(Near) Constant Codes
and
(Almost) Perfect Nonlinear Functions

Valentin SUDER
(Université de Rouen Normandie)

OpeRa 2024
Caserta, February 14th, 2024

Outline

Rank-metric codes

Let $\mathcal{M}_{m,n}(\mathbb{F}_q)$ be the $\mathbb{F}_q$-vector space of $m \times n$ matrices ovec the finite field $\mathbb{F}_q$.

Rank-Metric Code

A **Rank-metric Code** is a subset $\mathcal{C} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$ with the **(rank-)distance** defined as

$$d(A, B) = rank(A - B), \qquad A, B \in \mathcal{M}_{m,n}(\mathbb{F}_q)$$

The **minimum distance** of the code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{d(A, B) \mid A, B \in \mathcal{C}\}$$

Singleton-like bound

Let $\mathcal{C} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$ with $d(\mathcal{C}) = d$, then

$$|\mathcal{C}| \leq q^{n(m-d+1)}.$$

A code for which there is equality is called a **Maximum Rank Distance** (MRD) code.

Rank-metric codewords as vectors

We can represent a codeword $c \in \mathcal{M}_{m,n}(\mathbb{F}_q)$ as a vector in $\mathbb{F}_{q^m}^n$.

Example: Let $q = 5$, $m = 3$, $n = 4$, and $\mathbb{F}_{5^3} = \mathbb{F}_5(z)$,

$$\begin{pmatrix} 2 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ -2 & 1 & 2 & 1 \end{pmatrix} \sim (2 - z - 2z^2,\ 1 + z^2,\ z + 2z^2,\ -1 + z^2)$$

Linear Codes

Let $\mathbb{G}$ be a subfield of $\mathbb{F}_{q^m}$.
The code $\mathcal{C} \subseteq \mathcal{M}_{m,n}(\mathbb{F}_q)$ is $\mathbb{G}$-linear if it can be seen as a $\mathbb{G}$-subspace of $\mathbb{F}_{q^m}^n$.
$\mathcal{C}$ can therefore be represented by its **generator matrix** in $\mathcal{M}_{k,n}(\mathbb{F}_{q^m})$.
k is called the **dimension** of the code.

Representing functions over $\mathbb{F}_{p^n}$

$F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

Univariate representation

$$F(x) = \sum_{i=0}^{p^n-1} f_i x^i, \qquad \mathbb{F}_{p^n}[x]$$

By identifying $\mathrm{Tr}(\cdot)$ with $< \cdot >$ we can rewrite F as a **vectorial function**:

Multivariate representation

$$\begin{array}{cccl} F : & \mathbb{F}_p^n & \to & \mathbb{F}_p^n \\ & x_1, \ldots, x_n & \mapsto & (F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n)) \end{array}$$

Differentiality

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$

Discrete derivatives

The **discrete derivative** in the direction $\alpha \in \mathbb{F}_p^n \backslash \{0\}$ is

$$\Delta_\alpha F(x) = F(x+\alpha) - F(x)$$

and the **differential uniformity** is

$$\delta_F = \max_{\alpha \neq 0, \beta \in \mathbb{F}_p^n} |\{x \in \mathbb{F}_p^n \mid \Delta_\alpha F(x) = \beta\}|.$$

- if $\delta_F = 1$ then F is said to be Perfectly Nonlinear (PN)
  ($\Delta_\alpha F$ for any $\alpha \in \mathbb{F}_p^n \backslash \{0\}$ is a bijection)
- if $\delta_F = 2$ then F is said to be Almost Perfectly Nonlinear (APN)

Algebraic degree of a function

Algebraic Degree

The (algebraic) **degree** of a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\deg(F)$, is either:

- the maximum of the p-weight of its exponents in the **univariate representation**
- the maximum multivariate degree of its coordinate functions in the **vectorial representation**

Note that $\deg(\Delta_\alpha F) < \deg(F)$.

Affine functions

$\deg(A) = 1$

Affine polynomials

$$A(x) = a + \sum_{i=0}^{n-1} a_i x^{p^i} \qquad \in \mathbb{F}_{p^n}[x]$$

Quadratic functions

$\deg(Q) = 2$

Dembowski-Ostrom (DO) Polynomials

$$Q(x) = \sum_{0 \le i \le j \le n-1} q_{i,j} x^{p^i + p^j} \qquad \in \mathbb{F}_{p^n}[x]$$

Outline

(Pre)Semifields

A (pre)semifield is a ring with no zero-divisors, left and right distributivity and (not necessarily) a multiplicative identity.

(Pre)Semifields

A (pre)semifield is a ring with no zero-divisors, left and right distributivity and (not necessarily) a multiplicative identity.

(Pre)Semifields and PN functions

The following concepts are equivalent:

- Commutative presemifields in odd characteristics
- Quadratic PN functions

R.S. Coulter and M. Henderson,
Commutative presemifields and semifields,
Adv. in Math. 217(1), 2008 .

(Pre)Semifields

A (pre)semifield is a ring with no zero-divisors, left and right distributivity and (not necessarily) a multiplicative identity.

(Pre)Semifields and PN functions [Coulter & Henderson]

The following concepts are equivalent:

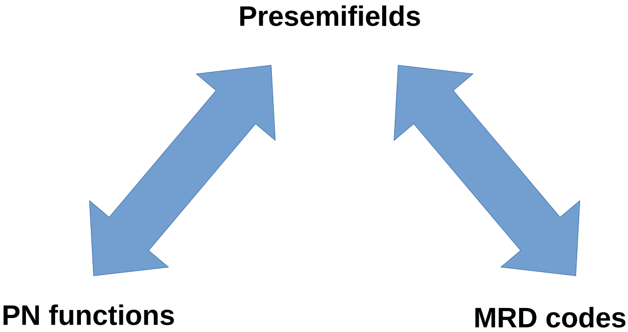
- Commutative presemifields in odd characteristics
- Quadratic PN functions

(Pre)Semifields and MRD Codes [de la Cruz et al.]

The following concepts are equivalent:

- Finite presemifields of dimension n over $\mathbb{F}_q$
- $\mathbb{F}_q$-linear MRD codes in $\mathcal{M}_{n,n}(\mathbb{F}_q)$ with minimum distance n

J. de la Cruz, M. Kiermaler, A. Wasserman and W. Willems,
Algebraic Structures of MRD Codes,
Adv. in Math. of Comm. 10(3), 2016.



What connects (A)PN functions and rank-metric codes?

What connects (A)PN functions and rank-metric codes?

A clue

For a **quadratic APN function** F over $\mathbb{F}_{2^n}$,
" it is easy to see that the function given by $\Delta_\alpha F(x) + \Delta_\alpha F(0)$ for each nonzero α can be viewed as a matrix M_α of rank $n-1$ in $\mathcal{M}_{n,n}(\mathbb{F}_{2^n})$. Furthermore, all M_α together with the zero matrix form a $\mathbb{F}_2$-linear code $\mathcal{C}$ in $\mathcal{M}_{n,n}(\mathbb{F}_{2^n})$ with $d(\mathcal{C}) = n-1$."

G. Lunardon, R. Trombetti and Y. Zhou,
On Kernels and Nuclei of Rank Metric Codes,
Journal of Alg. Comb. 46, 2017.

QAM – Quadratic APN Matrix

Y. Yu, M. Wang and Y. Li,
A Matrix approach for constructing quadratic APN functions,
DCC 73, 2014.

G. Weng, Y. Tan and G. Gong,
On Quadratic Almost Perfect Nonlinear Functions and their Related Algebraic Objects,
WCC, 2013.

Lemma

$F(x) \in \mathbb{F}_{2^n}$ is APN $\Leftrightarrow$ $\forall x, \Delta_{\alpha_0,\alpha_1} F(x) \neq 0$ for all $\alpha_0 \neq \alpha_1 \in \mathbb{F}_{2^n} \backslash \{0\}$

N.B.: $\Delta_{\alpha_0,\alpha_1} F(x) = \Delta_{\alpha_0}(\Delta_{\alpha_1} F(x)) = \Delta_{\alpha_1}(\Delta_{\alpha_0} F(x))$

If $Q(x) \in \mathbb{F}_{2^n}[x]$ is DO then:

- its derivatives are affine
- its second-order derivatives are constant

$$\Delta_{\alpha_0,\alpha_1} Q(x) = \Delta_{\alpha_1} Q(x+\alpha_0) + \Delta_{\alpha_1} Q(x) = \Delta_{\alpha_1} Q(\alpha_0) = \Delta_{\alpha_0} Q(\alpha_1)$$

QAM – Quadratic APN Matrix (II)

$\Delta_{\alpha_0,\alpha_1} Q(x) = \Delta_{\alpha_1} Q(\alpha_0)$

Let $\beta_1, \ldots, \beta_n \in \mathbb{F}_{2^n}$ be a basis over $\mathbb{F}_2$, and $Q(x) \in \mathbb{F}_{2^n}[x]$ be DO:

$$M_Q = \begin{pmatrix} \Delta_{\beta_1,\beta_1} Q & \Delta_{\beta_1,\beta_2} Q & \ldots & \Delta_{\beta_1,\beta_n} Q \\ \Delta_{\beta_2,\beta_1} Q & \ddots & & \\ \vdots & & & \vdots \\ \Delta_{\beta_n,\beta_1} Q & & \ldots & \Delta_{\beta_n,\beta_n} Q \end{pmatrix} = \begin{pmatrix} 0 & \Delta_{\beta_1,\beta_2} Q & \ldots & \Delta_{\beta_1,\beta_n} Q \\ \Delta_{\beta_1,\beta_2} Q & 0 & & \\ \vdots & & \ddots & \vdots \\ \Delta_{\beta_1,\beta_n} Q & & \ldots & 0 \end{pmatrix}$$

QAM – Quadratic APN Matrix (II)

$\Delta_{\alpha_0,\alpha_1} Q(x) = \Delta_{\alpha_1} Q(\alpha_0)$

Let $\beta_1, \ldots, \beta_n \in \mathbb{F}_{2^n}$ be a basis over $\mathbb{F}_2$, and $Q(x) \in \mathbb{F}_{2^n}[x]$ be DO:

$$M_Q = \begin{pmatrix} \Delta_{\beta_1,\beta_1} Q & \Delta_{\beta_1,\beta_2} Q & \ldots & \Delta_{\beta_1,\beta_n} Q \\ \Delta_{\beta_2,\beta_1} Q & \ddots & & \\ \vdots & & & \vdots \\ \Delta_{\beta_n,\beta_1} Q & & \ldots & \Delta_{\beta_n,\beta_n} Q \end{pmatrix} = \begin{pmatrix} 0 & \Delta_{\beta_1,\beta_2} Q & \ldots & \Delta_{\beta_1,\beta_n} Q \\ \Delta_{\beta_1,\beta_2} Q & 0 & & \\ \vdots & & \ddots & \vdots \\ \Delta_{\beta_1,\beta_n} Q & & \ldots & 0 \end{pmatrix}$$

$\Rightarrow$ M_Q is the **generator matrix** of a $\mathbb{F}_2$-linear code with minimum distance $n - \log_2(\delta_Q)$.
In particular, when Q is **APN**, the code is **constant rank** $n-1$.

Outline

Layers of the QAM

S. Ghosh and L. Perrin
Some Experimental Results on Quadratic APN Functions,
BFA, 2021.

$$M_Q = \begin{pmatrix} 0 & \Delta_{\beta_1,\beta_2} Q & \cdots & \Delta_{\beta_1,\beta_n} Q \\ \Delta_{\beta_1,\beta_2} Q & 0 & & \\ \vdots & & \ddots & \vdots \\ \Delta_{\beta_1,\beta_n} Q & & \cdots & 0 \end{pmatrix} \to \begin{pmatrix} 0 & \Delta_{\beta_1,\beta_2} Q_1 & \cdots & \Delta_{\beta_1,\beta_n} Q_1 \\ \Delta_{\beta_1,\beta_2} Q_1 & 0 & & \\ \vdots & & \ddots & \vdots \\ \Delta_{\beta_1,\beta_n} Q_1 & & \cdots & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & \Delta_{\beta_1,\beta_2} Q_2 & \cdots & \Delta_{\beta_1,\beta_n} Q_2 \\ \Delta_{\beta_1,\beta_2} Q_2 & 0 & & \\ \vdots & & \ddots & \vdots \\ \Delta_{\beta_1,\beta_n} Q_2 & & \cdots & 0 \end{pmatrix},$$

$$\cdots$$

Layers of the QAM (II)

$M_Q = [\Delta_{\beta_i,\beta_j} Q]_{i,j}$

M_Q gives another $\mathbb{F}_2$-linear code $\mathcal{L}$ for which the following codewords are the generators:

$$\left[\mathrm{Tr}(\beta_k \Delta_{\beta_i,\beta_j} Q)\right], \qquad \forall 1 \leq k \leq n.$$

Proposition

Let $Q : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be APN and consider its **layer code** $\mathcal{L}$:

- if n is **odd**, then $\mathcal{L}$ is constant rank $n-1$
- if n is **even**, then $\mathcal{L}$ is near constant rank $n, n-2$.

From an ex nihilo method

R.S. Selvaraj and J. Demamu,
Equidistant Rank metric codes: constructions and properties,
Communications in Informations and Systems 10(3), 2010.

Build the code $\mathcal{C}$ codeword by codeword as follow:

1. Choose 3 codewords that are equidistant to each other
2. Choose a 4th codewords, equidistant to the first 3 and their sum
3. Choose a 5th codewords, equidistant to any odd sum of the previous 4
4. $\vdots$

Proposition

$\mathcal{C}+\mathcal{C}=\{u+v \mid u,v\in\mathcal{C}\}$ is constant rank and $|\mathcal{C}+\mathcal{C}|<2|\mathcal{C}|$.

The Gabidulin example

Gabidulin Code (A reminder)

Let $a_1, \ldots, a_n \in \mathbb{F}_q^m$ be $\mathbb{F}_q$-linearly independent.
The **Gabidulin code** of dimension $1 \leq k \leq n$ is the $\mathbb{F}_{q^m}$-linear code defined by the generator matrix:

$$\begin{pmatrix} a_1 & \ldots & a_n \\ a_1^q & \ldots & a_n^q \\ \vdots & & \vdots \\ a_1^{q^k} & \ldots & a_n^{q^k} \end{pmatrix}$$

The Gabidulin example

Gabidulin Code (A reminder)

Let $a_1, \ldots, a_n \in \mathbb{F}_q^m$ be $\mathbb{F}_q$-linearly independent.
The **Gabidulin code** of dimension $1 \leq k \leq n$ is the $\mathbb{F}_{q^m}$-linear code defined by the generator matrix:

$$\begin{pmatrix} a_1 & \ldots & a_n \\ a_1^q & \ldots & a_n^q \\ \vdots & & \vdots \\ a_1^{q^k} & \ldots & a_n^{q^k} \end{pmatrix}$$

It is easy to see that the function x^2 over $\mathbb{F}_{p^n}$ (which is always PN) is equivalent to the Gabidulin code of dimension 1.

Outline

Conclusion

- Is there a gap in the litterature? (why? or why not?)
- Are there other ways to construct (near) constant rank codes ?
- What happens to generalizations of (A)PN functions?
- What happens when $m \neq n$?
- $\vdots$