THE NON-GAP SEQUENCE OF A SUBCODE OF A GENERALIZED REED-SOLOMON CODE

I. MÁRQUEZ-CORBELLA [1] E. MARTÍNEZ-MORO [2] R. PELLIKAAN [3]

[1] Department of Algebra, Geometry and Topology, University of Valladolid.
Supported by a FPU grant AP2008-01598 by Spanish MEC.

[2] Department of Applied Mathematics, University of Valladolid.

[3] Department of Mathematics and Computing Science, Eindhoven University of Technology.

Seventh International Workshop on Coding and Cryptography 2011

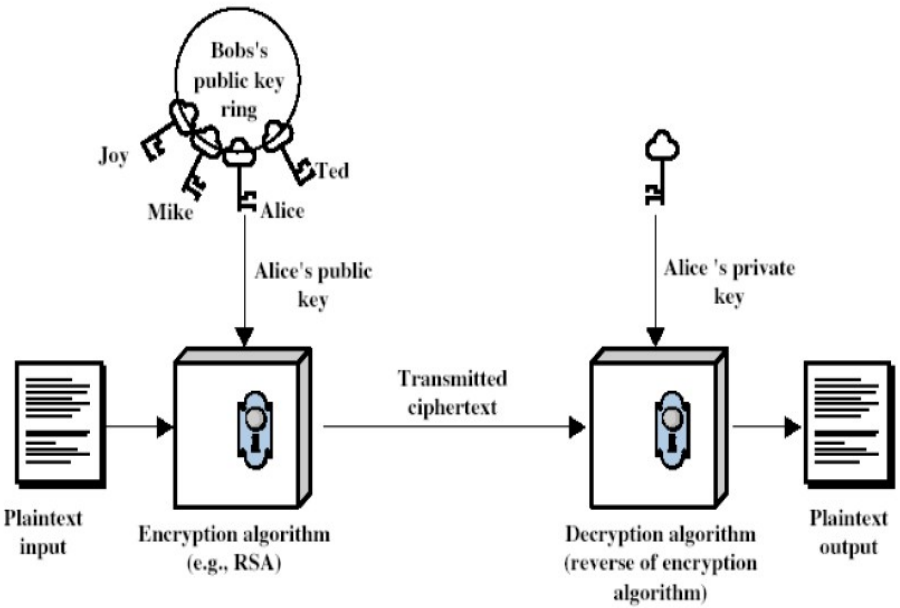
PUBLIC-KEY CRYPTOSYSTEMS

TWO KEYS:

- Private Key: Known only by the recipient.
- Public Key: Available to anyone.

MOST PKC ARE BASED ON NUMBER-THEORETIC PROBLEMS

➜ Quatum computers will break the most popular PKCs.



McEliece cryptosystem

Key Generation

1. Given:
   - $\mathcal{C}$ an $[n, k, d]$ linear code over $\mathbb{F}_q$
   - $G \in \mathbb{F}_q^{k \times n}$ a generator matrix of $\mathcal{C}$.
   - $S \in \mathbb{F}_q^{k \times k}$ a nonsingular matrix.
   - $P \in \mathbb{F}_q^{n \times n}$ a permutation matrix.
2. McEliece Public Key : $(G' = SGP, t)$.
3. McEliece Private Key: (G, S, P)

Encryption

Encrypt a message $\mathbf{m} \in \mathbb{F}_q^k$ as

$$\mathbf{y}' = \mathbf{m}G' + \mathbf{e}'$$

where $\mathbf{e} \in \mathbb{F}_q^n$ is a random error vector of weight $\leq t$.

Decryption

1. Compute $\mathbf{y} = \mathbf{y}'P^{-1} = \mathbf{m}G'P^{-1} + \mathbf{e}P^{-1} = \mathbf{m}SG + \mathbf{e}$.
2. Apply the decoding algorithm for $\mathcal{C}$ to find $\mathbf{m}S$.
3. $\mathbf{m} = \mathbf{m}SS^{-1}$.

- McEliece introduced the first PKC based on Error-Correcting Codes in 1978.
- Advantages:
  1. Interesting candidate for post-quantum cryptography.
  2. Fast encryption (matrix-vector multiplication) and decryption functions.
- Drawback: Large key size.

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

MOTIVATION

- Niederreiter in [**?**] presents a dual version of McEliece cryptosystem which is equivalent in terms of security.
  - ➜ He proposed the class of GRS codes over $\mathbb{F}_{2^m}$.
- Sidelnikov and Shestakov in [**?**] introduced an algorithm to break the initial Niederreiter scheme.
- Berger and Loidreau in [**?**] propose another version of the Niederreiter scheme designed to resist the Sidelnikov-Shestakov attack.
  - ➜ Main idea: work with subcodes of the original GRS code.

T. Berger and P. Loidreau.

How to mask the structure of codes for a cryptographic use.

Designs, Codes and Cryptography, 35: 63–79, 2005.

H. Niederreiter.

Knapsack-type crypto systems and algebraic coding theory.

Problems of Control and Information Theory, 15(2):159–166, 1986.

V. M. Sidelnikov and S. O. Shestakov.

On the insecurity of cryptosystems based on generalized Reed-Solomon codes.

Discrete Math. Appl., 2:439–444, 1992.

MOTIVATION

- In [**?**] Wieschebrink presents the first feasible attack to the Berger-Loidreau cryptosystem but is impractical for small subcodes.
- In [**?**] Wieschebrink notes that if the double code of a subcode of a GRS code is itself a GRS code of dimension $2k - 1$ then we can apply the Sidenikov-Shestakov attack.

MAIN TASK OF THIS PAPER

Confirm the previous question and give a characterization of the possible parameters that should be used to avoid attacks on the Berger-Loidreau cryptosystem.

C. Wieschebrink.

An attack on the modified Niederreiter encryption scheme.

In PKC 2006, Lecture Notes in Computer Science, volume 3958, 14–26, Berlin, 2006. Springer.

C. Wieschebrink.

Cryptoanalysis of the Niederreiter public key scheme based on GRS subcodes.

In Post-Quantum Cryptography, Lecture Notes in Computer Science, volume 6061, 6–72, Berlin, 2010. Springer.

NOTATION

Let :

- $\mathbb{F}_q$ be a finite field with q elements.
- $n, k, l \in \mathbb{N} \ : \ 1 \leq l \leq k \leq n \leq q$.
- $L_k := \{f \in \mathbb{F}_q[X] \ : \deg(f(X)) \leq k-1\}$.
- $\mathrm{ev}_{\mathbf{a},\mathbf{b}}$ be the evaluation map at the elements $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ i.e.

$$\begin{array}{rccc} \mathrm{ev}_{\mathbf{a},\mathbf{b}} : & L_k & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(a_1)b_1, \ldots, f(a_n)b_n) \end{array}$$

GENERALIZED REED-SOLOMON CODES (OR GRS CODES)

Let $\mathbf{a} \in \mathbb{F}_q^n$ such that $a_i \neq a_j$ for $1 \leq i < j \leq n$ and $\mathbf{b} \in \mathbb{F}_q^n$ with non-zero entries. The **GRS** code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is defined by:

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) := \left\{\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \ : \ f \in L_k\right\}$$

We define the star product $\mathbf{a} * \mathbf{b} \in \mathbb{F}_q^n$ by $\mathbf{a} * \mathbf{b} = (a_1 \cdot b_1, \ldots, a_n \cdot b_n)$.

REMARK

- ➜ $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) = \mathbf{b} * \mathrm{GRS}_k(\mathbf{a}, \mathbf{1})$.
- ➜ $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)g(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{1}}(f(X)) * \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g(X))$.

$(\mathbf{a}, \mathbf{b})$-GAP OF A CODE

Let $\mathcal{C}$ be an l-dimensional subcode of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, we denote by

$$\mathcal{C}_i := \mathcal{C} \cap \mathrm{GRS}_i(\mathbf{a}, \mathbf{b}).$$

Then $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \ldots \subseteq \mathcal{C}_k = \mathcal{C} \cap \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) = \mathcal{C}$.

$(\mathbf{a}, \mathbf{b})$-GAP OF THE CODE

$i \in \mathbb{Z}_{\geq 0}$ is called an **$(\mathbf{a}, \mathbf{b})$-gap** of the code $\mathcal{C}$ if $\mathcal{C}_i = \mathcal{C}_{i+1}$.
We define the **associated $(\mathbf{a}, \mathbf{b})$ non-gap** of the code $\mathcal{C}$ sequence of $\mathcal{C}$ by

$$\mathcal{I}(\mathbf{a}, \mathbf{b}, \mathcal{C}) = \mathcal{I}(\mathcal{C}) = \left\{ i \in \mathbb{Z}_{\geq 0} \ : \ i \text{ is a non-gap of } \mathcal{C} \right\}$$

PROPOSITION 1

$i \in \mathbb{Z}_{\geq 0}$ is an $(\mathbf{a}, \mathbf{b})$ non-gap of $\mathcal{C}$ $\iff$ $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$ such that $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \in \mathcal{C}$

COROLLARY 1

Let $\mathcal{C}$ be an l-dimensional subcode of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with associated non-gap sequence $\mathcal{I}(\mathcal{C})$. Then:

1. $\mathcal{I}(\mathcal{C}) = \left\{ i \mid \exists f \in \mathbb{F}_q[X] \text{ with } \deg(f(X)) = i < k \ : \ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \in \mathcal{C} \right\}$
2. $\mathcal{C} = \left\{ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \mid f = 0 \text{ or } f \in \mathbb{F}_q[X] \text{ and } \deg(f(x)) \in \mathcal{I}(\mathcal{C}) \right\}$

$(\mathbf{a}, \mathbf{b})$-GAP OF A CODE

We can obtain a basis of $\mathcal{C}$ just studying the associated $(\mathbf{a}, \mathbf{b})$ non-gap sequence of $\mathcal{C}$.

PROPOSITION 2

There is a set $\mathcal{I} = \{i_1, \ldots, i_l\}$ and there are l polynomials in unique normal form

$$f_j(X) = X^{i_j} + \sum_{\substack{s<i_j \\ s\notin\mathcal{I}}} f_{j,s}X^s \in \mathbb{F}_q[X], \text{ for all } j = 1, \ldots, l,$$

such that $\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_j(X)) \text{ with } j = 1, \ldots, l\rangle$.
Furthermore $\mathcal{I}(\mathcal{C}) = \mathcal{I}$ and $\dim(\mathcal{C}) = |\mathcal{I}(\mathcal{C})|$.

PROPOSITION 3

Let $\mathcal{I} = \{i_1, \ldots, i_l\}$ and

$$e(\mathcal{I}) = i_1 l + (i_2 - i_1 - 1)(l-1) + \cdots + (i_l - i_{l-1} - 1) = \sum_{s=1}^{l}(i_s - i_{s-1} - 1)(l - s + 1)$$

where $i_0 = -1$. Then the number of l-dimensional subcodes of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ over $\mathbb{F}_q$ with a given non-gap sequence $\mathcal{I}$ is equal to $q^{e(\mathcal{I})}$.

$(\mathbf{a}, \mathbf{b})$-GAP OF A CODE

REMARK

- $e(\mathcal{I})$ is minimal and equal to 0 for $\mathcal{I} = \{0, 1, \ldots, l-1\}$.
- $e(\mathcal{I})$ is maximal and equal to $l(k-l)$ for $\mathcal{I} = \{k-l, \ldots, k-1\}$.

➜ The number of l-dimensional subcodes of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ over $\mathbb{F}_q$ is equal to the Gaussian binomial:

$$\frac{(q^k-1)(q^k-q)\cdots(q^k-q^{l-1})}{(q^l-1)(q^l-q)\cdots(q^l-q^{l-1})} := \begin{bmatrix} k \\ l \end{bmatrix}_q = \sum_{\substack{\mathcal{I}\subseteq\{0,\ldots,k-1\} \\ |\mathcal{I}|=l}} q^{e(\mathcal{I})}.$$

➜ This number is polynomial in q with non-negative integers as coefficients.

GRS SUBCODES OF GRS CODES I

We study the l-dimensional subcodes $\mathcal{C}$ of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ that are themselves GRS codes.

1. $\mathcal{C} = \mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$ with $2 \leq l \leq k$.

PROPOSITION 4

$$\mathcal{C} = \mathrm{GRS}_l(\mathbf{a}, \mathbf{b}) \iff \mathcal{I}(\mathcal{C}) = \{0, \ldots, l-1\}$$

There is exactly **ONE** l-dimensional subcode $\mathcal{C}$ with $\mathcal{I}(\mathcal{C}) = \{0, \ldots, l-1\}$ which is $\mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$.

2. $\mathcal{C} = \mathrm{GRS}_l(\mathbf{a}, \mathbf{a}^i * b)$ with $i + l \leq k$.

PROPOSITION 5

Let $\mathcal{I}(\mathcal{C}) = \{i_1, \ldots, i_l\}$ and $\mathbf{c} = \mathrm{ev}_{\mathbf{a}}(f(X))$ with $f \in \mathbb{F}_q[X]$ and $\deg(f(X)) = i$. If $i + i_l < k$ then $\mathcal{I}(c * \mathcal{C}) = i + \mathcal{I}(\mathcal{C})$.

Note that the converse is not true in general.

COROLLARY 3

If $i + l \leq k$ then $\mathcal{I}(\mathrm{GRS}_l(\mathbf{a}, \mathbf{a}^i * \mathbf{b})) = \{i, i+1, \ldots, i+l-1\}$.

GRS SUBCODES OF GRS CODES II

3. $\mathcal{C} = \mathrm{GRS}_l(\mathbf{c}, \mathbf{d})$.

PROPOSITION 6

Let $l \geq 2$, $g_0, h_1 \in \mathbb{F}_q[X]$, $\mathbf{a} \in \mathbb{F}_q^n : a_i \neq a_j$ with $1 \leq i < j \leq n$, $d_0 = \deg(g_0(X))$, $\mathbf{b} \in \mathbb{F}_q^n : b_i \neq 0$ with $1 \leq i \leq n$, $d_1 = d_0 + \deg(h_1(X))$

If
1. $\mathrm{ev}_{\mathbf{a}}(h_1(X)) = \mathbf{c} : c_i \neq c_j$ with $1 \leq i < j \leq n$,
2. $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X)) = \mathbf{d} : d_i \neq 0$ with $1 \leq i \leq n$,
3. $d_0 < d_1$
4. $d_0 + (l-1)(d_1 - d_0) < k$.

Then the code $\mathcal{C} = \mathrm{GRS}_l(\mathbf{c}, \mathbf{d})$ is an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with :

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{d_0, d_1, \ldots, d_0 + j(d_1 - d_0), \ldots, d_0 + (l-1)(d_1 - d_0)\}$$

PROPOSITION 7

Assume that $\mathcal{C} = \mathrm{GRS}_l(\mathbf{c}, \mathbf{d}) \subseteq \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$. And let $d_0 < d_1$ be the first two elements of $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$. Then $\exists g_0, h_1 \in \mathbb{F}_q[X]$ such that:

1. $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X)) = \mathbf{d}$.
2. $\mathrm{ev}_{\mathbf{a}}(h_1(X)) = \mathbf{c}$.
3. $d_0 = \deg(g_0(X))$.
4. $d_1 = d_0 + \deg(h_1(X))$.

GRS SUBCODES OF GRS CODES III

COROLLARY 5

If $2k - 2 < n$ and $2 \leq l \leq k$. Then the number of l-dimensional subcodes of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ over $\mathbb{F}_q$ that are GRS code is at most q^{k-l+3}.

The probability that an arbitrary l-dimensional subcode of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is a GRS code is at most

$$\frac{q^{k-l+3}}{\begin{bmatrix} k \\ l \end{bmatrix}_q} \leq \frac{q^{k-l+3}}{q^{l(k-l)}} = q^{-(l-1)(k-l)+3}$$

This fraction tends to zero for $k \to \infty$ or $(k - l) \to \infty$.

THE SQUARE OF A CODE

THE SQUARE CODE

The square code of a $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ denoted by $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$ is the code generated by the set

$$\{\mathbf{r}_i * \mathbf{r}_j \ : \ 1 \leq i \leq j \leq k\}$$

where $\mathbf{r}_1, \ldots, \mathbf{r}_k$ denotes the rows of a generator matrix of $\mathcal{C}$.

Let:

- $\mathcal{C}$ be an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$.
- $\mathbf{r}_1, \ldots, \mathbf{r}_l$ be the rows of a generator matrix of $\mathcal{C}$.
- $f_1, \ldots, f_l$ be the polynomials associated to those rows.

Then

$$\mathbf{r}_i * \mathbf{r}_j = \left(b_1^2 f_i(a_1) f_j(a_1), \ldots, b_n^2 f_i(a_n) f_j(a_n)\right) = \mathrm{ev}_{\mathbf{a}, \mathbf{b}*\mathbf{b}}(f_i(X) f_j(X))$$

and $\deg(f_i(X) f_j(X)) = \deg(f_i(X)) + \deg(f_j(X)) \leq 2k - 2$ for $1 \leq i \leq j \leq l$
Thus the code $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \langle \mathbf{r}_i * \mathbf{r}_j \ : \ 1 \leq i \leq j \leq l \rangle$ is a subcode of the code $\mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

REMARK

The code $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \langle \mathbf{r}_i * \mathbf{r}_j \ : \ 1 \leq i \leq j \leq l \rangle$ is a subcode of the code $\mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

$(\mathbf{a}, \mathbf{b} * \mathbf{b})$ GAP OF $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$

We denote by $\mathcal{D}_i = \mathcal{D} \cap \mathrm{GRS}_i(\mathbf{a}, \mathbf{b} * \mathbf{b})$.
Then:

- $i \in \mathbb{Z}_{\geq 0}$ is an $(\mathbf{a}, \mathbf{b} * \mathbf{b})$ gap of $\mathcal{D}$ if $\mathcal{D}_i = \mathcal{D}_{i+1}$.
- $\mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}) = \{j \in \mathbb{Z}_{\geq 0} \ : \ j \text{ is an } (\mathbf{a}, \mathbf{b} * \mathbf{b})\text{-non gap of } \mathcal{D}\}$ is the $(\mathbf{a}, \mathbf{b} * \mathbf{b})$ non-gap sequence associated to the square code.

REMARK

$$j \in \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}) \iff \exists g \in \mathbb{F}_q[X] \text{ with } \deg(g(X)) = j \ : \mathrm{ev}_{\mathbf{a}, \mathbf{b}*\mathbf{b}}(g(X)) \in \mathcal{D}$$

PROPOSITION 8

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) + \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i + j \ : \ i, j \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})\} \subseteq \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b})$$

Furthermore:

1. If $0 \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b})$
2. Let $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$ with $i_1 + i_l < 2k - 1$ and $\mathbf{c} = \mathrm{ev}_{\mathbf{a}, \mathbf{b}}(f(X)) \in \mathcal{C}$ for $f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i_1$ then

$$\mathcal{I}(\mathbf{c} * \mathcal{C}, \mathbf{a}, \mathbf{b}) = i_1 + \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \mathcal{J}(\mathcal{D}).$$

PROPOSITION 9

$$\dim(\mathcal{D}) \leq \min\left\{2k-1, \binom{l+1}{2}\right\}$$

Furthermore:

1. If $\mathcal{D} = \mathrm{GRS}_r(\mathbf{a}, \mathbf{b} * \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \left\{0, \ldots, \lfloor \frac{r-1}{2} \rfloor\right\}$.
2. If $\mathcal{D} = \mathrm{GRS}_r(\mathbf{a}, \mathbf{a}^i * \mathbf{b} * \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \left\{\lfloor \frac{i}{2} \rfloor, \ldots, \lfloor \frac{i+r-1}{2} \rfloor\right\}$.
3. If $\mathcal{D} = \mathrm{GRS}_r(\mathbf{a}, \mathbf{a}^i * \mathbf{b} * \mathbf{b})$ then $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \left\{\lfloor \frac{d_0}{2} \rfloor, \ldots, \lfloor \frac{d_0+(r-1)(d_1-d_0)}{2} \rfloor\right\}$ where $d_0 < d_1$ and $d_0 + (r-1)(d_1 - d_0) < 2k - 1$

THE SQUARE CODE OF A GRS CODE

Let $\mathcal{C}$ be a GRS code then:

PROPOSITION 10

$$\langle \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) * \mathrm{GRS}_l(\mathbf{a}, \mathbf{c}) \rangle = \mathrm{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c})$$

In particular $\mathrm{GRS}_{2l-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ is the square code of $\mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$.

COROLLARY 6

If $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{0, \ldots, l-1\}$ then $\mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}) = \{0, \ldots, 2l-2\}$ i.e. $\mathcal{D} = \mathrm{GRS}_{2l-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

The converse is NOT true in general

When $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$?

Proposition 11

Let $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$. If $\mathcal{D} = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$, then

$$|\{ (u, v) \ : \ i_u + i_v \geq t \text{ and } 1 \leq u \leq v \leq l \}| \geq 2k - t - 1$$

for all $t = 0, \ldots, 2k - 2$.

Remark

Let $\mathcal{C}$ be an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$. If $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ then:

1. $2k - 1 \leq \binom{l+1}{2}$ (Particular case $t = 0$ of Proposition 11).
2. $i_l = k - 1$ (Case $t = 2k - 2$ of Proposition 11).
3. $i_{l-1} = k - 2$ (Case $t = 2k - 3$ of Proposition 11).
4. $i_{l-2} \geq k - 4$ (Case $t = 2k - 5$ of Proposition 11).

Remark

$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{k - l, \ldots, k - 1\}$ satisfies the conditions of Proposition 11 for all t. However this not imply that $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$ is exactly $\mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

Generator matrix of $\mathcal{D}$

Assume that we have two polynomials $f(X), g(X) \in L_k$, i.e. :

$$f(X) = \sum_{r=0}^{k-1} f_r X^r \quad \text{and} \quad g(X) = \sum_{s=0}^{k-1} g_s X^s$$

with $f_r, g_s \in \mathbb{F}_q$ for $r, s \in \{0, \ldots, k-1\}$.
Then:

$$f(X)g(X) = h(X) = h_0 + h_1 X + \ldots + h_{2k-2} X^{2k-2} \in L_{2k-2}.$$

This can be expressed in matrix form as follows:

$$R(f)S(g)^T = \begin{pmatrix} h_{2k-2} \\ h_{2k-3} \\ \vdots \\ h_{k-1} \\ \vdots \\ h_0 \end{pmatrix},$$

where

$$R(f) = \begin{pmatrix} f_0 & f_1 & \cdots & f_{k-1} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & f_0 & \cdots & f_{k-2} & f_{k-1} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f_0 & f_1 & \cdots & f_{k-1} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & f_0 & f_1 & \cdots & f_{k-1} \end{pmatrix} \in \mathbb{F}_q^{(2k-1)\times(3k-2)}$$

and

$$S(g) = (\underbrace{0 \quad \cdots \quad 0}_{k-1} \quad g_{k-1} \quad \cdots \quad g_0 \quad \underbrace{0 \quad \cdots \quad 0}_{k-1}) \in \mathbb{F}_q^{1\times(3k-2)}.$$

Generator matrix of $\mathcal{D}$

Let $\mathcal{C}$ be an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$.
By Proposition 2 there are l polynomials in normal form

$$f_j(X) = \sum_{s=0}^{i_j - 1} f_{j,s} X^s + X^{i_j} \text{ for } j = 1, \ldots, l.$$

such that

$$\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_i(X)) \text{ with } i \in \{1, \ldots, l\} \rangle.$$

Then the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X) f_v(X))$ with $1 \leq u \leq v \leq l$ generate the square code $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$.
Let us denote by

$$f_u(X) f_v(X) = g_{uv}(X) = g_{uv0} + g_{uv1} X + \cdots + g_{uv(2k-2)} X^{2k-2} \in L_{2k-1}$$

with $1 \leq u \leq v \leq l$.
Then the following matrix is a generator matrix of $\mathcal{D}$.

$$G_{\mathcal{D}} = \begin{pmatrix} g_{11(2k-2)} & \cdots & g_{1l(2k-2)} & g_{22(2k-2)} & \cdots & g_{2l(2k-2)} & \cdots & g_{ll(2k-2)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ g_{110} & \cdots & g_{1l0} & g_{220} & \cdots & g_{2l0} & \cdots & g_{ll0} \end{pmatrix}$$

$G_{\mathcal{D}}$ is a matrix of size $(2k-1) \times \binom{l+1}{2}$ over $\mathbb{F}_q$.

GENERATOR MATRIX OF $\mathcal{D}$

If we define

$$R = (\underbrace{R(f_1), \ldots, R(f_1)}_{l}, \underbrace{R(f_2), \ldots, R(f_2)}_{l-1}, \ldots, R(f_l)) \in \mathbb{F}_q^{(2k-1)\times\binom{l+1}{2}(3k-2)},$$

$$S(f_1, \ldots, f_l) = \begin{pmatrix} S(f_1) & 0 & 0 & \cdots & 0 \\ 0 & S(f_2) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & S(f_l) \end{pmatrix} \in \mathbb{F}_q^{l\times l(3k-2)}.$$

and

$$S = \begin{pmatrix} S(f_1, \ldots, f_l) & 0 & 0 & \cdots & 0 \\ 0 & S(f_2, \ldots, f_l) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & S(f_l) \end{pmatrix} \in \mathbb{F}_q^{\binom{l+1}{2}\times\binom{l+1}{2}(3k-2)}.$$

Then $RS^T = G_{\mathcal{D}}$.

NECESSARY CONDITIONS TO HAVE:

$$\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$$

FINAL REMARK

The following properties are necessary conditions to have that $\mathcal{D} = \langle \mathcal{C} * \mathcal{C} \rangle$ is the code $\mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$.

1. $\mathcal{I}(\mathcal{C}) = \{i_1, \ldots, i_l\} \subseteq \{0, \ldots, k-1\}$.
2. $i_l = k-1$, $i_{l-1} = k-2$ and $i_{l-2} \geq k-4$.
3. The matrix $G_{\mathcal{D}}$ has full rank, i.e. $\mathrm{rank}(R(f_1), \ldots, R(f_l)) = 2k-1$.

Thank for your attention

PROPOSITION 1

PROPOSITION 1

$i \in \mathbb{Z}_{\geq 0}$ is an $(\mathbf{a}, \mathbf{b})$ non-gap of $\mathcal{C}$ $\iff$ $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$ such that $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X)) \in \mathcal{C}$

$\Rightarrow$ Suppose that $i \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$ then by definition $\mathcal{C}_i \neq \mathcal{C}_{i+1}$. That is

$$\exists \mathbf{c} \in \mathcal{C}_{i+1} \setminus \mathcal{C}_i \Rightarrow \begin{cases} \mathbf{c} \in \mathcal{C} \\ \mathbf{c} \in \mathrm{GRS}_{i+1}(\mathbf{a}, \mathbf{b}) \setminus \mathrm{GRS}_i(\mathbf{a}, \mathbf{b}) \end{cases}$$

i.e. there exists a unique polynomial $f \in L_{i+1}$: $\mathbf{c} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X))$
But if $\deg(f(X)) < i$ then $\mathbf{c} \in \mathcal{C}_i$, thus $\deg(f(X)) = i$.

$\Leftarrow$ If $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) = i$ such that $\mathbf{c} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X))$ then $\mathbf{c} \in \mathcal{C}_{i+1} \setminus \mathcal{C}_i$.
Hence $i \in \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$.

PROPOSITION 2

- By Corollary 1, $\forall \mathbf{c} \in \mathcal{C}$, $\exists f \in \mathbb{F}_q[X]$ with $\deg(f(X)) \in \mathcal{I}(\mathcal{C})$: $\mathbf{c} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X))$.
- Furthermore the code $\mathcal{C}$ has dimension l,
  i.e. $\exists f_1, \ldots, f_l \in \mathbb{F}_q[X]$ with $\deg(f_i(X)) \in \mathcal{I}())$ for $i \in \{1, \ldots, l\}$ such that

$$\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_i(X)) \text{ with } i \in \{1, \ldots, l\} \rangle.$$

To make the notation easier we can assume that:

1. $\deg(f_j(X)) = i_j$ for $j \in \{1, \ldots, l\}$.
2. $\deg(f_1(X)) \leq \ldots \leq \deg(f_l(X))$, i.e. $\mathcal{I} = \{i_1, \ldots, i_l\}$.
3. The polynomials $f_1, \ldots, f_l$ are monics.

Thus each polynomial f_j can be written as

$$f_j(X) = \sum_{s=0}^{i_j - 1} f_{j,s} X^s + X^{i_j} \text{ for } j = 1, \ldots, l.$$

Let us define the matrix $M(f_1, \ldots, f_l) = (f_{j,s}) \in \mathbb{F}_q^{l \times k}$ as the matrix whose i-th row represent the coefficients with respect to the monomials $\{1, X, \ldots, X^{k-1}\}$ of the polynomial f_j for $j \in \{1, \ldots, l\}$. After applying Gaussian elimination on the previous matrix we obtain a matrix with the following form:

$$\begin{pmatrix} *_{1,0} & \cdots & *_{1,i_1-1} & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ *_{2,0} & \cdots & *_{2,i_1-1} & 0 & *_{2,i_1+1} & \cdots & *_{2,i_2-1} & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ *_{l,0} & \cdots & *_{l,i_1-1} & 0 & *_{l,i_1+1} & \cdots & *_{l,i_2-1} & 0 & \cdots & 0 \end{pmatrix}. \quad (1)$$

From the above matrix we can conclude the result of the Theorem.

PROPOSITION 3

Let $\mathcal{C}$ be an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with non-gap sequence $\mathcal{I}(\mathcal{C}) = \{i_1, \ldots, i_l\}$.
By Proposition 2 there are l polynomials in normal form

$$f_j(X) = \sum_{s=0}^{i_j - 1} f_{j,s} X^s + X^{i_j} \text{ for } j = 1, \ldots, l.$$

such that

$$\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_i(X)) \text{ with } i \in \{1, \ldots, l\} \rangle.$$

If we fix the set $\mathcal{I}$ there are $q^{e(\mathcal{I})}$ l-dimensional subcodes of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with associated non-gap sequence $\mathcal{I}$.

$$\begin{pmatrix}
*_{1,0} & \cdots & *_{1,i_1-1} & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
*_{2,0} & \cdots & *_{2,i_1-1} & 0 & *_{2,i_1+1} & \cdots & *_{2,i_2-1} & 1 & \cdots & 0 \\
\vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
*_{l,0} & \cdots & *_{l,i_1-1} & 0 & *_{l,i_1+1} & \cdots & *_{l,i_2-1} & 0 & \cdots & 0
\end{pmatrix}.$$

Note that $e(\mathcal{I})$ is equal to the number of elements of the matrix $M(f_1, \ldots, f_l)$ which are free to be chosen in $\mathbb{F}_q$ as long as the form of M is not changed.

PROPOSITION 4

$\Rightarrow$ If $\mathcal{C} = \mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$ by definition $\mathcal{I}(\mathcal{C}) = \{0, \ldots, l-1\}$

$\Leftarrow$ Suppose that the associated non-gap sequence of $\mathcal{C}$ is $\mathcal{I}(\mathcal{C}) = \{0, \ldots, l-1\}$ i.e. by Proposition 2 $\left\{\mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^i) \text{ with } i \in \{0, \ldots, l-1\}\right\}$ form a basis of $\mathcal{C}$ which is also a basis of $\mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$.
Thus $\mathcal{C} = \mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$.

REMARK

If $\mathcal{I} = \{0, \ldots, l-1\}$ then $e(\mathcal{I}) = 0$, thus there exists exactly **ONE** l-dimensional subcode $\mathcal{C}$ of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}) = \{0, \ldots, l-1\}$.
And by Proposition 4 we have that $\mathcal{C} = \mathrm{GRS}_l(\mathbf{a}, \mathbf{b})$.

PROPOSITION 5

Suppose that $\mathcal{I}(\mathcal{C}) = \{i_1, \ldots, i_l\}$, then there are l polynomials in normal form

$$f_j(X) = \sum_{s=0}^{i_j - 1} f_{j,s} X^s + X^{i_j} \text{ for } j = 1, \ldots, l.$$

such that

$$\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_i(X)) \text{ with } i \in \{1, \ldots, l\} \rangle.$$

Since $\mathbf{c} = \mathrm{ev}_{\mathbf{a}}(fX))$ with $f \in \mathbb{F}_q[X]$ and $\deg(f(X)) = i$. Then:

$$\mathbf{c} * \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_j(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X) f_j(X))$$

with $\deg(f(X) f_j(X)) = i + i_j \leq i + i_l < k$ for all $j \in \{1, \ldots, l\}$.

Hence

$$\mathbf{c} * \mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f(X) f_j(X)) \text{ with } j \in \{1, \ldots, l\} \rangle \subseteq \mathrm{GRS}_{i+i_l+1}(\mathbf{a}, \mathbf{b})$$

That is $\{i + i_1, \ldots, i + i_l\} = i + \mathcal{I}(\mathcal{C}) \subseteq \mathcal{I}(\mathbf{c} * \mathcal{C})$.
Since $\mathbf{c} * \mathcal{C}$ has dimension l then $|\mathcal{I}(\mathbf{c} * \mathcal{C})| = l$, thus

$$\mathcal{I}(\mathbf{c} * \mathcal{C}) = i + \mathcal{I}(\mathcal{C}).$$

PROPOSITION 6

Let us define $g_j(X) = g_0(X)\,(h_1(X))^j$ with $j \in \{0, \ldots, l-1\}$.

Then $0 \leq \deg(g_j(X)) = d_0 + j(d_1 - d_0) < k$ for all $j \in \{0, \ldots, l-1\}$.

Thus the degree of $g_j(X)$ is strictly increasing with j, (since $d_0 < d_1$).

Furthermore

$$\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_j(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X)) * (\mathrm{ev}_{\mathbf{a}}(h_1(X)))^j = \mathbf{d} * \mathbf{c}^j$$

i.e. the code $\mathrm{GRS}_l(\mathbf{c}, \mathbf{d})$ has $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_j(X))$ with $j \in \{0, \ldots, l-1\}$ as a basis.

That is $\mathrm{GRS}_l(\mathbf{c}, \mathbf{d})$ is an l-dimensional subcode of the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ and

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{d_0, d_1, d_0 + 2(d_1 - d_0), \ldots, d_0 + (l-1)(d_1 - d_0)\}$$

Proposition 7

Let us assume that $\mathcal{C} = \mathrm{GRS}_k(\mathbf{c}, \mathbf{d})$ is an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, i.e. $\exists g_j \in \mathbb{F}_q[X] \ : \ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_j(X)) = \mathrm{ev}_{\mathbf{c},\mathbf{d}}(X^j)$ with $j \in \{0, \ldots, l-1\}$.
Hence:

$$\begin{aligned} \mathbf{b} * \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_i(X)g_j(X)) &= \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_i(X)) * \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_j(X)) \\ &= \mathrm{ev}_{\mathbf{c},\mathbf{d}}(X^i) * \mathrm{ev}_{\mathbf{c},\mathbf{d}}(X^j) = \mathbf{d} * \mathrm{ev}_{\mathbf{c},\mathbf{d}}(X^{i+j}) \end{aligned}$$

So $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_i(X))g_j(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_u(X)g_v(X))$, i.e. $g_i(X)g_j(X) = g_u(X)g_v(X)$ with $0 \leq i, j, u, v \leq l$ such that $i + j = u + j$.
In particular we have that

$$g_0^{j-1}(X)g_j(X) = g_1^j(X) \quad (2)$$

$$g_0(X)g_2(X) = g_1(X)g_1(X) \quad (3)$$

From Equation **??** we can deduce that $\exists h_1 \in \mathbb{F}_q[X]$ such that $g_1(X) = g_0(X)h_1(X)$.
That is $g_j(X) = g_0(X)h_1^j(X)$.
And this imply that

$$\mathbf{d} * \mathbf{c}^j = \mathrm{ev}_{\mathbf{c},\mathbf{d}}(X^j) = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_j(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X)) * \mathrm{ev}_{\mathbf{a}}(h_1(X))^j$$

1. If $j = 0$ we deduce that $\mathbf{d} = \mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X))$.
2. If $j = 1$ we deduce that $\mathbf{c} = \mathrm{ev}_{\mathbf{a}}(h_1(X))$.

Let $\hat{d}_0 = \deg(g_0(X))$ and $\hat{d}_1 = \hat{d}_0 + \deg(h_1(X))$. Then the $(\mathbf{a}, \mathbf{b})$ non-gap sequence of $\mathcal{C}$ is

$$\hat{d}_0, \hat{d}_1, \hat{d}_0 + 2(\hat{d}_1 - \hat{d}_0), \ldots, \hat{d}_0 + (l-1)(\hat{d}_1 - \hat{d}_0).$$

Therefore $\hat{d}_0 = d_0$ and $\hat{d}_1 = d_1$.

PROPOSITION 8

If $i_1 + i_2 \in \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C}) \Rightarrow$

$$\begin{cases} i_1 \in \mathcal{I}(\mathcal{C}) & \overset{Prop.1}{\Longrightarrow} \quad \exists f_1 \in \mathbb{F}_q[X] \text{ with } \deg(f_1(X)) = i_1 \ : \ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_1(X)) \in \mathcal{C} \\ i_2 \in \mathcal{I}(\mathcal{C}) & \overset{Prop.1}{\Longrightarrow} \quad \exists f_2 \in \mathbb{F}_q[X] \text{ with } \deg(f_2(X)) = i_2 \ : \ \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_2(X)) \in \mathcal{C} \end{cases}$$

Therefore:

$$\mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_1(X)) * \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_2(X)) = \mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_1(X)f_2(X)) \in \mathcal{D}$$

with $\deg(f_1(X)f_2(X)) = \deg(f_1(X)) + \deg(f_2(X)) = i_1 + i_2$
Thus $i_1 + i_2 \in \mathcal{J}(\mathcal{D})$.

COUNTEREXAMPLE: THE EQUALITY DOES NOT HOLD IN GENERAL

Consider $\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_1), \ldots, mathrmev_{\mathbf{a},\mathbf{b}}(f_l) \rangle \subseteq \mathrm{GRS}_5(\mathbf{a}, \mathbf{b})$ where

$$f_1 = 1, \qquad f_2 = X^2 + X, \qquad f_3 = X^3 \qquad \text{and} \qquad f_4 = X^4$$

Then:

1. $\mathcal{I}(\mathcal{C}) = \{0, 2, 3, 4\} \Rightarrow \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C}) = \{0, 2, 3, 4, 5, 6, 7, 8\}$.
2. $1 \in \mathcal{J}(\mathcal{D})$ since

$$X = f_1(X)f_2(X) - f_2^2(X) + f_1(X)f_4(X) + 2f_1(X)f_3(X) \in \langle \mathcal{C} * \mathcal{C} \rangle = \mathcal{D}.$$

But $1 \notin \mathcal{I}(\mathcal{C}) + \mathcal{I}(\mathcal{C})$.

In fact $\mathcal{J}(\mathcal{D}) = \{0, 1, \ldots, 8\} \Rightarrow \mathcal{D} = \mathrm{GRS}_9(\mathbf{a}, \mathbf{b})$.

PROPOSITION 9

- Let $g_1, \ldots, g_l$ be a basis of $\mathcal{C}$. Then the elements $g_i * g_j$ with $1 \leq i \leq j \leq l$ generate $\mathcal{D}$. Therefore

$$\dim \mathcal{D} \leq \sum_{i=1}^{l} i = \binom{l+1}{2}.$$

- Since $\mathcal{D} \subseteq \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ then $\dim \mathcal{D} \leq 2k-1$

Furthermore:

1. If $\mathcal{D} = \mathrm{GRS}_r(\mathbf{a}, \mathbf{b}) \Rightarrow \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \{0, \ldots, \lfloor \frac{r-1}{2} \rfloor\}$.
   In fact since $\mathcal{D} = \mathrm{GRS}_r(\mathbf{a}, \mathbf{b})$ then by Proposition 4:

$$\mathcal{J}(\mathcal{D}) = \{0, \ldots, r-1\}$$

   and by Proposition 8:

$$\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) + \mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) \subseteq \mathcal{J}(\mathcal{D}, \mathbf{a}, \mathbf{b} * \mathbf{b}).$$

   i.e. if $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$ then:

   1. $2i_1 = i_1 + i_1 \geq 0 \Rightarrow i_1 \geq 0$.
   2. If $2i_l \leq 2k-1$ then $2i_l = i_l + i_l \in \mathcal{J}(\mathcal{D}) \Rightarrow i_l \leq \lfloor \frac{r-1}{2} \rfloor$.

2. Similarly to the previous procedure we can conclude 2 and 3.

PROPOSITION 10

Recall that the code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is generated by the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^i)$ with $i \in \{0, \ldots, k-1\}$.

Thus the code $\langle \mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) * \mathrm{GRS}_l(\mathbf{a}, \mathbf{c}))\rangle$ is generated by the elements:

$$\mathrm{ev}_{\mathbf{a},\mathbf{b}}(X^i) * \mathrm{ev}_{\mathbf{a},\mathbf{c}}(X^j) = \mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{c}}(X^{i+j})$$

with $i \in \{0, \ldots, k-1\}$ and $j \in \{0, \ldots, l-1\}$ i.e. $0 \leq i+j \leq k+l-2$.

Therefore the right hand side of the previous equality is a complete set of generators of the code $\mathrm{GRS}_{k+l-1}(\mathbf{a}, \mathbf{b} * \mathbf{c})$.

PROPOSITION 11

Let $\mathcal{C}$ be an l-dimensional subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ with $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b}) = \{i_1, \ldots, i_l\}$.
Then by Proposition 2 there are l polynomials in normal form

$$f_j(X) = X^{i_j} + \sum_{\substack{s<i_j \\ s\notin\mathcal{I}}} f_{j,s}X^s \in \mathbb{F}_q[X], \text{ for all } j = 1, \ldots, l,$$

with $j \in \{1, \ldots, l\}$ such that $\mathcal{C} = \langle \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_1(X)), \ldots, \mathrm{ev}_{\mathbf{a},\mathbf{b}}(f_l(X))\rangle$.
Then the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X)f_v(X))$ with $1 \le u \le v \le l$ generate the square code $\mathcal{D} = \langle \mathcal{C} * \mathcal{C}\rangle$ where

$$\deg(f_u(X)f_v(X)) = \deg(f_u(X)) + \deg(f_v(X)) = i_u + i_v$$

Assume that $\mathcal{D} = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b})$ i.e. the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(X^j)$ with $0 \le j \le 2k-2$ form a basis of $\mathcal{D}$.
Hence $\forall t \in \{0, \ldots, 2k-2\}, \exists(u, v) \ : \ i_u + i_v \ge t$ and $1 \le u \le v \le l$.
Since $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X)f_v(X)) \in \mathrm{GRS}_t(\mathbf{a}, \mathbf{b} * \mathbf{b}) \Rightarrow i_u + i_v < t$ and $1 \le u \le v \le l$.
Then the vector space $V_t = \mathrm{GRS}_{2k-1}(\mathbf{a}, \mathbf{b} * \mathbf{b}) \setminus \mathrm{GRS}_t(\mathbf{a}, \mathbf{b} * \mathbf{b})$ is generated by the elements $\mathrm{ev}_{\mathbf{a},\mathbf{b}*\mathbf{b}}(f_u(X)f_v(X))$ with $i_u + i_v \ge t$ and $1 \le u \le v \le l$, i.e.

$$\dim V_t = 2k - 1 - t.$$

Thus this is a lower bound of the number of elements that generates V_t.

COROLLARY 5

Let $\mathcal{C}$ be an l-dimensional GRS subcode of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, i.e. $\mathcal{C} = \mathrm{GRS}_l(\mathbf{c}, \mathbf{d})$ and $d_0 < d_1$ be the first two elements of $\mathcal{I}(\mathcal{C}, \mathbf{a}, \mathbf{b})$.
By Proposition 7 there exists $g_0, h_1 \in \mathbb{F}_q[X]$ such that:

1. $\mathrm{ev}_{\mathbf{a},\mathbf{b}}(g_0(X)) = \mathbf{d}$.
2. $\mathrm{ev}_{\mathbf{a}}(h_1(X)) = \mathbf{c}$.
3. $d_0 = \deg(g_0(X))$.
4. $d_1 = d_0 + \deg(h_1(X))$.

Note that

- The number of possible polynomials $g_0 \in \mathbb{F}_q[X]$ is at most $(q-1)q^{d_0}$.
- The number of possible polynomials $h_1 \in \mathbb{F}_1[X]$ is at most $(q-1)q^{d_1-d_0}$.

Since the pair (g_0, h_1) determines the code $\mathcal{C}$ uniquely and the number of possible pairs of given degree d_0 and d_1 is at most $(q-1)^2 q^{d_1}$, then the number of l-dimensional subcodes of $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ that are GRS is at most

$$\sum_{d_1=1}^{k-l+1} (q-1)^2 q^{d_1} \leq q^{k-l+3}.$$