Weighted Reed-Muller codes: local decoding properties, applications to Private Information Retrieval and lift

Julien Lavauzelle, **Jade Nardi**

Institut de recherche mathématique de Rennes
INRIA Saclay

17/10/2019

Partially funded by ANR *Manta*

Weighted Projective Reed-Muller codes and η-lines

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

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

Rk: $\mathrm{WRM}_q^\eta(d) = \mathrm{RM}_q(2, d)$.

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

$$\mathrm{WRM}_q^\eta(d) = \langle \widetilde{\mathrm{ev}}(X_0^{d-i-\eta j} X_1^i X_2^j),\ (i,j) \in \mathbb{N}^2 \mid i + \eta j \leq d \rangle$$

Weighted Projective Reed-Muller codes and η-lines

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

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

Rk: $\mathrm{WRM}_q^{\eta}(d) = \mathrm{RM}_q(2, d)$.

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

$$\mathrm{WRM}_q^{\eta}(d) = \langle \widetilde{\mathrm{ev}}(X_0^{d-i-\eta j} X_1^i X_2^j),\ (i,j) \in \mathbb{N}^2 \mid i + \eta j \leq d \rangle$$

Aim: Highlight some local decoding properties

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:

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

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

Lemma

Any polynomial $f \in \mathbb{F}_q[X,Y]$ with $\deg_{(1,\eta)} \leq d$ 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 $i + \eta j \leq d$.
$\forall\ \phi \in \Phi_\eta$, $(f \circ L_\phi)(T) = T^i \phi(T)^j$ 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

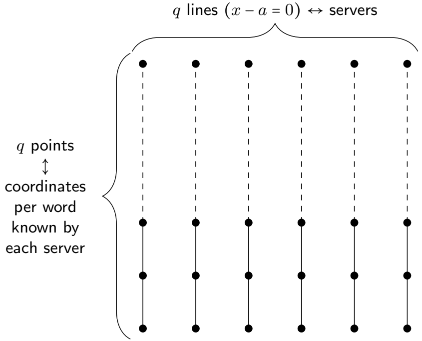
How to retrieve a datum stored on servers without giving any information about it?

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

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

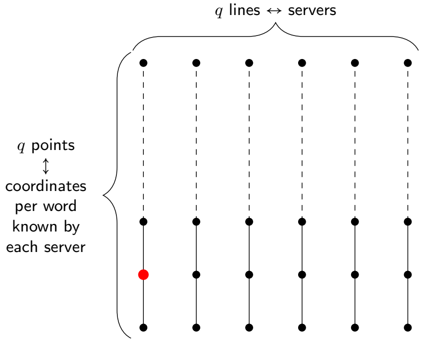
$\mathbb{A}^2(\mathbb{F}_q) = \bigsqcup_{i=1}^{q} L_i(\mathbb{F}_q)$

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



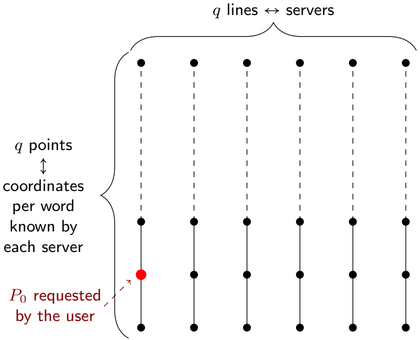
PIR Protocol linked to $\mathrm{WRM}_q^\eta(d)$

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 $\mathrm{WRM}_q^\eta(d)$

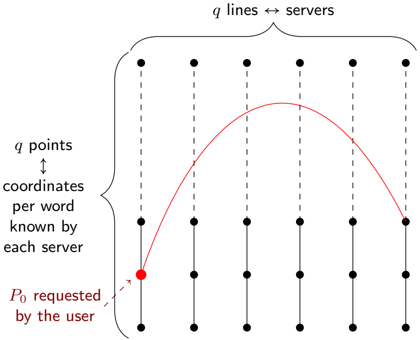
1. Word of $\mathrm{WRM}_q^\eta(d)$ restricted along an η-line = codeword of $\mathrm{RS}_q(d)$
2. An η-line meets each line $x = a$ at a unique point.



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.

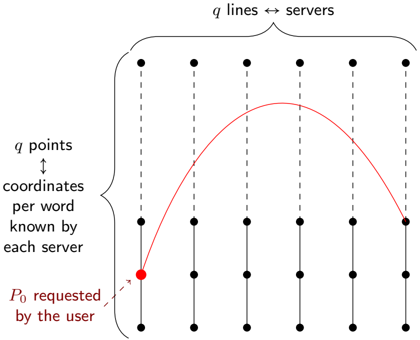


Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

Randomly pick an η-line L containing P_0.

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.

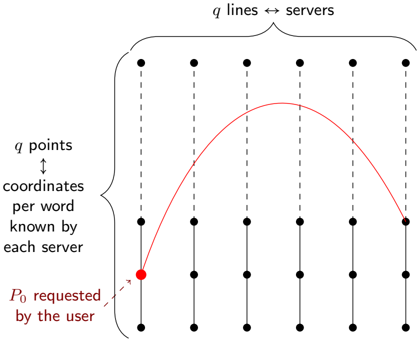


Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

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.

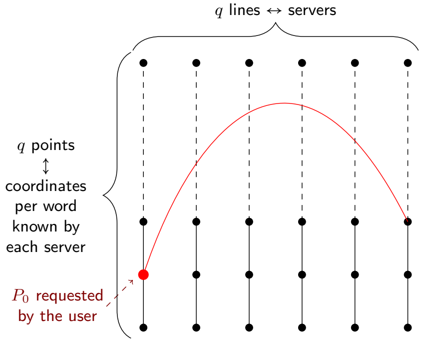


Wanted datum: c_{P_0}
with $c \in \mathrm{WRM}_q^\eta(d)$
and $d < q - 2$.

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

$\Rightarrow$ Word of RS(d) with 1 error = easily correctable!

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)
Because restricting a word of $\mathrm{RM}_q(2, d)$ along a line gives a word of $\mathrm{RS}_q(d)$.

Why take $\eta > 1$?

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)
Because restricting a word of $\mathrm{RM}_q(2,d)$ along a line gives a word of $\mathrm{RS}_q(d)$.

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

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

What's new?

Case $\eta = 1$ already known (PIR protocol from locally decodable codes)
Because restricting a word of $\mathrm{RM}_q(2,d)$ along a line gives a word of $\mathrm{RS}_q(d)$.

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)
Because restricting a word of $\mathrm{RM}_q(2,d)$ along a line gives a word of $\mathrm{RS}_q(d)$.

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

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

$\eta = 1 \Rightarrow$ 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)
Because restricting a word of $\mathrm{RM}_q(2, d)$ along a line gives a word of $\mathrm{RS}_q(d)$.

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 $d = 2$. $\mathrm{WRM}_q^\eta(d,(1) = \langle \mathrm{ev}(X^iY^j)\rangle$ 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 $t \in \mathbb{F}_4$,

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

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

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 $t \in \mathbb{F}_4$,

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

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

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

Two phenomena:

❶ Vanishing coefficients in characteristic p,

❷ $t^q = t$ for $t \in \mathbb{F}_q$.

Strategy to handle $\mathrm{Lift}^{\eta}(\mathrm{RS}_q(d))$

1. Vanishing coefficients in characteristic p.
   In the previous example, on $\mathbb{F}_4$,

$$(aT^2 + bT + c)^2 = a^2T^4 + b^2T^2 + c^2$$

   $\Rightarrow$ No monomials of odd power.

Strategy to handle $\mathrm{Lift}^{\eta}(\mathrm{RS}_q(d))$

1. Vanishing coefficients in characteristic p.
   In the previous example, on $\mathbb{F}_4$,

$$(aT^2 + bT + c)^2 = a^2T^4 + b^2T^2 + c^2$$

   $\Rightarrow$ No monomials of odd power.

   Strategy:
   Determining the monomials X^iY^j s.t. $\mathrm{ev}(T^i\phi(T)^j) \in \mathrm{RS}_q(d)$.

   1st step:
   Which monomials appear in $\phi(T)^j$ when $\deg(\phi) \leq \eta$ for a fixed j ?

Fix $\phi(T) = \sum_{m=0}^{\eta} a_m T^m \in \mathbb{F}_q[T]$. The multinomial theorem gives

$$\phi(T)^j = \sum_{k_1+\cdots+k_\eta \le j} \underbrace{\binom{j}{\mathbf{k}}}_{\text{multinomial coeff.}} \lambda_{\mathbf{k}} T^{k_1+2k_2+\cdots+\eta k_\eta},$$

where $\lambda_{\mathbf{k}}$ only depends on $a_0, \dots, a_\eta$ and $\mathbf{k}$.

Fix $\phi(T) = \sum_{m=0}^{\eta} a_m T^m \in \mathbb{F}_q[T]$. The multinomial theorem gives

$$\phi(T)^j = \sum_{k_1+\cdots+k_\eta \le j} \underbrace{\binom{j}{\mathbf{k}}}_{\text{multinomial coeff.}} \lambda_{\mathbf{k}} T^{k_1+2k_2+\cdots+\eta k_\eta},$$

where $\lambda_{\mathbf{k}}$ only depends on $a_0, \dots, a_\eta$ and $\mathbf{k}$.

$$\phi(T)^j = \sum_{\alpha \in \mathbb{N}} c_\alpha T^\alpha, \text{ with } c_\alpha = \sum_{\mathbf{k} \in K_\alpha} \binom{j}{\mathbf{k}} \lambda_{\mathbf{k}}$$

where

$$K_\alpha = \{\mathbf{k} \in \mathbb{N}^\eta \mid \sum_{\ell=1}^{\eta} k_\ell \le j \text{ and } \sum_{\ell=1}^{\eta} \ell k_\ell = \alpha\}.$$

Claim: $c_\alpha = 0$ for every $\phi \in \Phi_\eta$ **iif** $\binom{j}{\mathbf{k}} = 0$ for every $\mathbf{k} \in K_\alpha$.

The monomial T^α **appears** as a term of $\phi(T)^j$ **iif** there exists $\mathbf{k} \in K_\alpha$ s.t. $\binom{j}{\mathbf{k}} \neq 0$.

Recall: The monomial T^α **appears** in some $\phi(T)^j$ **iif**

$$\exists\, \mathbf{k} \in \mathbb{N}^\eta \text{ s.t. } |\mathbf{k}| \leq j \text{ and } \sum_{\ell=1}^{\eta} \ell k_\ell = \alpha,\ \binom{j}{\mathbf{k}} \neq 0,$$

where $\binom{j}{\mathbf{k}} = \binom{j}{k_1}\binom{j-k_1}{k_2}\binom{j-k_1-k_2}{k_3}\cdots\binom{j-k_1-k_2-\cdots-k_{\eta-1}}{k_\eta}$.

Recall: The monomial T^α **appears** in some $\phi(T)^j$ **iif**

$$\exists\, \mathbf{k} \in \mathbb{N}^\eta \text{ s.t. } |\mathbf{k}| \leq j \text{ and } \sum_{\ell=1}^{\eta} \ell k_\ell = \alpha, \binom{j}{\mathbf{k}} \neq 0,$$

where $\binom{j}{\mathbf{k}} = \binom{j}{k_1}\binom{j-k_1}{k_2}\binom{j-k_1-k_2}{k_3}\cdots\binom{j-k_1-k_2-\cdots-k_{\eta-1}}{k_\eta}$.

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

Order relation : $x \leq_p y \Leftrightarrow \forall\, i \in \mathbb{N}, x^{(i)} \leq y^{(i)}$. LT: $\binom{a}{b} \neq 0 \Leftrightarrow b \leq_p a$.

The monomial T^α **appears** as a term of a $\phi(T)^j$ **iif** there exists $\mathbf{k} \in \mathbb{N}^\eta$ such that $\alpha = \sum_{\ell=1}^{\eta} \ell k_\ell$ and

$$\forall m \in [1, \eta], k_m \leq_p j - \sum_{\ell=1}^{m-1} k_\ell.$$

Recall: $a^{(r)}$ is the r^{th} digit of the representation of a in base p.

Lemma

Fix $j \in \mathbb{N}$. For any $\mathbf{k} \in \mathbb{N}^\eta$ such that $\sum_{\ell=1}^{\eta} k_\ell \leq j$, the following assertions are equivalent.

- $\forall m \in [1, \eta], k_m \leq_p j - \sum_{\ell=1}^{m-1} k_\ell,$
- $\forall m \in [1, \eta],\ \forall\, r \in \mathbb{N},\ \sum_{\ell=1}^{m} k_\ell^{(r)} \leq j^{(r)},$
- $\forall\, r \in \mathbb{N},\ \sum_{\ell=1}^{\eta} k_\ell^{(r)} \leq j^{(r)}.$

Two phenomena:

1. Vanishing coefficients in characteristic p

Two phenomena:

1. Vanishing coefficients in characteristic p

   The monomials appearing in some $\phi(T)^j$ are those of the form $T^{\sum_{\ell=1}^{\eta} \ell k_\ell}$ for $\mathbf{k} \in \mathbb{N}^\eta$ such that

$$\forall\, r \in \mathbb{N},\ \sum_{\ell=1}^{\eta} k_\ell^{(r)} \le j^{(r)}.$$

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

Two phenomena:

1. Vanishing coefficients in characteristic p

   The monomials appearing in some $\phi(T)^j$ are those of the form $T^{\sum_{\ell=1}^{\eta} \ell k_\ell}$ for $\mathbf{k} \in \mathbb{N}^\eta$ such that

$$\forall\, r \in \mathbb{N},\ \sum_{\ell=1}^{\eta} k_\ell^{(r)} \leq j^{(r)}.$$

2. $t^q = t$ for $t \in \mathbb{F}_q$ $\Rightarrow$ Considering polynomials modulo $T^q - T$

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

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

   In other words, $\mathrm{Red}_q^\star(a)$ is the remainder of a modulo $q-1$ unless a is a non-zero multiple of $q-1$. In this case, $\mathrm{Red}_q^\star(a) = q - 1$.

Two phenomena:

1. Vanishing coefficients in characteristic p

   The monomials appearing in some $\phi(T)^j$ are those of the form $T^{\sum_{\ell=1}^{\eta} \ell k_\ell}$ for $\mathbf{k} \in \mathbb{N}^\eta$ such that

$$\forall\, r \in \mathbb{N},\ \sum_{\ell=1}^{\eta} k_\ell^{(r)} \leq j^{(r)}.$$

2. $t^q = t$ for $t \in \mathbb{F}_q$ $\Rightarrow$ Considering polynomials modulo $T^q - T$

   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 $\mathrm{Red}_q^\star(a)$.

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

   In other words, $\mathrm{Red}_q^\star(a)$ is the remainder of a modulo $q-1$ unless a is a non-zero multiple of $q-1$. In this case, $\mathrm{Red}_q^\star(a) = q-1$.

   Fix $P(T) = \sum c_m T^m$.
   $\mathrm{ev}_{\mathbb{F}_q}(P(T)) \in \mathrm{RS}_q(d)$ **iif** $\mathrm{Red}_q^\star(m) \leq d$ for every m s.t. $c_m \neq 0$.

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

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

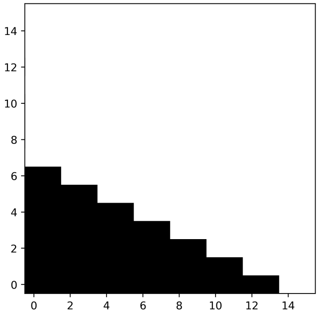
Only interesting when $d < q-1$ since $\mathrm{RS}_q(q-1)$ is trivial.

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 $\{0,\dots,q-1\}^2$ → **Degree set**



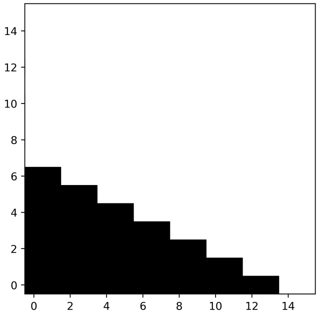
$\mathrm{WRM}^2_{16}(13)$

Total square are $=$ length / Black area $=$ dimension

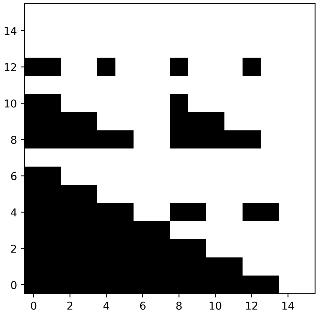
Representation of the monomials $x^i y^j$ whose evaluation belongs to $\mathrm{Lift}^\eta(\mathrm{RS}_q(d))$

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

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



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



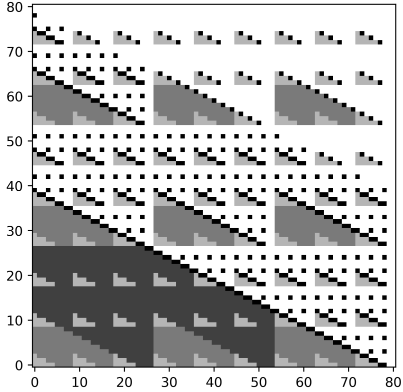
$\mathrm{Lift}^2(\mathrm{RS}_{16}(13))$

Total square are $=$ length / Black area $=$ dimension

How big can be our η-lifted codes ?

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

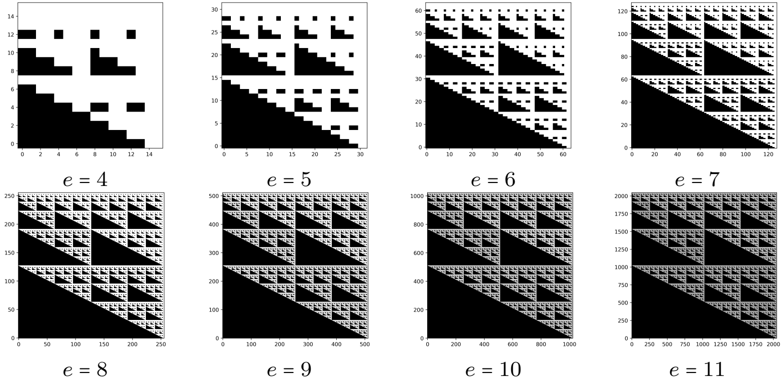
For a fixed $\alpha \geq 2$, the degree set of $\mathrm{Lift}^\eta \mathrm{RS}_q(q-\alpha)$ contains many copies of the degree set of $\mathrm{WRM}^\eta_{p^\varepsilon}(p^\varepsilon - \alpha - \eta)$, for $\varepsilon \leq e$.



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

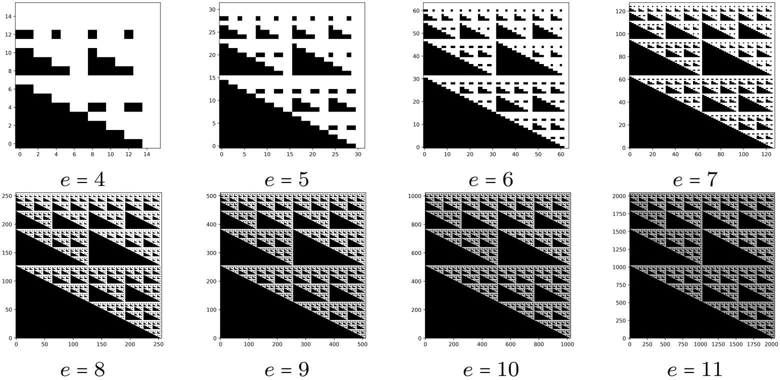
Information rate of $\mathrm{Lift}^\eta \mathrm{RS}_q(q-\alpha)$ when $q \to \infty$ and α is fixed

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



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

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



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 $e \to \infty$.

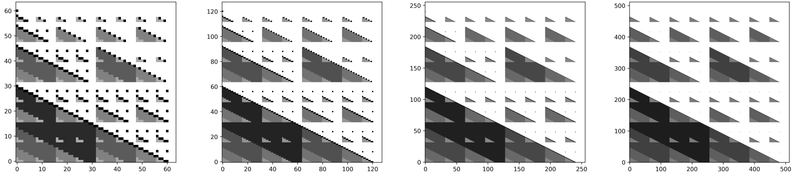
Information rate of $\mathrm{Lift}^{\eta}\,\mathrm{RS}_q(\lfloor \gamma q \rfloor)$ when $q \to \infty$ and γ is fixed

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.



$e = 5$ $e = 6$ $e = 7$ $e = 8$

Thank you for your attention!