Some questions about the Gray map

Carlos Vela

University of St.Gallen, Switzerland

30th Applications of Computer Algebra
July 17th 2025



Joint work with Anna-Lena Horlemann and Adrien Pasquereau

Metrics

Let $u \in \mathbb{Z}_{p^s}$ we consider the following metrics:

- The homogeneous metric

$$wt_{HW}(u) = \begin{cases} p^{s-2}(p-1) & \text{if } u \notin p^{s-1}\mathbb{Z}_{p^s} \\ p^{s-1} & \text{if } u \in p^{s-1}\mathbb{Z}_{p^s} \\ 0 & \text{if } u = 0 \end{cases}$$

- The Lee metric

$$wt_L(u) = min\{u, p^s - u\}.$$

- The Hamming metric

$$wt_H(u) \begin{cases} 1 & \text{if } u \neq 0 \\ 0 & \text{if } u = 0 \end{cases}$$

We can component-wise extend these metrics for elements in $\mathbb{Z}_{p^s}^n$. We define the distance between two elements $u, v \in \mathbb{Z}_{p^s}^n$ as $d(u, v) = wt(u - v)$.

Gray map

The first used Gray map was a map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$:

- Formal definition by

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

then $\phi(u) = (\beta(u), \gamma(u))$.

[1] Hammons, A. R., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

Gray map

The first used Gray map was a map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$:

- Formal definition by

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

then $\phi(u) = (\beta(u), \gamma(u))$.

[1] Hammons, A. R., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

Gray map

The first used Gray map was a map from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$:

- Formal definition by

c	$\alpha(c)$	$\beta(c)$	$\gamma(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

  then $\phi(u) = (\beta(u), \gamma(u))$.

- Linearity properties:

Theorem

ϕ is a distance-preserving map or isometry from $(\mathbb{Z}_4^n, d_L)$ to $(\mathbb{Z}_2^{2n}, d_H)$

[1] Hammons, A. R., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, *The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

Gray map (II)

We will say that a binary code C is $\mathbb{Z}_4$-**linear** if there exists a linear code $\mathcal{C}$ over $\mathbb{Z}_4$ such that $\phi(\mathcal{C}) = C$.

Theorem

The binary image $\phi(\mathcal{C})$ of a quaternary linear code $\mathcal{C}$ is linear if and only if

$$a, b \in \mathcal{C} \Rightarrow 2\alpha(a) * \alpha(b) \in \mathcal{C}$$

Generalized Gray map

The **generalized Gray map** can be defined in terms of a matrix. Let $u \in \mathbb{Z}_{2^s}$ and $u = \sum_{i=0}^{s-1} 2^i u_i$:

$$G(u) = (u_0, \ldots, u_{s-1}) \begin{pmatrix} Y \\ \hline \mathbf{1} \end{pmatrix} \in \mathbb{Z}_2^{2^{s-1}},$$

where Y is a $(s-1) \times 2^{s-1}$ matrix whose columns are the elements of $\mathbb{Z}_2^{s-1}$. The case $s = 3$, Y has all the elements of $\mathbb{Z}_2^2$:

Generalized Gray map

The **generalized Gray map** can be defined in terms of a matrix. Let $u \in \mathbb{Z}_{2^s}$ and $u = \sum_{i=0}^{s-1} 2^i u_i$:

$$G(u) = (u_0, \ldots, u_{s-1}) \left(\frac{Y}{\mathbf{1}}\right) \in \mathbb{Z}_2^{2^{s-1}},$$

where Y is a $(s-1) \times 2^{s-1}$ matrix whose columns are the elements of $\mathbb{Z}_2^{s-1}$. The case $s = 3$, Y has all the elements of $\mathbb{Z}_2^2$:

$$G(u) = (u_0, u_1, u_2) \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Generalized Gray map

The **generalized Gray map** can be defined in terms of a matrix. Let $u \in \mathbb{Z}_{2^s}$ and $u = \sum_{i=0}^{s-1} 2^i u_i$:

$$G(u) = (u_0, \ldots, u_{s-1}) \left(\frac{Y}{\mathbf{1}}\right) \in \mathbb{Z}_2^{2^{s-1}},$$

where Y is a $(s-1) \times 2^{s-1}$ matrix whose columns are the elements of $\mathbb{Z}_2^{s-1}$. The case $s = 3$, Y has all the elements of $\mathbb{Z}_2^2$:

$$G(u) = (u_0, u_1, u_2) \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Generalized Gray map

The **generalized Gray map** can be defined in terms of a matrix. Let $u \in \mathbb{Z}_{2^s}$ and $u = \sum_{i=0}^{s-1} 2^i u_i$:

$$G(u) = (u_0, \ldots, u_{s-1}) \left(\frac{Y}{\mathbf{1}}\right) \in \mathbb{Z}_2^{2^{s-1}},$$

where Y is a $(s-1) \times 2^{s-1}$ matrix whose columns are the elements of $\mathbb{Z}_2^{s-1}$. The case $s = 3$, Y has all the elements of $\mathbb{Z}_2^2$:

$$G(1) = (1,0,0) \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = (1,0,1,0)$$

Generalized Gray map

The **generalized Gray map** can be defined in terms of a matrix. Let $u \in \mathbb{Z}_{2^s}$ and $u = \sum_{i=0}^{s-1} 2^i u_i$:

$$G(u) = (u_0, \ldots, u_{s-1}) \left(\frac{Y}{\mathbf{1}}\right) \in \mathbb{Z}_2^{2^{s-1}},$$

where Y is a $(s-1) \times 2^{s-1}$ matrix whose columns are the elements of $\mathbb{Z}_2^{s-1}$. The case $s = 3$, Y has all the elements of $\mathbb{Z}_2^2$:

$$G(1) = (1,0,0) \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = (1,0,1,0)$$

Example

0	$\longmapsto$	0000	4	$\longmapsto$	1111
1	$\longmapsto$	0101	5	$\longmapsto$	1010
2	$\longmapsto$	0011	6	$\longmapsto$	1100
3	$\longmapsto$	0110	7	$\longmapsto$	1001

Generalized Gray map

- The generalized Gray map holds the following properties:

Proposition

Let $u, v \in \mathbb{Z}_{2^s}$. Then $d_H(G(u), G(v)) = wt_H(G(u - v))$

Theorem

The generalized Gray map is an isometry between $(\mathbb{Z}_{2^s}, d_{HW})$ and $(\mathbb{Z}_2, d_H)$.

Corollary

Let $u \in \mathbb{Z}_{2^s}$, then $G(u) + G(2^{s-1}) = G(u + 2^{s-1})$.

[1] C. Carlet, $\mathbb{Z}_{2^k}$*-linear codes*, IEEE Trans. Inform. Theory, **44**, 4 (1998), 1543–1547.

Modular Gray maps

The $\mathbb{Z}_{2^s}$-linear codes are not just binary. We can define a modular Gray map that $\eta_g^s : \mathbb{Z}_{2^s} \to \mathbb{Z}_{2^{s-1}}^2$. Let

$$\begin{aligned} A_1 &= \{0, 1, 2, 3, \ldots, 2^{s-2} - 1\}, \\ A_2 &= \{2^{s-2}, 2^{s-2} + 1, \ldots, 2^{s-1} - 1\}, \\ A_3 &= \{2^{s-1}, 2^{s-1} + 1, \ldots, 2^{s-1} + 2^{s-2} - 1\}, \\ A_4 &= \{2^{s-1} + 2^{s-2}, 2^{s-1} + 2^{s-2} + 1, \ldots, 2^{s-1} + 2^{s-1} - 1\} \end{aligned}$$

Then

$$\eta_g^s(i) = \begin{cases} (i, i) & i \in A_1 \\ (i - 2^{s-2}, i) & i \in A_2 \\ (i - 2^{s-2}, i - 2^{s-2}) & i \in A_3 \\ (i - 2^{s-1}, i - 3 \cdot 2^{s-2}) & i \in A_4 \end{cases}$$

[1] M.K.Gupta, *On modular Gray maps*, ArXiv:2210.16165.

[2] C. Fernandez-Cordoba, C. Vela, M. Villanueva: *Equivalences among $\mathbb{Z}_{2^s}$-linear Hadamard codes.* Discrete Mathematics 343(3), 111721 (2020).

Modular Gray map

- Can be seen as:
$$\eta_g^s : \mathbb{Z}_{2^s} \to RM_{\mathbb{Z}_{2^{s-1}}}(1,1)$$
- Modular Gray map is an isometry between $(\mathbb{Z}_{2^s}, d_{HW})$ and $\mathbb{Z}_{2^{s-1}}, d_{HW})$.

Example

0	$\longmapsto$	00	4	$\longmapsto$	22
1	$\longmapsto$	11	5	$\longmapsto$	33
2	$\longmapsto$	02	6	$\longmapsto$	20
3	$\longmapsto$	13	7	$\longmapsto$	31

Modular Gray map

- Modular Gray map for $s = 2$ is the usual Gray map:

Theorem

The generalised Gray map can be written as a product of $s-1$ modular Gray maps.

$$G = \eta_g^s \cdot \eta_g^{s-1} \cdots \eta_g^3 \cdot \eta_g^2$$

Now we have isometries between all the intermediate rings:

$$\mathbb{Z}_{2^s} \to \mathbb{Z}_{2^{s-1}} \to \mathbb{Z}_{2^{s-1}} \to \cdots \to \mathbb{Z}_4 \to \mathbb{Z}_2$$

Motivation

Is it a one-way function?

Dimension by dimension (step by step)

Theorem

For all $s \geq 2$, for all $0 \leq k \leq s$, the image $\Gamma^s(\langle 2^{s-k} \rangle)$ is a $[2^{s-1}, k]_2$-linear code generated by

$$\mathbf{G}_{s,k} = \begin{cases} \begin{pmatrix} 0 & \dots & 0 \end{pmatrix} \in \mathbb{F}_2^{1 \times 2^{s-1}} & \text{if } k = 0, \\ \begin{pmatrix} 1 & \dots & 1 \end{pmatrix} \in \mathbb{F}_2^{1 \times 2^{s-1}} & \text{if } k = 1, \\ \begin{pmatrix} \mathbf{G}_{s-1,k-1} & \mathbf{G}_{s-1,k-1} \\ \mathbf{G}_{s-1,0} & \mathbf{G}_{s-1,1} \end{pmatrix} \in \mathbb{F}_2^{k \times 2^{s-1}} & \text{if } 2 \leq k \leq s, \end{cases}$$

with the convention that $\mathbf{G}_{1,0} = 0$ and $\mathbf{G}_{1,1} = 1$.

An example

Let $s = 3$ consider the quotient ring $\mathbb{Z}_8$. The Gray image of the ideal $\Gamma^3(\langle 2^2 \rangle) = \Gamma_3(\{0, 4\})$:

$$\Gamma_3(0) = (0\,, 0\,, 0\,, 0)\,;\, \Gamma_3(4) = (\Gamma_2(2), \Gamma_2(2)) = (1\,, 1\,, 1\,, 1)$$

As you can see is the subspace generated by $G_{3,1} = (1\,, 1\,, 1\,, 1)$ as the previous theorem says for $k = 1$!!

An example

We can also compute $\Gamma^3(\langle 2 \rangle) = \Gamma^3(\{0, 2, 4, 6\})$ which:

$$\Gamma^3(2) = (\Gamma^2(0), \Gamma^2(2)) = (0\,, 0\,, 1\,, 1)$$
$$\Gamma^3(6) = (\Gamma^3(2), \Gamma^2(0)) = (1\,, 1\,, 0\,, 0)$$

Again, is easy to see that this set is generated by the matrix:

$$G_{3,2} = \begin{pmatrix} G_{2,1} & G_{2,1} \\ G_{2,0} & G_{2,1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Dimension by dimension (step by step)

Corollary

For all $s \geq 2$, *for all* $0 \leq k \leq s$, *for all* $m \geq 0$,

$$\mathbf{G}_{s+m,k} = \mathbf{G}_{s,k} \otimes_{\mathbb{F}_2} \left((1\ 1)^{\otimes m} \right),$$

in particular, $\Gamma^{s+m}(\langle 2^{s-k+m} \rangle)$ *can be derived as a* 2^m*-fold repetition code from* $\Gamma^s(\langle 2^{s-k} \rangle)$.

Step by step

Let $s = 3, m = 2$ and $k = 2$ as in the above Corollary:

$$G_{3+2,2} = \begin{pmatrix} G_{4,1} & G_{4,1} \\ G_{4,0} & G_{4,1} \end{pmatrix} =$$

$$= \left(\begin{array}{cccccccc|cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

On the other hand:

$$G_{3+2,2} = G_{3,2} \otimes ((1\ 1)^{\otimes 2}) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \otimes ((1\ 1)^{\otimes 2})$$

Step by step

Lemma

Let $s \geq 2$, and let $\mathcal{P}_s$ the lexicographically ordered list of all points of the affine space $\mathrm{AG}^{s-1}(\mathbb{F}_2)$ associated with the equation $x_0 - 1 = 0$. Then, for all $0 \leq k \leq s$,

$$\Gamma^s(\langle 2^{s-k} \rangle) = \mathrm{ev}(\mathcal{P}_s, \langle x_i \mid i \in \{0, ..., k-1\} \rangle_{\mathbb{F}_2}).$$

More precisely, $\Gamma^s(2^{s-k}) = \mathrm{ev}(\mathcal{P}_s, x_{k-1})$.

An example

Let $s = 3$ and $k = 2$ We want to see that
$\Gamma^3(\langle 2^{3-2} \rangle) = \mathrm{ev}(\mathcal{P}_3, \langle x_0, x_1, x_0 + x_1 \rangle_{\mathbb{F}_2})$

- from above:

$$\Gamma^3(\langle 2 \rangle) = \left\langle \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \right\rangle$$

- The set $\mathcal{P}_3 = \{(1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$ and the evaluations:

	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
0	0	0	0	0
x_0	1	1	1	1
x_1	0	0	1	1
$x_0 + x_1$	1	1	0	0

We could get to

Corollary

The generalised Gray map is invertible in $O(s)$-time.

Require: $\vec{y} = (y_1, y_2, ..., y_{2^{s-1}}) \in \mathbb{F}_2^{2^{s-1}}$
Ensure: $\Gamma^s(a + 2^s\mathbb{Z}) = \vec{y}$
  $b \leftarrow y_1$
  $a \leftarrow b \star 2^{s-1}$
  for $i = 0, ..., s-2$ **do**
    $a \leftarrow a + (b \oplus y_{2^i+1}) \star 2^i$
  end for

where $\star : \mathbb{F}_2 \times \mathbb{Z}/2^s\mathbb{Z} \to \mathbb{Z}/2^s\mathbb{Z}$ with $0 \star a = 0$ and $1 \star a = a$.

The answer

Corollary

The Gray map is not a one-way function.

Some Notation

- We denote $\varphi : \mathbb{Z}/2^s\mathbb{Z} \to \mathbb{F}_2[x_0, ..., x_{s-1}]$ the map defined by, for all $a = \sum_{i=0}^{s-1} \alpha_i 2^i \in \mathbb{Z}/2^s\mathbb{Z}$ with $\alpha_i \in \{0, 1\}$ for all $0 \leq i \leq s-1$,

$$\varphi\left(\sum_{i=0}^{s-1} \alpha_i 2^i\right) = \sum_{i=0}^{s-1} \alpha_i \cdot x_{i+1} \pmod{s}.$$

  By extension, we define a family of maps

$$\{\Phi_n : (\mathbb{Z}/2^s\mathbb{Z})^n \to \mathbb{F}_2[x_0, ..., x_{s-1}, y_1, ..., y_n] \mid n \geq 1\},$$

  where, for all $n \geq 1$, for all $\vec{a} = (a_1, ..., a_n) \in (\mathbb{Z}/2^s\mathbb{Z})^n$

$$\Phi_n(\vec{a}) = \sum_{j=1}^{n} y_j \cdot \varphi(a_j).$$

Some notations

- For any $n \geq 1$, let

$$\mathcal{P}_{s,n} = \bigcup_{j=1}^{n} \mathcal{V}(\langle x_0 - 1, y_1, ..., y_{j-1}, y_j - 1, y_{j+1}, ..., y_n \rangle)$$

be a subset of $n2^{s-1}$ points in $\mathrm{PG}^{s+n-1}(\mathbb{F}_2)$.

Some new about linearity

Lemma

For any set $\mathfrak{C} \subseteq (\mathbb{Z}/2^s\mathbb{Z})^n$, *the following conditions are equivalent:*

1. *the image*

$$\mathcal{C} = \Gamma^s(\mathfrak{C}) \subseteq \mathbb{F}_2^{n2^{s-1}}$$

under the composed Gray map is additive,

2. *the restriction*

$$\mathcal{C}' = \{(c_{(j-1)2^{s-1}+2^i})_{\substack{0\leq i\leq s-2\\ 1\leq j\leq n}} \mid \vec{c} = (c_1, c_2, ..., c_{n2^{s-1}}) \in \mathcal{C}\} \subseteq \mathbb{F}_2^{ns}$$

is additive,

3. *the set of polynomials*

$$\Phi_n(\mathfrak{C}) \subseteq \mathbb{F}_2[x_0, ..., x_{s-1}, y_1, ..., y_n]$$

is additive.

A consequence

Corollary

For any set $\mathfrak{C} \subseteq (\mathbb{Z}/2^s\mathbb{Z})^n$, $\mathcal{C} = \Gamma^s(\mathfrak{C})$ *is linear if and only if* $\mathrm{ev}(\mathcal{P}'_{s,n}, \Phi_n(\mathfrak{C}))$ *is linear, where* $\mathcal{P}'_{s,n} \subseteq \mathcal{P}_{s,n}$ *is the embedding of* AG^{s+n-1} *with respect to the chart* $x_0 - 1 = 0$ *of the set*

$$\{(\vec{e}_i \,||\, \vec{f}_j) \mid i \in \{1, ..., s-1\}, j \in \{1, ..., n\}\},$$

where $(\vec{e}_i)_i$ *(resp.* $(\vec{f}_j)_j$*) form the canonical basis of* $\mathbb{F}_2^{s-1}$ *(resp.* $\mathbb{F}_2^n$*).*

Example

Let $\mathcal{C} \subset \mathbb{Z}_8^2$ be the code $\{(0,0),(5,0),(1,4),(4,4)\}$. Its Gray map image is

$$\Gamma^3(\mathcal{C}) = \left\langle \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \right\rangle$$

The set of polynomials $\Phi_2(\mathcal{C}) \subset \mathbb{F}_2[x_0, x_1, x_2; y_1, y_2]$

$$\Phi_2 = \{0, (x_0 + x_1)y_1, x_0y_2 + x_1y_1, x_0(y_1 + y_2)\}$$

Finally, we have that the sets of points are:

$$\begin{aligned} \mathcal{P}_{3,2} = \{&(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1}) \\ &(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1}) \\ &(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0}), (\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}) \\ &(1,1,1,1,0), (1,1,1,0,1)\} \end{aligned}$$

where $\mathcal{P}'_{3,2}$ are the bolded points.

Example

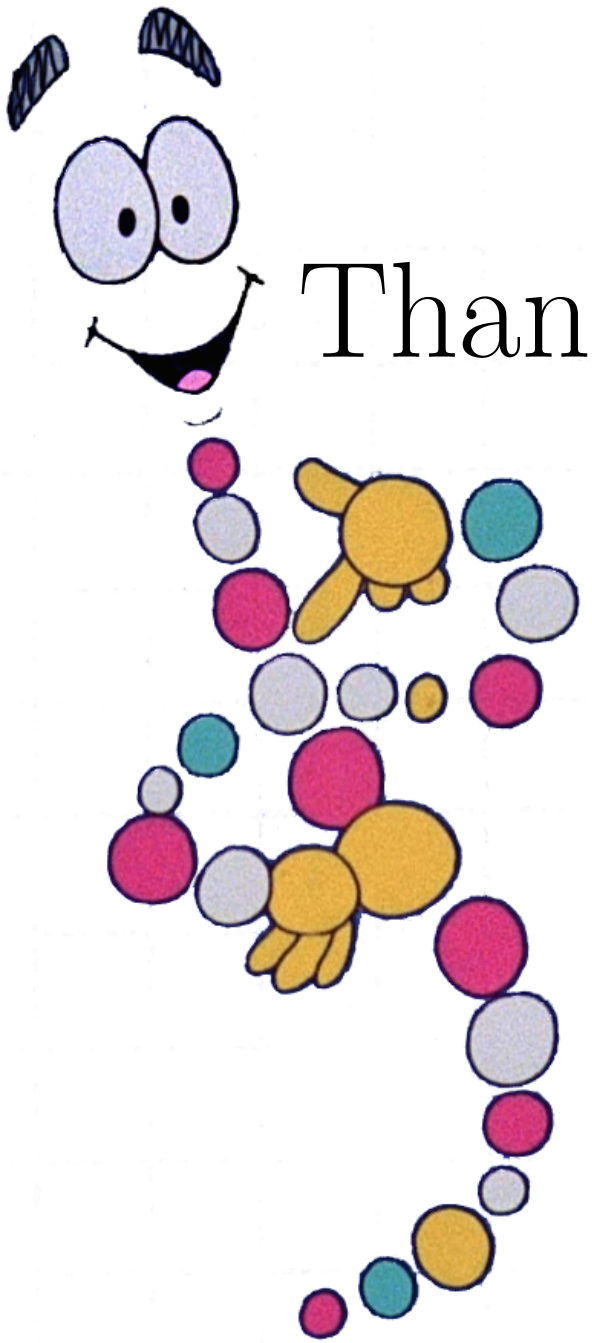
Let's do the evaluations:

$\mathrm{ev}(\mathcal{P}'_{3,2}, \Phi_2(\mathcal{C}))$	0	$(x_0+x_1)y_1$	$x_0y_2+x_1y_1$	$x_0(y_1+y_2)$
$(1,1,0,1,0)$	0	0	1	1
$(1,0,1,1,0)$	0	1	0	1
$(1,0,0,1,0)$	0	1	0	1
$(1,1,0,0,1)$	0	0	1	1
$(1,0,1,0,1)$	0	0	1	1
$(1,0,0,0,1)$	0	0	1	1

If we look at the columns we have a linear set!

Conclusions

- Can we see gray map as a one-way function if adding a permitation?
- In the composition of the partial Gray map, where do the image of an additive code is nonlinear for the first time.
- How other properties of the modules behave after applying the gray map?
- Can we use it for Cryptographic purposes?



Thank you for your attention!

Questions?

Comments?

Suggestions?