Error-correcting codes on weighted projective planes and applications to Private Information Retrieval

Julien Lavauzelle, **Jade Nardi**

Institut de recherche mathématique de Rennes
Institut de Mathématiques de Toulouse

14/06/2019

Partially funded by ANR *Manta*

Weighted Projective Reed-Muller codes and η-lines

Fix $\eta \in \mathbb{N}^*$. Consider the weighted Reed-Muller code of weight $(1, \eta)$:

$$\mathrm{WRM}_q^{\eta}(d) := \langle \mathrm{ev}(x^i y^j),\ (i,j) \in \mathbb{N}^2 \mid i + \eta j \leq d \rangle \subset \mathbb{F}_q^{q^2}$$

Can be seen as an AG code on $\mathbb{P}^{(1,1,\eta)}$ outside the line $(X_0 = 0)$

Weighted Projective Reed-Muller codes and η-lines

Fix $\eta \in \mathbb{N}^*$. Consider the weighted Reed-Muller code of weight $(1, \eta)$:

$$\mathrm{WRM}_q^\eta(d) := \langle \mathrm{ev}(x^i y^j),\ (i,j) \in \mathbb{N}^2 \mid i + \eta j \leq d \rangle \subset \mathbb{F}_q^{q^2}$$

Can be seen as an AG code on $\mathbb{P}^{(1,1,\eta)}$ outside the line $(X_0 = 0)$

Definition (η-line)

(Non-vertical) η-*line* :

- on $\mathbb{P}^{(1,1,\eta)}$: Set of zeroes of $P(X_0, X_1, X_2) = X_2 - \Phi(X_0, X_1)$, where $\phi \in \mathbb{F}_q[X_0, X_1]_h$ and $\deg \phi = \eta$.
- on $\mathbb{A}^2$: Set of zeroes of $P(x, y) = y - \phi(x)$, where $\phi \in \mathbb{F}_q[X]$ and $\deg \phi \leq \eta$.

Parametrization of η-lines

Recalls:

- $\mathrm{WRM}_q^\eta(d) := \langle \mathrm{ev}(x^i y^j),\ (i,j) \in \mathbb{N}^2 \mid i + \eta j \leq d \rangle$
- η-line: $y = \phi(x)$ with $\phi \in \mathbb{F}_q[X]$ and $\deg \phi \leq \eta$.

Parametrization of an η-line: $t \mapsto (t, \phi(t))$
Set of embeddings of η-lines into the affine plane $\mathbb{A}^2$:

$$\Phi_\eta = \{L_\phi : t \mapsto (t, \phi(t)) \mid \phi \in \mathbb{F}_q[T] \text{ and } \deg \phi \leq \eta\},$$

Parametrization of η-lines

Recalls:

- $\mathrm{WRM}_q^\eta(d) := \langle \mathrm{ev}(x^i y^j),\ (i,j) \in \mathbb{N}^2 \mid i + \eta j \le d \rangle$
- η-line: $y = \phi(x)$ with $\phi \in \mathbb{F}_q[X]$ and $\deg \phi \le \eta$.

Parametrization of an η-line: $t \mapsto (t, \phi(t))$
Set of embeddings of η-lines into the affine plane $\mathbb{A}^2$:

$$\Phi_\eta = \{ L_\phi : t \mapsto (t, \phi(t)) \mid \phi \in \mathbb{F}_q[T] \text{ and } \deg \phi \le \eta \},$$

Lemma

Any polynomial $f \in \mathbb{F}_q[X,Y]$ with $\deg_{(1,\eta)} \le d$ satisfies $\mathrm{ev}(f \circ L) \in \mathrm{RS}_q(d)$ for any $L \in \Phi_\eta$.

Check on monomials: set $f = X^i Y^j$ with $i + \eta j \le d$.
$\forall\ \phi \in \Phi_\eta$, $(f \circ L_\phi)(T) = T^i \phi(T)^j$ has degree less than d.

PIR Protocol

PIR Protocol

How to retrieve a datum stored on servers without giving any information about it?

$\rightsquigarrow$ Aim of **P**rivate **I**nformation **R**etrieval protocols

PIR Protocol

How to retrieve a datum stored on servers without giving any information about it?

$\rightsquigarrow$ Aim of **P**rivate **I**nformation **R**etrieval protocols

[Augot,Levy-dit-Vehel,Shikfa (2014)] Share the database on several servers.

PIR Protocol

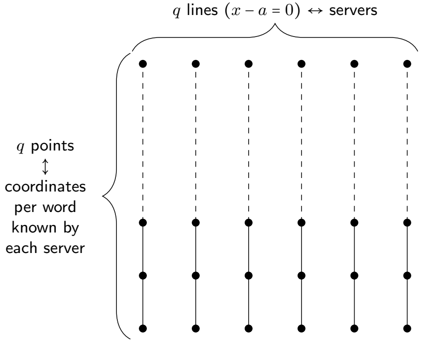
How to retrieve a datum stored on servers without giving any information about it?

$\rightsquigarrow$ Aim of **P**rivate **I**nformation **R**etrieval protocols

[Augot,Levy-dit-Vehel,Shikfa (2014)] Share the database on several servers.

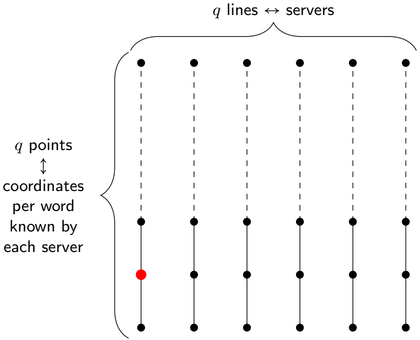
$\mathbb{A}^2(\mathbb{F}_q) = \bigsqcup_{i=1}^{q} L_i(\mathbb{F}_q)$
(lines of the ruling)

Database: Codewords of $\mathrm{WRM}_q(d,(1,\eta))$ shared by **q servers**.



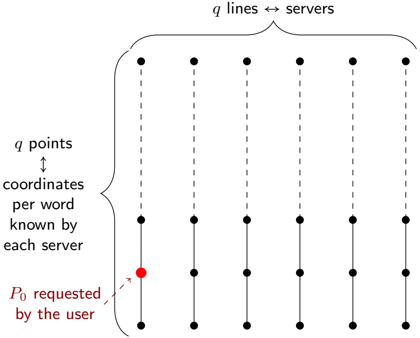
PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.



PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

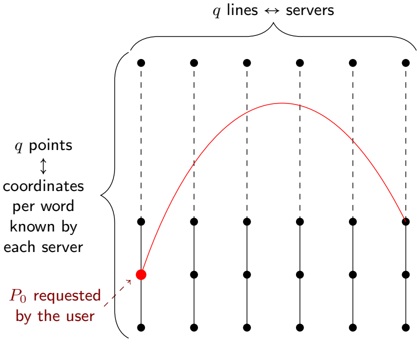
1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.



Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.

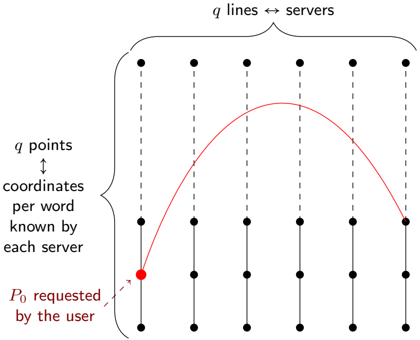


Randomly pick an η-line L containing P_0.

Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.

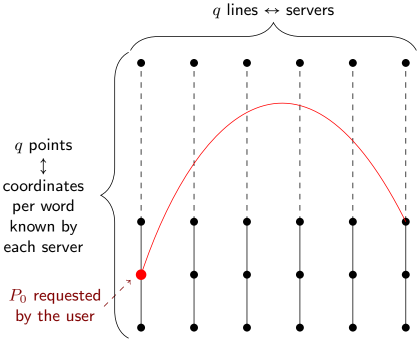


Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

Randomly pick an η-line L containing P_0.
Server ↔ line not containing P_0: ask for $c_{L_i \cap L}$

PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.

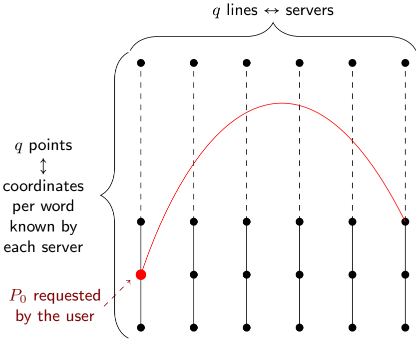


Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

Randomly pick an η-line L containing P_0.
Server ↔ line not containing P_0: ask for $c_{L_i \cap L}$
Server ↔ line containing P_0: ask for c_{P_1} for P_1 random on this line

PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.



Wanted datum: c_{P_0} with $c \in \mathrm{WRM}_q^\eta(d)$ and $d < q - 2$.

Randomly pick an η-line L containing P_0.
Server ↔ line not containing P_0: ask for $c_{L_i \cap L}$
Server ↔ line containing P_0: ask for c_{P_1} for P_1 random on this line

⇒ Word of RS(d) with 1 error = easily correctable!

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)

Why take $\eta > 1$?

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)

Why take $\eta > 1$? What if servers communicate...?

η-line $\leftrightarrow$ Polynomial $\phi \in \mathbb{F}_q[X]$ with $\deg(\phi) \leq \eta$.

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)

Why take $\eta > 1$? What if servers communicate...?

η-line $\leftrightarrow$ Polynomial $\phi \in \mathbb{F}_q[X]$ with $\deg(\phi) \leq \eta$.

$\eta = 1 \Rightarrow$ the protocol does not resist to colluding servers!

$\eta > 1 \Rightarrow$ the protocol resists to the collusion of η servers!

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)

Why take $\eta > 1$? What if servers communicate...?

η-line $\leftrightarrow$ Polynomial $\phi \in \mathbb{F}_q[X]$ with $\deg(\phi) \leq \eta$.

$\eta = 1 \Rightarrow$ the protocol does not resist to colluding servers!

$\eta > 1 \Rightarrow$ the protocol resists to the collusion of η servers!

... **Counterpart**...

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)

Why take $\eta > 1$? What if servers communicate...?

η-line $\leftrightarrow$ Polynomial $\phi \in \mathbb{F}_q[X]$ with $\deg(\phi) \leq \eta$.

$\eta = 1 \Rightarrow$ the protocol does not resist to colluding servers!

$\eta > 1 \Rightarrow$ the protocol resists to the collusion of η servers!

... **Counterpart**... For $d < q - 1$,

$$\dim \mathrm{WRM}_q^\eta(d) \approx \frac{d^2}{2\eta}$$

decreases as η grows $\Rightarrow$ Loss of storage when η grows.

Can we enhance the dimension while keeping the resistance to collusions?

Only property useful to the PIR protocol:
Restricting words along η-lines gives $\mathsf{RS}(d)$ codewords.

Can we enhance the dimension while keeping the resistance to collusions?

Only property useful to the PIR protocol:
Restricting words along η-lines gives RS(d) codewords.

$\rightsquigarrow$ *Lifting process* introduced by Guo,Kopparty,Sudan (2013)

Definition (η-lifting of a Reed-Solomon code)

Let q be a prime power. The *η-lifting of the Reed-Solomon code* $\mathrm{RS}_q(d)$ is the code of length $n = q^2$ defined as follows:

$$\mathrm{Lift}^\eta(\mathrm{RS}_q(d)) = \{\mathrm{ev}_{\mathbb{F}_q^2}(f) \mid f \in \mathbb{F}_q[X,Y], \forall L \in \Phi_\eta, \mathrm{ev}_{\mathbb{F}_q}(f \circ L) \in \mathrm{RS}_q(d)\}.$$

Recall: $\Phi_\eta = \{L_\phi : t \mapsto (t, \phi(t)) \mid \phi \in \mathbb{F}_q[T]$ and $\deg \phi \leq \eta\}$.

Of course, $\mathrm{WRM}_q^\eta(d) \subset \mathrm{Lift}^\eta \mathrm{RS}_q(d)$.
Question: $\mathrm{WRM}_q^\eta(d) \subsetneq \mathrm{Lift}^\eta \mathrm{RS}_q(d)$?

Example of $\mathrm{WRM}_q^\eta(d) \subsetneq \mathrm{Lift}^\eta(\mathrm{RS}_q(d))$

Let $q = 4$, $\eta = 2$ and $d = 2$. $\mathrm{WRM}_q^\eta(d, (1) = \langle \mathrm{ev}(X^i Y^j) \rangle$ with

$$(i, j) \in \{(0,0), (0,1), (1,0), (2,0)\} .$$

Take $f(X,Y) = Y^2 \in \mathbb{F}_4[X,Y] \setminus \mathrm{WRM}_4^2(2)$.
η-line: $L(T) = (T, aT^2 + bT + c) \in \Phi_2$, with $a, b, c \in \mathbb{F}_4$.
For every $t \in \mathbb{F}_4$,

$$(f \circ L)(t) = (at^2 + bt + c)^2 = a^2 t^4 + b^2 t^2 + c^2 = b^2 t^2 + a^2 t + c .$$

$\Rightarrow \mathrm{ev}_{\mathbb{F}_4}(f \circ L) \in \mathrm{RS}_4(2)$ for every $L \in \Phi_2$.

Example of $\mathrm{WRM}_q^\eta(d) \subsetneq \mathrm{Lift}^\eta(\mathrm{RS}_q(d))$

Let $q = 4$, $\eta = 2$ and $d = 2$. $\mathrm{WRM}_q^\eta(d,(1) = \langle \mathrm{ev}(X^iY^j)\rangle$ with

$$(i,j) \in \{(0,0),(0,1),(1,0),(2,0)\}\,.$$

Take $f(X,Y) = Y^2 \in \mathbb{F}_4[X,Y] \setminus \mathrm{WRM}_4^2(2)$.
η-line: $L(T) = (T, aT^2 + bT + c) \in \Phi_2$, with $a,b,c \in \mathbb{F}_4$.
For every $t \in \mathbb{F}_4$,

$$(f \circ L)(t) = (at^2 + bt + c)^2 \overset{❶}{=} a^2t^4 + b^2t^2 + c^2 \overset{❷}{=} b^2t^2 + a^2t + c\,.$$

$\Rightarrow \mathrm{ev}_{\mathbb{F}_4}(f \circ L) \in \mathrm{RS}_4(2)$ for every $L \in \Phi_2$.

$$\mathrm{WRM}_4^2(2) \subsetneq \mathrm{Lift}^2(\mathrm{RS}_4(2))\,.$$

Two phenomena:

1. Vanishing coefficients in characteristic p,
2. $t^q = t$ for $t \in \mathbb{F}_q$.

Two phenomena:

1. Vanishing coefficients in characteristic p

2. $t^q = t$ for $t \in \mathbb{F}_q$

Two phenomena:

1. Vanishing coefficients in characteristic p

Theorem (Lucas theorem - 1978)

Let $a, b \in \mathbb{N}$ and p be a prime number. Write $a = \sum_{i \geq 0} a^{(i)} p^i$, the representation of a in base p. Then

$$\binom{a}{b} = \prod_{i \geq 0} \binom{a^{(i)}}{b^{(i)}} \mod p\,.$$

2. $t^q = t$ for $t \in \mathbb{F}_q$

Two phenomena:

1. Vanishing coefficients in characteristic p

Theorem (Lucas theorem - 1978)

Let $a, b \in \mathbb{N}$ and p be a prime number. Write $a = \sum_{i\geq 0} a^{(i)} p^i$, the representation of a in base p. Then

$$\binom{a}{b} = \prod_{i\geq 0} \binom{a^{(i)}}{b^{(i)}} \mod p\,.$$

2. $t^q = t$ for $t \in \mathbb{F}_q$
   For $a \in \mathbb{N}$, there exists a unique $r \in \{0, \dots, q-1\}$ s.t. $t^a = t^r$ for every $t \in \mathbb{F}_q$, denoted by $\mathrm{Red}_q^\star(a)$.

$$\left(q - 1 \mid \mathrm{Red}_q^\star(a) - a\right) \text{ and } \left(\mathrm{Red}_q^\star(a) = 0 \Leftrightarrow a = 0\right)$$

Theorem [Lavauzelle, N - 2019]

1. The linear code $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ is spanned by monomials.
2. A monomial X^iY^j belongs to $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ if and only if for every $\mathbf{k} \in \mathbb{N}^\eta$ such that for all $r \geq 0$, $\sum_{l=1}^{\eta} k_l^{(r)} \leq j^{(r)}$, we have

$$\mathrm{Red}_q^\star\left(i + \sum_{l=1}^{\eta} l k_l\right) \leq d.$$

Only interesting when $d < q - 1$ since $\mathrm{RS}_q(q-1)$ is trivial.

Theorem [Lavauzelle, N - 2019]

1. The linear code $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ is spanned by monomials.
2. A monomial X^iY^j belongs to $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ if and only if for every $\mathbf{k} \in \mathbb{N}^\eta$ such that for all $r \geq 0$, $\sum_{l=1}^{\eta} k_l^{(r)} \leq j^{(r)}$, we have

$$\mathrm{Red}_q^\star\left(i + \sum_{l=1}^{\eta} l k_l\right) \leq d.$$

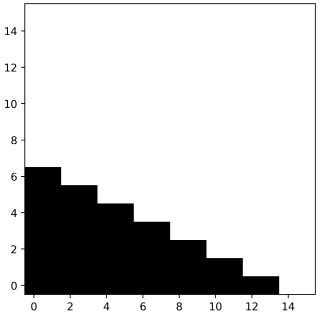
Only interesting when $d < q - 1$ since $\mathrm{RS}_q(q-1)$ is trivial.

Question: Is $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$ really bigger than $\mathrm{WRM}_q^\eta(d)$?

Representation of the monomials $x^i y^j$ whose evaluation belongs to $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$

Remark: i and j can be assumed $\leq q-1$.

Represent couples (i,j) in the square $\{0,\ldots,q-1\}^2$ → **Degree set**



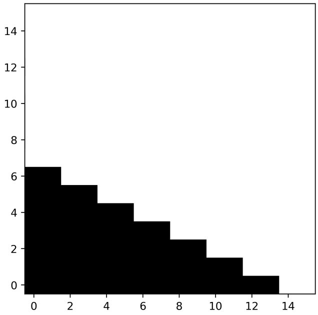
$\mathrm{WRM}^2_{16}(13)$

Total square are = length / Black area = dimension

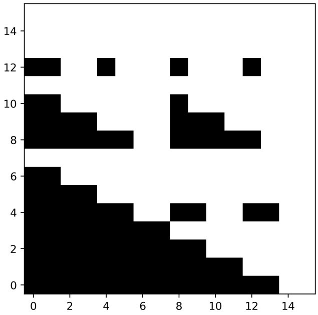
Representation of the monomials $x^i y^j$ whose evaluation belongs to $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$

Remark: i and j can be assumed $\leq q-1$.

Represent couples (i,j) in the square $\{0,\ldots,q-1\}^2$ → **Degree set**



$\mathrm{WRM}^2_{16}(13)$



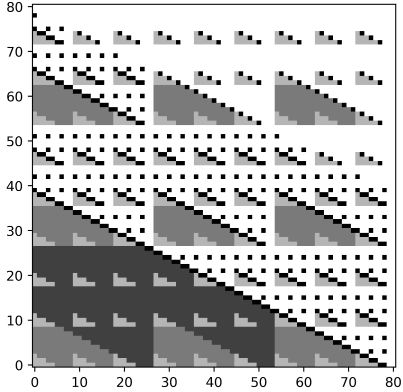
$\mathrm{Lift}^2(\mathrm{RS}_{16}(13))$

Total square are = length / Black area = dimension

How big can be our η-lifted codes ?

Uselful property of the degree set of $\mathrm{Lift}^\eta \mathrm{RS}_q(q-\alpha)$

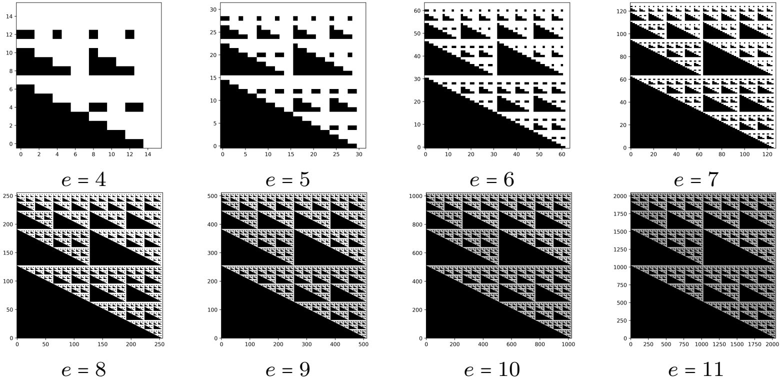
For a fixed $\alpha \geq 2$, the degree set of $\mathrm{Lift}^\eta \mathrm{RS}_q(q-\alpha)$ contains many copies of the degree set of $\mathrm{WRM}^\eta_{p^\varepsilon}(p^\varepsilon - \alpha - \eta)$, for $\varepsilon \leq e$.



$\mathrm{Lift}^2(\mathrm{RS}_{3^4}(3^4-3))$

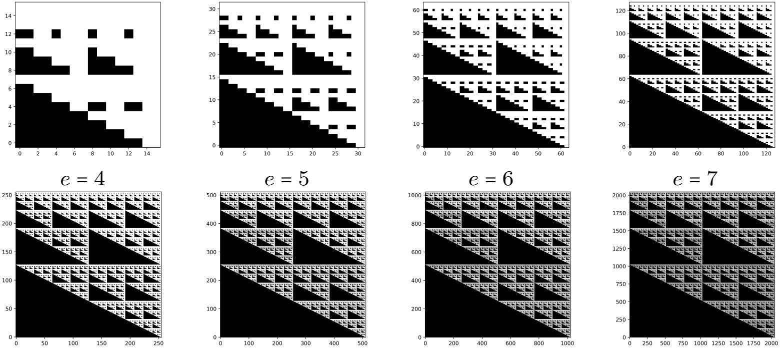
Information rate of $\mathrm{Lift}^\eta \mathrm{RS}_q(\alpha)$ when $q \to \infty$ and α is fixed

$\mathrm{Lift}^2(\mathrm{RS}(2^e - 3)$ on $\mathbb{F}_{2^e}$



Information rate of $\mathrm{Lift}^\eta \mathrm{RS}_q(\alpha)$ when $q \to \infty$ and α is fixed

$\mathrm{Lift}^2(\mathrm{RS}(2^e - 3)$ on $\mathbb{F}_{2^e}$



$e = 4$ | $e = 5$ | $e = 6$ | $e = 7$

$e = 8$ | $e = 9$ | $e = 10$ | $e = 11$

Theorem [L,N - 2019]

Let $\alpha \geq 2$, $\eta \geq 1$ and p be a prime number.
For each $e \in \mathbb{N}$, set $\mathcal{C}_e = \mathrm{Lift}^\eta \mathrm{RS}_{p^e}(p^e - \alpha)$.
Then, the information rate R_e of $\mathcal{C}_e$ approaches 1 when $e \to \infty$.

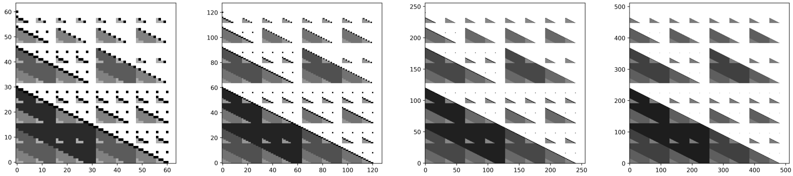
Information rate of $\mathrm{Lift}^{\eta}\,\mathrm{RS}_q(\lfloor \gamma q \rfloor)$ when $q \to \infty$ and γ is fixed

Theorem [L,N - 2019]

Let $c \geq 1$, $\eta \geq 1$ and p be a prime number. Fix $\gamma = 1 - p^{-c}$. For $e \geq c+1$, set $\mathcal{C}_e = \mathrm{Lift}^{\eta}\,\mathrm{RS}_{p^e}(\gamma p^e)$. Then, the information rate R_e of $\mathcal{C}_e$ satisfies:

$$\lim_{e\to\infty} R_e \geq \frac{1}{2\eta} \sum_{\varepsilon=0}^{c-1} (p^{-\varepsilon} - p^{-c})^2 N_{\varepsilon}\,.$$

Degree set of $\mathrm{Lift}^2\,\mathrm{RS}_{2^e}(2^e - 2^{e-c})$ for $c = 4$.
Number of differents shades of grey $= c$.



$e = 5$ $\quad$ $e = 6$ $\quad$ $e = 7$ $\quad$ $e = 8$

Thank you for your attention!