^{f,g,h}_{a,b,c,d}$ are the following.*

$$\Lambda^{f,g,h}_{a,b,c,d} = \begin{cases} 0 & \text{if } b \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q^* \text{ or } c \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q^* \\ q^{2m} \sum_{z\in\mathbb{F}_{q^m}} \chi(\frac{b}{c^2}(a + Tr_{q^m/q}(dz) - bNorm_{q^m/q}(z))) & \text{otherwise.} \end{cases}$$

For $q = 2$ or $m = 2$ and odd $q$, it is possible to determine the values of the sums and, hence, the parameters and weights of the subfield code.

# Application to specific functions

Let $q = 2$ and consider $f(x) = \mathrm{Tr}_{2^m/2}(x)$, $g(y) = \mathrm{Tr}_{2^m/2}(y^2)$ and $h(z)$ a generic function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

## Proposition (F.)

*The code $\mathcal{C}_{f,g,h}$ is of length $1 + 2^{3m-1}$ and dimension $4$. In addition, the values of the sum $\Lambda^{f,g,h}_{a,b,c,d}$ are the following*

$$\Lambda^{f,g,h}_{a,b,c,d} = \begin{cases} (-1)^a 2^{2m} W_h(d) & \textit{if } b = 1 \textit{ and } c = 1 \\ 0 & \textit{otherwise,} \end{cases}$$

*where $W_h$ is the Walsh transform of the function $h$.*

# The bent case

We study the case in which $h$ is bent, so $m$ must be even.

## Theorem (F.)

*Let $m$ be even, $f(x) = Tr_{2^m/2}(x)$, $g(y) = Tr_{2^m/2}(y^2)$ and $h(z) = B(z)$, a bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Then $\mathcal{C}^{(2)}_{f,g,h}$ is a five-weights $[2^{3m-1}+1, 3m+1, 2^{3m-2}-2^{\frac{5m-4}{2}}]$ binary linear code, with the following weight distribution*

| Weight | Multiplicity |
|---|---|
| 0 | 1 |
| $2^{3m-2}-2^{\frac{5m-4}{2}}$ | $2^m$ |
| $2^{3m-2}$ | $2^{3m}-2^{m+1}-2$ |
| $2^{3m-2}+1$ | $2^{3m}$ |
| $2^{3m-2}+2^{\frac{5m-4}{2}}$ | $2^m$ |
| $2^{3m-1}$ | 1 |

*The dual code $\mathcal{C}^{(q)\perp}_{f,g,h}$ is a $[2^{3m-1}+1, 2^{3m-1}-3m, 3]$ binary linear code.*

# THE BENT CASE

If we consider the dual of the punctured code, we obtain a distance optimal code with respect to the sphere packing bound.

## THEOREM (F.)

*Let m be even, $f(x) = Tr_{2^m/2}(x)$, $g(y) = Tr_{2^m/2}(y^2)$ and $h(z) = B(z)$, a bent function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Then $\mathcal{C}_{f,g,h}^{*(2)}$ is a four-weights $[2^{3m-1}, 3m+1, 2^{3m-2} - 2^{\frac{5m-4}{2}}]$ binary linear code, with the following weight distribution*

| *Weight* | *Multiplicity* |
|---|---|
| *0* | *1* |
| $2^{3m-2} - 2^{\frac{5m-4}{2}}$ | $2^m$ |
| $2^{3m-2}$ | $2^{3m+1} - 2^{m+1} - 2$ |
| $2^{3m-2} + 2^{\frac{5m-4}{2}}$ | $2^m$ |
| $2^{3m-1}$ | *1* |

*The dual code $\mathcal{C}_{f,g,h}^{*(q)\perp}$ is a $[2^{3m-1}, 2^{3m-1} - 3m - 1, 4]$ binary linear code, which is distance optimal with respect to the sphere packing bound.*

# Application to the vectorial framework

We can propose the same construction with two vectorial function $f$ and $g$ from $\mathbb{F}_{q^m}$ to itself. Again, define a subset $\mathcal{D}$ of $\mathbb{F}_{q^m}^2$ as

$$\mathcal{D} = \left\{(x, y) \in \mathbb{F}_{q^m}^2 : f(x) + g(y) = 0\right\}$$

and a $3 \times (\#\mathcal{D})$ matrix $G^*_{f,g}$ over $\mathbb{F}_{q^m}$ as

$$G^*_{f,g} = \left(\begin{array}{c} 1 \\ x \\ y \end{array}\right)_{(x,y)\in\mathcal{D}} .$$

Then a $[\#\mathcal{D} + 1, 3]$ linear code $\mathcal{C}_{f,g}$ over $\mathbb{F}_{q^m}$ can be obtained with the generator matrix

$$G_{f,g} = \left(\begin{array}{cc} 0 & \\ 1 & G^*_{f,g} \\ 0 & \end{array}\right).$$

# Application to the vectorial framework

Let $\chi$ and $\chi'$ be the canonical additive character of $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$, respectively.

We define the following two character sums

$$\overline{\Phi}_{f,g} = \sum_{s \in \mathbb{F}_{q^m}^*} \sum_{x \in \mathbb{F}_{q^m}} \chi'(sf(x)) \sum_{y \in \mathbb{F}_{q^m}} \chi'(sg(y))$$

and

$$\overline{\Lambda}_{a,b,c}^{f,g} = \sum_{s \in \mathbb{F}_q^*} \chi(sa) \sum_{\omega \in \mathbb{F}_{q^m}^*} \sum_{(x,y) \in \mathbb{F}_{q^m}^2} \chi'(\omega f(x) + \omega g(y)) \chi'(sbx + scy),$$

for any $(a, b, c) \in \mathbb{F}_q \times \mathbb{F}_{q^m}^2$.

# The parameters of the codes

Let $\delta : \mathbb{F}_{q^m} \to \{0,1\}$ be a function such that $\delta(x) = 0$ if $\mathrm{Tr}_{q^m/q}(x) = 0$ and $\delta(x) = 1$ otherwise.

## Proposition (F.)

*The length of the code $\mathcal{C}_{f,g}^{(q)}$ is $n = 1 + q^m + \frac{1}{q^m}\overline{\Phi}_{f,g}$. Also, for any $(a,b,c) \in \mathbb{F}_q \times \mathbb{F}_{q^m}^2$, the weight of the codeword $\mathbf{c}_{a,b,c}$ is given by*

$$wt(\boldsymbol{c}_{a,b,c}) = \begin{cases} 0 & \text{if } a = b = c = 0, \\ q^m + \frac{1}{q^m}\overline{\Phi}_{f,g} & \text{if } a \neq 0 \text{ and } b = c = 0 \\ \delta(b) + q^{m-1}(q-1) + \frac{1}{q^{m+1}}\left[(q-1)\overline{\Phi_{f,g}} - \overline{\Lambda}_{a,b,c}^{f,g}\right] & \text{otherwise.} \end{cases}$$

## The parameters of the codes

Let $\delta : \mathbb{F}_{q^m} \to \{0,1\}$ be a function such that $\delta(x) = 0$ if $\mathrm{Tr}_{q^m/q}(x) = 0$ and $\delta(x) = 1$ otherwise.

### Proposition (F.)

*The length of the code $\mathcal{C}_{f,g}^{(q)}$ is $n = 1 + q^m + \frac{1}{q^m}\overline{\Phi}_{f,g}$. Also, for any $(a,b,c) \in \mathbb{F}_q \times \mathbb{F}_{q^m}^2$, the weight of the codeword $\mathbf{c}_{a,b,c}$ is given by*

$$wt(\mathbf{c}_{a,b,c}) = \begin{cases} 0 & \text{if } a = b = c = 0, \\ q^m + \frac{1}{q^m}\overline{\Phi}_{f,g} & \text{if } a \neq 0 \text{ and } b = c = 0 \\ \delta(b) + q^{m-1}(q-1) + \frac{1}{q^{m+1}}\left[(q-1)\overline{\Phi_{f,g}} - \overline{\Lambda}_{a,b,c}^{f,g}\right] & \text{otherwise.} \end{cases}$$

Hence, the length of the punctured code $\mathcal{C}_{f,g}^{*(q)}$ is equal to $q^m + \frac{1}{q^m}\overline{\Phi}_{f,g}$ and $\mathrm{wt}(\mathbf{c}_{a,b,c}^{*}) = \mathrm{wt}(\mathbf{c}_{a,b,c}) - \delta(b)$.

# APPLICATIONS TO SPECIFIC FUNCTIONS

If at least one function between $f$ and $g$ is a permutation polynomial, then $\overline{\Phi}_{f,g} = 0$, which means that the length of the codes is equal to $1 + q^m$.

For $q = 2$, it is interesting to notice that

$$\begin{aligned}\overline{\Lambda}_{a,b,c}^{f,g} &= (-1)^a \sum_{\omega \in \mathbb{F}_{q^m}^*} \sum_{(x,y) \in \mathbb{F}_{q^m}^2} \chi'(\omega f(x) + \omega g(y))\chi'(bx + cy) \\ &= (-1)^a \sum_{\omega \in \mathbb{F}_{q^m}^*} \sum_{x \in \mathbb{F}_{q^m}} \chi'(\omega f(x) + bx) \sum_{y \in \mathbb{F}_{q^m}} \chi'(\omega g(y) + cy) \\ &= (-1)^a \sum_{\omega \in \mathbb{F}_{q^m}^*} W_f(\omega, b) W_g(\omega, c).\end{aligned}$$

In the $s$-plateaued case, and especially in the almost-bent one, we can better estimate this sum (notice that there do not exist any bent functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$.

# NEXT DIRECTIONS

- Apply the construction of the code $\mathcal{C}_{f,g,h}$ to other families of $q$-ary functions, especially bent or almost bent.
- Increase the number of involved functions to more than three, if it leads to new optimal codes.
- Modify the defining set $\mathcal{D}$ in order to obtain new constructions of linear codes.
- Apply the construction of the code $\mathcal{C}_{f,g}$ to specific families of vectorial functions, especially almost-bent in the classes Niho and Gold.

# Next directions

- Apply the construction of the code $\mathcal{C}_{f,g,h}$ to other families of $q$-ary functions, especially bent or almost bent.
- Increase the number of involved functions to more than three, if it leads to new optimal codes.
- Modify the defining set $\mathcal{D}$ in order to obtain new constructions of linear codes.
- Apply the construction of the code $\mathcal{C}_{f,g}$ to specific families of vectorial functions, especially almost-bent in the classes Niho and Gold.

Thank you for your attention!