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 $\eta$-lines

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

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

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

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

$$\text{WRM}_q^\eta(d) = \langle \text{ev}(X_0^{d-i-\eta j} X_1^i X_2^j), (i, j) \in \mathbb{N}^2 | i + \eta j \leq d \rangle$$
Fix $\eta \in \mathbb{N}^*$. Consider the plane weighted Reed-Muller code of weight $(1, \eta)$:

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

**Rk:** $\text{WRM}_q^n(d) = \text{RM}_q(2, d)$.

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

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

**Aim:** Highlight some local decoding properties

### Definition ($\eta$-line)

(Non-vertical) $\eta$-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 $\phi \in F_q[X_0, X_1]_h \text{ and } \deg \phi = \eta$.

- on $\mathbb{A}^2$: Set of zeroes of $P(x, y) = y - \phi(x)$, where $\phi \in F_q[X] \text{ and } \deg \phi \leq \eta$. 

---

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

Julien Lavauzelle, Jade Nardi
Recalls:

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

Parametrization of an \(\eta\)-line: \(t \mapsto (t, \phi(t))\)

Set of embeddings of \(\eta\)-lines into the affine plane \(\mathbb{A}^2\):

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

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

Parametrization of an \( \eta \)-line: \( t \mapsto (t, \phi(t)) \)

Set of embeddings of \( \eta \)-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 \( \text{ev}(f \circ L) \in \text{RS}_q(d) \) 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

Lifting process

Asymtotically good families of codes

PIR Protocol

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

Aim of Private Information Retrieval protocols [Augot, Levy-dit-Vehel, Shikfa (2014)] Share the database on several servers.

\[ \mathbb{F}_q[i \rightarrow \mathbb{F}_q(i)] = \]

Database: Codewords of Weighted Reed-Muller codes \( \eta_q(d) \) shared by \( q \) servers.

\( q \) points \( \downarrow \) coordinates per word known by each server

\( q \) lines \( (x-a=0) \leftrightarrow \) servers

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

Julien Lavauzelle, Jade Nardi
How to retrieve a datum stored on servers without giving any information about it?

\[ \sim \text{Aim of Private Information Retrieval protocols} \]
How to retrieve a datum stored on servers without giving any information about it?

→ Aim of Private Information Retrieval protocols

[Augot, Levy-dit-Vehel, Shikfa (2014)] Share the database on several servers.
How to retrieve a datum stored on servers without giving any information about it?

Aim of Private Information Retrieval protocols

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

\[ \mathbb{A}^2(\mathbb{F}_q) = \bigcup_{i=1}^{q} L_i(\mathbb{F}_q) \]

Database: Codewords of WRM\(^n_q\)(d) shared by q servers.

q lines \((x - a = 0) \leftrightarrow\) servers

q points
coordinates per word known by each server
1. Word of $\text{WRM}_q^n(d)$ restricted along an $\eta$-line = codeword of $\text{RS}_q(d)$
2. An $\eta$-line meets each line $x = a$ at a unique point.
1. Word of $\text{WRM}_q^n(d)$ restricted along an $\eta$-line = codeword of $\text{RS}_q(d)$

2. An $\eta$-line meets each line $x = a$ at a unique point.

Wanted datum: $c_{P_0}$ with $c \in \text{WRM}_q^n(d)$ and $d < q - 2$. 
1. Word of $\text{WRM}_q^n(d)$ restricted along an $\eta$-line = codeword of $\text{RS}_q(d)$
2. An $\eta$-line meets each line $x = a$ at a unique point.

Randomly pick an $\eta$-line $L$ containing $P_0$.

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

$q$ lines $\leftrightarrow$ servers

$q$ points
coordinates per word
known by each server

$P_0$ requested by the user
① Word of $\text{WRM}_q^n(d)$ restricted along an $\eta$-line = codeword of $\text{RS}_q(d)$
② An $\eta$-line meets each line $x = \alpha$ at a unique point.

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

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

Weighted Reed-Muller codes: local decoding properties, applications to Private Information Retrieval and lift
Julien Lavauzelle, Jade Nardi
PIR Protocol linked to $\text{WRM}_q^n(d)$

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

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

Randomly pick an $\eta$-line $L$ containing $P_0$.
Server $\leftrightarrow$ line not containing $P_0$: ask for $c_{L \cap L}$
Server $\leftrightarrow$ line containing $P_0$: ask for $c_{P_1}$ for $P_1$ random on this line
**PIR Protocol linked to \( \text{WRM}_q^n(d) \)**

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

Randomly pick an \( \eta \)-line \( L \) containing \( P_0 \).
Server \( \leftrightarrow \) line not containing \( P_0 \): ask for \( c_{L_i \cap L} \)
Server \( \leftrightarrow \) line containing \( P_0 \): ask for \( c_{P_1} \) for \( P_1 \) random on this line
\[ \Rightarrow \text{Word of RS}(d) \text{ with } 1 \text{ error} = \text{easily correctable!} \]
Case $\eta = 1$ already known (PIR protocol from locally decodable codes)
Because restricting a word of $RM_q(2, d)$ along a line gives a word of $RS_q(d)$.

**Why take** $\eta > 1$?
Case $\eta = 1$ already known (PIR protocol from locally decodable codes)
Because restricting a word of $RM_q(2, d)$ along a line gives a word of $RS_q(d)$.

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

$\eta$-line $\leftrightarrow$ Polynomial $\phi \in \mathbb{F}_q[X]$ with $\deg(\phi) \leq \eta$. 
Case $\eta = 1$ already known (PIR protocol from locally decodable codes)
Because restricting a word of $\text{RM}_q(2, d)$ along a line gives a word of $\text{RS}_q(d)$.

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

$\eta$-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 $\eta$ servers!
Case $\eta = 1$ already known (PIR protocol from locally decodable codes) 
Because restricting a word of $RM_q(2, d)$ along a line gives a word of $RS_q(d)$.

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

$\eta$-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 $\eta$ servers!

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

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

$\eta$-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 $\eta$ servers!

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

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

decreases as $\eta$ grows $\Rightarrow$ Loss of storage when $\eta$ grows.
Can we enhance the dimension while keeping the resistance to collusions?

Only property useful to the PIR protocol:
Restricting words along $\eta$-lines gives RS$(d)$ codewords.
Can we enhance the dimension while keeping the resistance to collusions?

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

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

**Definition ($\eta$-lifting of a Reed-Solomon code)**

Let $q$ be a prime power. The $\eta$-lifting of the Reed-Solomon code $RS_q(d)$ is the code of length $n = q^2$ defined as follows:

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

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

Of course, $\text{WRM}^\eta_q(d) \subset \text{Lift}^\eta RS_q(d)$.

**Question:** $\text{WRM}^\eta_q(d) \nsubset \text{Lift}^\eta RS_q(d)$?
Example of $\text{WRM}_q^n(d) \nless \text{Lift}_q^n(\text{RS}_q(d))$

Let $q = 4$, $\eta = 2$ and $d = 2$. $\text{WRM}_q^n(d, (1) = \langle \text{ev}(X^iY^j) \rangle$ with $(i, j) \in \{(0, 0), (0, 1), (1, 0), (2, 0)\}$.

Take $f(X, Y) = Y^2 \in \mathbb{F}_4[X, Y] \setminus \text{WRM}_4^2(2)$.

$\eta$-line: $L(T) = (T, aT^2 + bT + c) \in \Phi_2$, with $a, b, c \in \mathbb{F}_4$.

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

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

$\Rightarrow \text{ev}_{\mathbb{F}_4}(f \circ L) \in \text{RS}_4(2)$ for every $L \in \Phi_2$. 
Example of $\text{WRM}_q^n(d) \not\subset \text{Lift}^n(\text{RS}_q(d))$

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

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

Take $f(X, Y) = Y^2 \in \mathbb{F}_4[X, Y] \setminus \text{WRM}_4^2(2)$.

$\eta$-line: $L(T) = (T, aT^2 + bT + c) \in \Phi_2$, with $a, b, c \in \mathbb{F}_4$.

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

$$(f \circ L)(t) = (at^2 + bt + c)^2 \overset{1}{=} a^2 t^4 + b^2 t^2 + c^2 \overset{2}{=} b^2 t^2 + a^2 t + c.$$ 

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

$$\text{WRM}_4^2(2) \not\subset \text{Lift}^2(\text{RS}_4(2)).$$

Two phenomena:

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

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

Julien Lavauzelle, Jade Nardi
Strategy to handle $\text{Lift}^\eta(RS_q(d))$

   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 $\text{Lift}^\eta(\text{RS}_q(d))$

   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. $\text{ev}(T^i\phi(T)^j) \in \text{RS}_q(d)$.

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

$$\phi(T)^j = \sum_{k_1 + \cdots + k_\eta \leq j} \binom{j}{k} \lambda_k T^{k_1 + 2k_2 + \cdots + \eta k_\eta},$$

where $\lambda_k$ only depends on $a_0, \ldots, a_\eta$ and $k$. 

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

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

$$
\phi(T)^j = \sum_{k_1+\ldots+k_\eta \leq j} \binom{j}{k} \lambda_k T^{k_1+2k_2+\ldots+\eta k_\eta},
$$

where $\lambda_k$ only depends on $a_0, \ldots, a_\eta$ and $k$.

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

where

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

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

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

---

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

Julien Lavauzelle, Jade Nardi
Recall: The monomial $T^\alpha$ appears in some $\phi(T)^j$ if

$$\exists \, k \in \mathbb{N}^\eta \text{ s.t. } \left| k \right| \leq j \text{ and } \sum_{\ell=1}^{\eta} \ell k_\ell = \alpha, \left( \begin{array}{c} j \\ k \end{array} \right) \neq 0,$$

where

$$\left( \begin{array}{c} j \\ k \end{array} \right) = \left( \begin{array}{c} j \\ k_1 \end{array} \right) \left( \begin{array}{c} j - k_1 \\ k_2 \end{array} \right) \left( \begin{array}{c} j - k_1 - k_2 \\ k_3 \end{array} \right) \cdots \left( \begin{array}{c} j - k_1 - k_2 - \cdots - k_{\eta-1} \\ k_\eta \end{array} \right).$$
Recall: The monomial $T^\alpha$ 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: $x \leq_p y \iff \forall i \in \mathbb{N}, x^{(i)} \leq y^{(i)}$. LT: $\binom{a}{b} \neq 0 \iff b \leq_p a$.

The monomial $T^\alpha$ 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 $k \in \mathbb{N}^\eta$ such that $\sum_{\ell=1}^\eta k_\ell \leq j$, the following assertions are equivalent.

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

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

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

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

Julien Lavauzelle, Jade Nardi
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 \( T^{\sum_{\ell=1}^n \ell k_\ell} \) for \( k \in \mathbb{N}^n \) such that

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

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 $T^{\sum_{\ell=1}^{n} \ell k_\ell}$ for $k \in \mathbb{N}^n$ such that

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

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 $\text{Red}_q^*(a)$.

   $$(q-1 \mid \text{Red}_q^*(a) - a) \text{ and } (\text{Red}_q^*(a) = 0 \iff a = 0)$$

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

Weighted Reed-Muller codes: local decoding properties, applications to Private Information Retrieval and lift Julien Lavauzelle, Jade Nardi
Two phenomena:

1. **Vanishing coefficients in characteristic** $p$
   
   The monomials appearing in some $\phi(T)^j$ are those of the form $T^{\sum_{\ell=1}^{n} \ell k_\ell}$ for $k \in \mathbb{N}^n$ such that
   
   $$\forall r \in \mathbb{N}, \sum_{\ell=1}^{n} k_\ell^{(r)} \leq j^{(r)}.$$

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 $\text{Red}^*_q(a)$.
   
   $$(q - 1 \mid \text{Red}^*_q(a) - a) \text{ and } (\text{Red}^*_q(a) = 0 \iff a = 0)$$

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

Fix $P(T) = \sum c_m T^m$.

$\text{ev}_{\mathbb{F}_q}(P(T)) \in \text{RS}_q(d)$ **iff** $\text{Red}_q^*(m) \leq d$ for every $m$ s.t. $c_m \neq 0$. 

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

Julien Lavauzelle, Jade Nardi
Theorem [Lavauzelle, N - 2019]

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

\[
\text{Red}_q^* \left( i + \sum_{l=1}^{\eta} l k_l \right) \leq d.
\]

Only interesting when \( d < q - 1 \) since \( \text{RS}_q(q - 1) \) is trivial.
Theorem [Lavauzelle, N - 2019]

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

\[
\text{Red}_q^* \left( i + \sum_{l=1}^{\eta} lk_l \right) \leq d.
\]

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

**Question:** Is \( \text{Lift}^\eta(\text{RS}_q(d)) \) really bigger than \( \text{WRM}_q^\eta(d) \)?
Representatoin of the monomials $x^i y^j$ whose evaluation belongs to $\text{Lift}^\eta(\text{RS}_q(d))$

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

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

\[
\text{WRM}_2^{16}(13)
\]

Total square area = length / Black area = dimension
Remark: $i$ and $j$ can be assumed $\leq q - 1$.

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

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

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

Total square area = length / Black area = dimension

How big can be our $\eta$-lifted codes?
For a fixed $\alpha \geq 2$, the degree set of $\text{Lift}^\eta \text{RS}_q(q - \alpha)$ contains many copies of the degree set of $\text{WRM}^\eta_{p^\varepsilon} (p^\varepsilon - \alpha - \eta)$, for $\varepsilon \leq e$. 

$Lift^2(\text{RS}_{3^4}(3^4 - 3))$
Theorem [L,N - 2019]

Let $\alpha \geq 2$, $\eta \geq 1$ and $p$ be a prime number. For each $e \in \mathbb{N}$, set $C_e = \text{Lift}^\eta \text{RS}_p(e)(p^e - \alpha)$. Then, the information rate $R_e$ of $C_e$ approaches 1 when $e \to \infty$.
Information rate of $\text{Lift}^\eta \text{RS}_q(q - \alpha)$ when $q \to \infty$ and $\alpha$ is fixed

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

Theorem [L,N - 2019]
Information rate of \( \text{Lift}^\eta \text{RS}_q(\lceil \gamma q \rceil) \) when \( q \to \infty \) and \( \gamma \) 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 \( C_e = \text{Lift}^\eta \text{RS}_{pe}(\gamma p^e) \). Then, the information rate \( R_e \) of \( C_e \) 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 \( \text{Lift}^2 \text{RS}_{2e}(2^e - 2^{e-c}) \) for \( c = 4 \).

Number of different shades of grey = \( c \).

\[e = 5\]  \[e = 6\]  \[e = 7\]  \[e = 8\]
Thank you for your attention!