Linearized Polynomial Modules and their Application to Network Coding

Anna-Lena Horlemann-Trautmann

Algorithmics Laboratory
EPF Lausanne, Switzerland

October 18th, 2016
Clemson University
1 Linearized Polynomials
   - The Ring $\mathcal{L}_q(x, q^m)$
   - Modules over $\mathcal{L}_q(x, q^m)$

2 Network Coding and Gabidulin Codes
   - Introduction
   - Gabidulin Codes and Interpolation Decoding

3 Summary and Conclusion
Brief Recap of Finite Fields

- $\mathbb{F}_q$ exists (uniquely) for $q = p^r$, $p$ prime
- $\mathbb{F}_p \cong \mathbb{Z}_p$
- $\mathbb{F}_{q^m} \cong \mathbb{F}_q[\alpha]$, $\alpha$ root of irreducible polynomial of degree $m$
- Freshman’s Dream: $(a + b)^q = a^q + b^q$ for $a, b \in \mathbb{F}_{q^m}$
- $a^q = a$ for $a \in \mathbb{F}_q \leq \mathbb{F}_{q^m}$
Definition

A (q-)linearized polynomial is of the form

\[ f(x) = \sum_{i=0}^{n} a_i x^{q^i} \]

for \( a_i \in \mathbb{F}_{q^m} \). If \( a_n \neq 0 \), \( n \) is called the q-degree of \( f(x) \).
Definition

A \emph{(q-)linearized polynomial} is of the form

\[ f(x) = \sum_{i=0}^{n} a_i x^{q^i} \]

for \( a_i \in \mathbb{F}_{q^m} \). If \( a_n \neq 0 \), \( n \) is called the \emph{q-degree} of \( f(x) \).

Theorem

The set \( \mathcal{L}_q(x, q^m) \) of all \( q \)-linearized polynomials over \( \mathbb{F}_{q^m} \) forms a non-commutative ring, equipped with the normal addition + and composition (symbolic multiplication) \( \circ \).
Example in $\mathcal{L}_3(x, 3^2)$

- $\mathbb{F}_{3^2} \cong \mathbb{F}_3[\alpha]$, where $\alpha^2 + 1 = 0$
- $(2x^3 + x) + (\alpha x^9 + x^3) = \alpha x^9 + x$
- $(2x^3 + x) \circ (\alpha x^9 + x^3) = 2(\alpha x^9 + x^3)^3 + (\alpha x^9 + x^3)$
  $= 2\alpha^3 x^{27} + (2 + \alpha)x^9 + x^3 = \alpha x^{27} + (2 + \alpha)x^9 + x^3$
- $(\alpha x^9 + x^3) \circ (2x^3 + x) = \alpha(2x^3 + x)^9 + (2x^3 + x)^3$
  $= 2\alpha x^{27} + (2 + \alpha)x^9 + x^3$
Symbolic division:

- $f(x)$ is (symbolically) divisible on the left by $g(x)$ with quotient $m(x)$ if

$$g(x) \circ m(x) = f(x)$$

- $f(x)$ is (symbolically) divisible on the right by $g(x)$ with quotient $m(x)$ if

$$m(x) \circ g(x) = f(x)$$

- Left division with remainder: for any $f(x), g(x)$ we have

$$f(x) = g(x) \circ m(x) + r(x), \quad \text{qdeg}(r) < \text{qdeg}(g)$$

- Right division with remainder: for any $f(x), g(x)$ we have

$$f(x) = m(x) \circ g(x) + r(x), \quad \text{qdeg}(r) < \text{qdeg}(g)$$
A linearized polynomial $f(x) \in \mathcal{L}_q(x, q^m)$ is an $\mathbb{F}_q$-linear map. If $q\text{deg}(f) = k$, then $\ker(f)$ is a $k$-dimensional $\mathbb{F}_q$-vector space (over some extension field).
Linearized Polynomial Modules and their Application to Network Coding

Linearized Polynomials

The Ring $\mathcal{L}_q(x, q^m)$

**Theorem**

A linearized polynomial $f(x) \in \mathcal{L}_q(x, q^m)$ is an $\mathbb{F}_q$-linear map. If $q\text{deg}(f) = k$, then $\ker(f)$ is a $k$-dimensional $\mathbb{F}_q$-vector space (over some extension field).

**Example in $\mathcal{L}_3(x, 3^2)$**

- $f(x) = x^3 + 2\alpha^2 x$
- $f(\lambda x + \mu y) = (\lambda x + \mu y)^3 + 2\alpha^2(\lambda x + \mu y) = \lambda x^3 + \mu y^3 + 2\alpha^2 \lambda x + 2\alpha^2 \mu y = \lambda(x^3 + 2\alpha^2 x) + \mu(y^3 + 2\alpha^2 y) = \lambda f(x) + \mu f(y)$, for $\lambda, \mu \in \mathbb{F}_3$
- $\ker(f) = \{0, \alpha, 2\alpha\}$
Two special linearized polynomials

- Let \( g = (g_1, \ldots, g_n), r = (r_1, \ldots, r_n) \in \mathbb{F}_q^n \).
- Annihilator polynomial:
  \[
  \Pi_g(x) := \prod_{\beta \in \langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q}} (x - \beta)
  \]
- \( q \)-Lagrange polynomial:
  \[
  \Lambda_{g,r}(x) := \sum_{i=1}^{n} (-1)^{n-i} r_i \frac{\det(D_i(g, x))}{\det(M_n(g))}
  \]

**Theorem**

- \( \Pi_g(x) \in \mathcal{L}_q(x, q^m) \) and \( \Pi_g(g_i) = 0 \) for \( i = 1, \ldots, n \)
- \( \text{qdeg}(\Pi_g(g_i)) = \text{dim} \langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q} \)
- \( \Lambda_{g,r}(x) \in \mathcal{L}_q(x, q^m) \) and \( \Lambda_{g,r}(g_i) = r_i \) for \( i = 1, \ldots, n \)
- \( \text{qdeg}(\Lambda_{g,r}(x)) = \text{dim} \langle g_1, \ldots, g_n \rangle_{\mathbb{F}_q} - 1 \)
1 Linearized Polynomials
   - The Ring $\mathcal{L}_q(x, q^m)$
   - Modules over $\mathcal{L}_q(x, q^m)$

2 Network Coding and Gabidulin Codes
   - Introduction
   - Gabidulin Codes and Interpolation Decoding

3 Summary and Conclusion
Linearized Polynomial Modules and their Application to Network Coding

**Linearized Polynomials**

Modules over $\mathcal{L}_q(x, q^m)$

**Left Module** $\mathcal{L}_q(x, q^m)^\ell$

- for $f_i(x) \in \mathcal{L}_q(x, q^m)$, the elements of $\mathcal{L}_q(x, q^m)^\ell$ are

\[
\mathbf{f} := [f_1(x) \ldots f_\ell(x)] = \sum_{i=1}^{\ell} f_i(x)e_i
\]

- for $h(x) \in \mathcal{L}_q(x, q^m)$

\[
h(x) \circ \mathbf{f} := [h(f_1(x)) \ldots h(f_\ell(x))] = \sum_{i=1}^{\ell} h(f_i(x))e_i.
\]

**Definition**

A subset $M \subseteq \mathcal{L}_q(x, q^m)^\ell$ is a *(left) submodule* of $\mathcal{L}_q(x, q^m)^\ell$ if it is closed under addition and composition with $\mathcal{L}_q(x, q^m)$ on the left.
Definition

Consider \( f^{(1)}, \ldots, f^{(s)} \in \mathcal{L}_q(x, q^m)^\ell \). \( f^{(1)}, \ldots, f^{(s)} \) are linearly independent if for any \( a_1(x), \ldots, a_s(x) \in \mathcal{L}_q(x, q^m) \)

\[
\sum_{i=1}^{s} a_i(x) \circ f^{(i)} = [0 \ldots 0] \quad \implies \quad a_1(x) = \cdots = a_s(x) = 0.
\]

A generating set of a submodule \( M \subseteq \mathcal{L}_q(x, q^m)^\ell \) is called a basis of \( M \) if all its elements are linearly independent.
Monomials

- Notation: $[i] := q^i$
- The monomials of $\mathbf{f} = [f_1(x) \ldots f_\ell(x)]$ are of the form $x^{[k]}e_i$ for all $k$ such that $f_{ik} \neq 0$.
- A monomial order $<$ on $\mathcal{L}_q(x, q^m)\ell$ is a total order on $\mathcal{L}_q(x, q^m)\ell$, analogous to normal polynomial ring.
- The $(k_1, \ldots, k_\ell)$-weighted term-over-position monomial order is defined as

$$x^{[i_1]}e_{j_1} <_{(k_1, \ldots, k_\ell)} x^{[i_2]}e_{j_2} : \iff$$

$$i_1 + k_{j_1} < i_2 + k_{j_2} \text{ or } [i_1 + k_{j_1} = i_2 + k_{j_2} \text{ and } j_1 < j_2].$$
Definition

For any monomial order we define the following:

- the *leading monomial* \( \text{lm}(f) = x^{[i_1]}e_{j_1} \) is the greatest monomial of \( f \).
- the *leading position* \( \text{lpos}(f) = j_1 \) is the vector coordinate of the leading monomial.
- the *leading term* \( \text{lt}(f) = f_{j_1,i_1}x^{[i_1]}e_{j_1} \) is the complete term of the leading monomial.

The \( (k_1, \ldots, k_\ell) \)-weighted \( q \)-degree of \([f_1(x) \ldots f_\ell(x)]\) is defined as \( \max\{k_i + \text{qdeg}(f_i(x)) \mid i = 1, \ldots, \ell\} \).
Let \( f, h \in L_q(x, q^m) \ell \) and let \( F = \{f^{(1)}, \ldots, f^{(s)}\} \). We say that \( f \) reduces to \( h \) modulo \( F \) in one step if and only if

\[
h = f - ((b_1 x^{[a_1]}) \circ f^{(1)} + \cdots + (b_k x^{[a_k]}) \circ f^{(k)})
\]

for some \( a_1, \ldots, a_k \in \mathbb{N}_0 \) and \( b_1, \ldots, b_k \in \mathbb{F}_{q^m} \). We say that \( f \) is minimal with respect to \( F \) if it cannot be reduced modulo \( F \).

**Definition**

A module basis \( B \) is called minimal if all its elements \( b \) are minimal with respect to \( B \setminus \{b\} \).
Let $f, h \in \mathcal{L}_q(x, q^m)^\ell$ and let $F = \{f^{(1)}, \ldots, f^{(s)}\}$. We say that $f$ reduces to $h$ modulo $F$ in one step if and only if

$$h = f - ((b_1 x^{[a_1]}) \circ f^{(1)} + \cdots + (b_k x^{[a_k]}) \circ f^{(k)})$$

for some $a_1, \ldots, a_k \in \mathbb{N}_0$ and $b_1, \ldots, b_k \in \mathbb{F}_{q^m}$. We say that $f$ is minimal with respect to $F$ if it cannot be reduced modulo $F$.

**Definition**

A module basis $B$ is called minimal if all its elements $b$ are minimal with respect to $B \setminus \{b\}$.

**Theorem**

Let $B$ be a basis of a module $M \subseteq \mathcal{L}_q(x, q^m)^\ell$. Then $B$ is a minimal basis if and only if all leading positions of the elements of $B$ are distinct.
Example in \( \mathcal{L}_3(x, 3^2)^2 \)

- consider \((1, 2)\)-weighted TOP order and 

  \[ f = [x^3 + x \alpha x^3], \quad g = [2x^9 + x^3 \quad 2x] \]

- \(q\text{deg}_{(1,2)}(f) = \max(1 + 1, 1 + 2) = 3,\) 
  \(q\text{deg}_{(1,2)}(g) = \max(2 + 1, 0 + 2) = 3\)

- \(\text{lpos}(f) = 2, \quad \text{lpos}(g) = 1\)

- \(\text{lm}(f) = [0 \quad x^3], \quad \text{lm}(g) = [x^9 \quad 0]\)

- \(\text{lt}(f) = [0 \quad \alpha x^3], \quad \text{lt}(g) = [2x^9 \quad 0]\)
Example in $\mathcal{L}_3(x, 3^2)^2$

- consider $(1, 2)$-weighted TOP order and
  
  \[ f = [x^3 + x \ \alpha x^3], \quad g = [2x^9 + x^3 \ 2x] \]

- $q\text{deg}_{(1,2)}(f) = \max(1 + 1, 1 + 2) = 3$, $q\text{deg}_{(1,2)}(g) = \max(2 + 1, 0 + 2) = 3$

- $\text{lpos}(f) = 2$, $\text{lpos}(g) = 1$

- $\text{lm}(f) = [0 \ x^3], \text{lm}(g) = [x^9 \ 0]$

- $\text{lt}(f) = [0 \ \alpha x^3], \text{lt}(g) = [2x^9 \ 0]$

$\implies \{f, g\}$ is a minimal basis of

\[
\text{rowspan} \begin{bmatrix} x^3 + x & \alpha x^3 \\ 2x^9 + x^3 & 2x \end{bmatrix}
\]
Computation of minimal bases (EEA)

- Start with a basis \( \{ f^{(1)}, f^{(2)}, \ldots, f^{(s)} \} \subseteq \mathcal{L}_q(x, q^m) \ell \) of the module.
- Consider all elements with leading position 1 and reduce all but one of them such that they have leading position > 1.
- Consider all elements with leading position 2 and reduce all but one of them such that they have leading position > 2.
- etc.
- Receive another basis with all distinct leading positions.  
  \( \implies \) minimal basis!
Example in $\mathcal{L}_3(x, 3^2)^2$

- $f = [2x^{27} + x^9 + x^3 + x \ (\alpha + 2)x^3]$, $g = [2x^9 + x^3 \ 2x]$
- both have leading position 1 in $(1, 2)$-weighted order
- compute $h = f - x^3 \circ g = [x^3 + x \ \alpha x^3]$
- $h$ has leading position 2
- $\{g, h\}$ is minimal basis of $\langle f, g \rangle$
Let $M$ be a module in $\mathcal{L}_q(x, q^m)^\ell$ with minimal basis $B = \{b^{(1)}, \ldots, b^{(L)}\}$. Then for any $0 \neq f \in M$, written as

$$f = a_1(x) \circ b^{(1)} + \cdots + a_L(x) \circ b^{(L)},$$

where $a_1(x), \ldots, a_L(x) \in \mathcal{L}_q(x, q^m)$, we have

$$\text{lm}(f) = \max_{1 \leq i \leq L; a_i(x) \neq 0} \{\text{lm}(a_i) \circ \text{lm}(b^{(i)})\}$$

where $\text{lm}(a_i(x))$ is the term of $a_i(x)$ of highest $q$-degree.
Theorem (Predictable Leading Monomial Property)

Let $M$ be a module in $\mathcal{L}_q(x, q^m)^\ell$ with minimal basis $B = \{b^{(1)}, \ldots, b^{(L)}\}$. Then for any $0 \neq f \in M$, written as

$$f = a_1(x) \circ b^{(1)} + \cdots + a_L(x) \circ b^{(L)},$$

where $a_1(x), \ldots, a_L(x) \in \mathcal{L}_q(x, q^m)$, we have

$$\text{lm}(f) = \max_{1 \leq i \leq L; a_i(x) \neq 0} \{\text{lm}(a_i) \circ \text{lm}(b^{(i)})\}$$

where $\text{lm}(a_i(x))$ is the term of $a_i(x)$ of highest $q$-degree.

Corollary

The leading positions and weighted $q$-degrees of elements of two distinct minimal bases for the same module in $\mathcal{L}_q(x, q^m)^\ell$ have to be the same. $\implies$ cardinalities of minimal bases are equal.
The Interpolation Module

- Let \( \mathbf{g} = (g_1, \ldots, g_n), \mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{F}_{q^m}^n \).
- Remember: annihilator \( \Pi_{\mathbf{g}}(x) \), \( q \)-Lagrange \( \Lambda_{\mathbf{g}, \mathbf{r}}(x) \)
- Define the \textit{interpolation module}

\[
\mathcal{M}(\mathbf{g}, \mathbf{r}) = \text{rowspan} \begin{bmatrix} \Pi_{\mathbf{g}}(x) & 0 \\ -\Lambda_{\mathbf{g}, \mathbf{r}}(x) & x \end{bmatrix}
\]
The Interpolation Module

- Let \( g = (g_1, \ldots, g_n), r = (r_1, \ldots, r_n) \in \mathbb{F}_{q^m}^n \).
- Remember: annihilator \( \Pi_g(x) \), \( q \)-Lagrange \( \Lambda_{g,r}(x) \).
- Define the interpolation module

\[
\mathcal{M}(g, r) = \text{rowspan} \begin{bmatrix} \Pi_g(x) & 0 \\ -\Lambda_{g,r}(x) & x \end{bmatrix}
\]

**Theorem**

\( \mathcal{M}(g, r) \subseteq \mathcal{L}_q(x, q^m)^2 \) contains exactly all \( [f_1(x) \quad - f_2(x)] \) with

\[
f_1(g_i) - f_2(r_i) = 0.
\]
The Interpolation Module

- Let \( g = (g_1, \ldots, g_n), r = (r_1, \ldots, r_n) \in \mathbb{F}_{q^m}^n. \)
- Remember: annihilator \( \Pi_g(x), q\)-Lagrange \( \Lambda_{g,r}(x) \)
- Define the interpolation module

\[
\mathcal{M}(g, r) = \text{rowspan} \begin{bmatrix}
\Pi_g(x) & 0 \\
-\Lambda_{g,r}(x) & x
\end{bmatrix}
\]

**Theorem**

\( \mathcal{M}(g, r) \subseteq \mathcal{L}_q(x, q^m)^2 \) contains exactly all \( [f_1(x) - f_2(x)] \) with

\[ f_1(g_i) - f_2(r_i) = 0. \]

\( \implies \) minimal basis of \( \mathcal{M}(g, r) \) can be computed in \( \mathcal{O}_{q^m}(n^3) \) operations with EEA
1 Linearized Polynomials
   • The Ring $\mathcal{L}_q(x, q^m)$
   • Modules over $\mathcal{L}_q(x, q^m)$

2 Network Coding and Gabidulin Codes
   • Introduction
   • Gabidulin Codes and Interpolation Decoding

3 Summary and Conclusion
Classical coding theory (simple channel):

- codewords are vectors of length $n$ over a finite field $\mathbb{F}_q$
- received word = codeword + error vector ($r = c + e \in \mathbb{F}_q^n$)
- most likely sent codeword $\approx$ closest codeword w.r.t. \textit{Hamming distance}:

$$d_H((u_1, \ldots, u_n), (v_1, \ldots, v_n)) := |\{i \mid u_i \neq v_i\}|.$$
Classical coding theory (simple channel):

- codewords are vectors of length $n$ over a finite field $\mathbb{F}_q$
- received word = codeword + error vector ($r = c + e \in \mathbb{F}_q^n$)
- most likely sent codeword \( \cong \) closest codeword w.r.t. Hamming distance:

\[
d_H((u_1, \ldots, u_n), (v_1, \ldots, v_n)) := |\{i \mid u_i \neq v_i\}|.
\]
Classical coding theory (simple channel):

- codewords are vectors of length $n$ over a finite field $\mathbb{F}_q$
- received word = codeword + error vector ($r = c + e \in \mathbb{F}_q^n$)
- most likely sent codeword $\approx$ closest codeword w.r.t. *Hamming distance:*

\[
d_H((u_1, \ldots, u_n), (v_1, \ldots, v_n)) := |\{i \mid u_i \neq v_i\}|.
\]

yes = (111111)
no = (000000)
Multicast Channel

All receivers want to receive the same information.
Example (Butterfly Network)

*Linearly combining is better than forwarding:*

R1 receives only $a$, R2 receives $a$ and $b$.

- Forwarding: need 2 transmissions to transmit $a, b$ to both receivers
Example (Butterfly Network)

*Linearly combining is better than forwarding:*

R1 and R2 can both recover $a$ and $b$ with one operation.

- **Forwarding:** need 2 transmissions to transmit $a, b$ to both receivers
- **Linearly combining:** need 1 transmission to transmit $a, b$ to both receivers
It turns out that linear combinations at the inner nodes are “sufficient” to reach capacity:

**Theorem**

One can reach the capacity of a single-source multicast network channel with linear combinations at the inner nodes.
It turns out that linear combinations at the inner nodes are “sufficient” to reach capacity:

**Theorem**

One can reach the capacity of a single-source multicast network channel with linear combinations at the inner nodes.

**Problem:** Hamming metric does not reflect the number of errors in the network.
It turns out that linear combinations at the inner nodes are “sufficient” to reach capacity:

**Theorem**
One can reach the capacity of a single-source multicast network channel with linear combinations at the inner nodes.

**Problem:** Hamming metric does not reflect the number of errors in the network.

**Solution:** Use metric space \((\mathbb{F}_q^{m\times n}, d_R)\),

\[ d_R(A, B) = \text{rank}(A - B). \]
Definition

A rank-metric code is a subset of $\mathbb{F}_q^{m \times n}$. The minimum distance of $C \subseteq \mathbb{F}_q^{m \times n}$ is defined as

$$d_R(C) := \min \{ d_R(A, B) \mid A, B \in C, A \neq B \}.$$  

- For a codeword $A \in C$, error matrix $E \in \mathbb{F}_q^{m \times n}$ and channel operation matrix $M_c$, the channel output is

$$M_c A + E.$$  

- Decoding a received word $\cong$ finding the closest codeword w.r.t. $d_R$. 

Definition

A rank-metric code is a subset of $\mathbb{F}_q^{m \times n}$. The minimum distance of $C \subseteq \mathbb{F}_q^{m \times n}$ is defined as

$$d_R(C) := \min\{d_R(A, B) \mid A, B \in C, A \neq B\}.$$ 

- For a codeword $A \in C$, error matrix $E \in \mathbb{F}_q^{m \times n}$ and channel operation matrix $M_c$, the channel output is

$$M_cA + E.$$ 

- Decoding a received word $\approx$ finding the closest codeword w.r.t. $d_R$.

- The error correction capability of $C$ is $(d_R(C) - 1)/2$.

- The transmission rate of $C$ is $\log_q(|C|)/(mn)$. 
Definition

A rank-metric code is a subset of $\mathbb{F}_q^{m \times n}$. The minimum distance of $C \subseteq \mathbb{F}_q^{m \times n}$ is defined as

$$d_R(C) := \min\{d_R(A, B) \mid A, B \in C, A \neq B\}.$$  

- For a codeword $A \in C$, error matrix $E \in \mathbb{F}_q^{m \times n}$ and channel operation matrix $M_c$, the channel output is

$$M_c A + E.$$  

- Decoding a received word $\approx$ finding the closest codeword w.r.t. $d_R$.  
- The error correction capability of $C$ is $(d_R(C) - 1)/2$.  
- The transmission rate of $C$ is $\log_q(|C|)/(mn)$.  
- We can use $\mathbb{F}_q^{m \times n} \cong \mathbb{F}_q^{mn}$ and define $C \subseteq \mathbb{F}_q^{nm}$. 

1 Linearized Polynomials
   • The Ring $\mathcal{L}_q(x, q^m)$
   • Modules over $\mathcal{L}_q(x, q^m)$

2 Network Coding and Gabidulin Codes
   • Introduction
   • Gabidulin Codes and Interpolation Decoding

3 Summary and Conclusion
Definition

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. Then

$$C_{Gab} := \{(f(g_1), \ldots, f(g_n)) \mid f(x) \in \mathcal{L}_q(x, q^m), \text{qdeg} < k\}$$

is called a *Gabidulin code* in $\mathbb{F}_{q^m}$ of dimension $k$. 
**Definition**

Let $g_1, \ldots, g_n \in \mathbb{F}_{q^m}$ be linearly independent over $\mathbb{F}_q$. Then

$$C_{Gab} := \{(f(g_1), \ldots, f(g_n)) \mid f(x) \in \mathcal{L}_q(x, q^m), \text{qdeg} < k\}$$

is called a *Gabidulin code* in $\mathbb{F}^n_{q^m}$ of dimension $k$.

**Theorem**

A Gabidulin code $C \subseteq \mathbb{F}^n_{q^m}$ of dimension $k$ has minimum rank distance $n - k + 1$, which is optimal (Singleton bound). Therefore, it is called a *maximum rank distance (MRD) code*. 
Example:
Consider $\mathbb{F}_2^2 \cong \mathbb{F}_2[\alpha]$, with $\alpha^2 + \alpha + 1 = 0$. Fix $g_1 = 1$, $g_2 = \alpha$ (linearly independent). The Gabidulin code of length $n = 2$, dimension $k = 1$ and minimum distance $n - k + 1 = 2$ is

\begin{align*}
(0 & 0) \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad & f(x) = 0 \\
(1 & \alpha) \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad & f(x) = x \\
(\alpha & \alpha + 1) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad & f(x) = \alpha x \\
(\alpha + 1 & 1) \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad & f(x) = (\alpha + 1)x
\end{align*}
Interpolation Decoding:

- \( c = (f(g_1), \ldots, f(g_n)) \in \mathbb{F}_{q^m}^n \) codeword;
- \( r = c + e \in \mathbb{F}_{q^m}^n \) received word.

**Theorem**

\( d_R(c, r) = t \) if and only if there exists a \( D(x) \in \mathcal{L}_q(x, q^m) \), such that \( q\deg(D(x)) = t \) and

\[
D(f(g_i)) = D(r_i) \quad \forall i \in \{1, \ldots, n\}.
\]

This \( D(x) \) is called the *error span polynomial*. 
Interpolation Decoding:

- \( \mathbf{c} = (f(g_1), \ldots, f(g_n)) \in \mathbb{F}_{q^m}^n \) codeword;
- \( \mathbf{r} = \mathbf{c} + \mathbf{e} \in \mathbb{F}_{q^m}^n \) received word.

**Theorem**

\[ d_R(\mathbf{c}, \mathbf{r}) = t \text{ if and only if there exists a } D(x) \in \mathcal{L}_q(x, q^m), \text{ such that } q\deg(D(x)) = t \text{ and } \]

\[ D(f(g_i)) = D(r_i) \quad \forall i \in \{1, \ldots, n\}. \]

This \( D(x) \) is called the *error span polynomial*.

- Set \( N(x) := D(f(x)) \). Then \( N(g_i) - D(r_i) = 0. \)
- \( \implies [N(x) - D(x)] \in \mathcal{M}(\mathbf{g}, \mathbf{r}) \) (interpolation module)!
The elements \([N(x) - D(x)]\) of \(\mathfrak{M}(g, r)\) that fulfill

1. \(\text{qdeg}(N(x)) \leq t + k - 1\),
2. \(\text{qdeg}(D(x)) = t\),
3. \(N(x)\) is symbolically divisible on the left by \(D(x)\), i.e. there exists \(f(x) \in \mathcal{L}_q(x, q^m)\) such that \(D(f(x)) = N(x)\),

are in one-to-one correspondence with the codewords of rank distance \(t\) to \(r\).
The elements \([N(x) - D(x)]\) of \(\mathcal{M}(g, r)\) that fulfill

1. \(\text{qdeg}(N(x)) \leq t + k - 1\),
2. \(\text{qdeg}(D(x)) = t\),
3. \(N(x)\) is symbolically divisible on the left by \(D(x)\), i.e. there exists \(f(x) \in \mathcal{L}_q(x, q^m)\) such that \(D(f(x)) = N(x)\),

are in one-to-one correspondence with the codewords of rank distance \(t\) to \(r\).

The quotient is the respective message polynomial in \(\mathcal{L}_q(x, q^m)\).
The Parametrization:

**Goal:** Find all \([N(x) - D(x)] \in \mathcal{M}(r)\) with

1. \(\text{qdeg}(N(x)) \leq t + k - 1\),
2. \(\text{qdeg}(D(x)) = t\),
The Parametrization:

Goal: Find all \([N(x) - D(x)] \in \mathcal{M}(r)\) with

1. \(\text{qdeg}(N(x)) \leq t + k - 1\),
2. \(\text{qdeg}(D(x)) = t\),

Solution: If \(\{b_1, b_2\}\) is minimal basis (ordered by leading positions) with \(\ell_1, \ell_2\) the respective weighted row \(q\)-degrees, then

\[
\lambda(x) \circ b_1 + \mu(x) \circ b_2 \quad \text{with}
\]

1. \(\text{qdeg}(\lambda(x)) \leq t - \ell_1 + k - 1\),
2. \(\text{qdeg}(\mu(x)) = t - \ell_2 + k - 1\) and \(\mu(x)\) is monic

yield all the desired elements.
The Parametrization:

**Goal:** Find all \([N(x) - D(x)] \in \mathcal{M}(r)\) with

1. \(\text{qdeg}(N(x)) \leq t + k - 1,\)
2. \(\text{qdeg}(D(x)) = t,\)

**Solution:** If \(\{b_1, b_2\}\) is minimal basis (ordered by leading positions) with \(\ell_1, \ell_2\) the respective weighted row \(q\)-degrees, then

\[
\lambda(x) \circ b_1 + \mu(x) \circ b_2
\]

with

1. \(\text{qdeg}(\lambda(x)) \leq t - \ell_1 + k - 1,\)
2. \(\text{qdeg}(\mu(x)) = t - \ell_2 + k - 1\) and \(\mu(x)\) is monic

yield all the desired elements.

**Proof:** Based on the *Predictable Leading Monomial Property*. 
The Decoding Algorithm:

Precomputed and stored: $\Pi_g(x) \in \mathcal{L}_q(x, q^m)$ (annihilator)

Input: received word $r \in \mathbb{F}_{q^m}^n$

- Compute $q$-Lagrange polynomial $\Lambda_{g,r}(x)$.
- Compute a minimal basis $\{b_1, b_2\}$ of the interpolation module

$$\mathcal{M}(g, r) = \text{rowspan} \begin{bmatrix} \Pi_g(x) & 0 \\ -\Lambda_{g,r}(x) & x \end{bmatrix}.$$

- Check all elements of the form $\lambda(x) \circ b_1 + \mu(x) \circ b_2$ with restricted degrees of $\lambda(x), \mu(x) \in \mathcal{L}_q(x, q^m)$ for divisibility.

Output: the symbolic quotients (where existent)
The Decoding Algorithm:

Precomputed and stored: $\Pi_g(x) \in \mathcal{L}_q(x, q^m)$ (annihilator)

Input: received word $r \in \mathbb{F}_q^n$

- Compute $q$-Lagrange polynomial $\Lambda_{g, r}(x)$.
- Compute a **minimal basis** $\{b_1, b_2\}$ of the interpolation module

$$\mathcal{M}(g, r) = \text{rowspan} \begin{bmatrix} \Pi_g(x) & 0 \\ -\Lambda_{g, r}(x) & x \end{bmatrix}.$$ 

- Check all elements of the form $\lambda(x) \circ b_1 + \mu(x) \circ b_2$ with restricted degrees of $\lambda(x), \mu(x) \in \mathcal{L}_q(x, q^m)$ for divisibility.

Output: the symbolic quotients (where existent)
Example:
Consider the Gabidulin code $C$ over $\mathbb{F}_{2^3} \cong \mathbb{F}_2[\alpha]$ (with $\alpha^3 = \alpha + 1$) with generator matrix

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix}.$$ 

$$\implies d_R = n - k + 1 = 3 - 2 + 1 = 2$$

$$\implies C \text{ is no-error correcting}$$
Example:
Consider the Gabidulin code $C$ over $\mathbb{F}_{2^3} \cong \mathbb{F}_2[\alpha]$ (with $\alpha^3 = \alpha + 1$) with generator matrix

\[
G = \begin{pmatrix}
1 & \alpha & \alpha^2 \\
1 & \alpha^2 & \alpha^4
\end{pmatrix}.
\]

\[d_R = n - k + 1 = 3 - 2 + 1 = 2\]

\[\implies C\text{ is no-error correcting}\]

Received word:
\[
r = (\alpha + 1 \quad 0 \quad \alpha).
\]
Example:
Consider the Gabidulin code $C$ over $\mathbb{F}_{2^3} \cong \mathbb{F}_2[\alpha]$ (with $\alpha^3 = \alpha + 1$) with generator matrix

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix}.$$ 

$\implies d_R = n - k + 1 = 3 - 2 + 1 = 2$
$\implies C$ is no-error correcting

Received word:

$$r = (\alpha + 1 \ 0 \ \alpha).$$

Interpolation module:

$$\mathcal{M}(r) = \text{rowspan} \begin{bmatrix} \Pi g(x) & 0 \\ \Lambda_{g,r}(x) & x \end{bmatrix} = \text{rowspan} \begin{bmatrix} x^8 + x & 0 \\ \alpha^2 x^4 + \alpha^5 x & x \end{bmatrix}.$$
Finding the minimal basis with the Euclidean algorithm:

\[ x^8 + x = (\alpha^3 x^2) \circ (\alpha^2 x^4 + \alpha^5 x) + (\alpha^6 x^2 + x). \]

Since \( qdeg(\alpha^3 x^2) + k - 1 = 2 \geq 1 = qdeg(\alpha^6 x^2 + x) \), the algorithm terminates and a minimal basis (w.r.t. the \((0, 1)\)-weighted 2-degree) of this module is

\[
\begin{bmatrix}
0 & x \\
x & \alpha^3 x^2 \\
\end{bmatrix} \circ \begin{bmatrix}
x^8 + x & 0 \\
\alpha^2 x^4 + \alpha^5 x & x \\
\end{bmatrix} = \begin{bmatrix}
\alpha^2 x^4 + \alpha^5 x & x \\
\alpha^6 x^2 + x & \alpha^3 x^2 \\
\end{bmatrix}.
\]

original basis

minimal basis
Parametrization $\lambda(x) \circ b_1 + \mu(x) \circ b_2$:

Use all $\lambda(x) \in \mathcal{L}_2(x, 2^3)$ with 2-degree 0 and all monic $\mu(x) \in \mathcal{L}_2(x, 2^3)$ with 2-degree 0.

$$\implies \lambda(x) = a_0 x, \quad a_0 \in \mathbb{F}_{2^3}, \quad \text{and} \quad \mu(x) = x$$
Parametrization $\lambda(x) \circ b_1 + \mu(x) \circ b_2$:

Use all $\lambda(x) \in \mathcal{L}_2(x, 2^3)$ with 2-degree 0 and all monic $\mu(x) \in \mathcal{L}_2(x, 2^3)$ with 2-degree 0.

$$\implies \lambda(x) = a_0 x, \quad a_0 \in \mathbb{F}_{2^3}, \quad \text{and} \quad \mu(x) = x$$

E.g. for $a_0 = \alpha$:

$$(\alpha x) \circ [\alpha^2 x^4 + \alpha^5 x \quad x] + [\alpha^6 x^2 + x \quad \alpha^3 x^2]$$

$$= [\alpha^3 x^4 + \alpha^6 x \quad \alpha x] + [\alpha^6 x^2 + x \quad \alpha^3 x^2]$$

$$= [\alpha^3 x^4 + \alpha^6 x^2 + \alpha^2 x \quad \alpha^3 x^2 + \alpha x]$$
Parametrization $\lambda(x) \circ b_1 + \mu(x) \circ b_2$:

Use all $\lambda(x) \in \mathcal{L}_2(x, 2^3)$ with 2-degree 0 and all monic $\mu(x) \in \mathcal{L}_2(x, 2^3)$ with 2-degree 0.

$$\implies \lambda(x) = a_0 x, \quad a_0 \in \mathbb{F}_{2^3}, \quad \text{and} \quad \mu(x) = x$$

E.g. for $a_0 = \alpha$:

$$(\alpha x) \circ [\alpha^2 x^4 + \alpha^5 x \quad x] + [\alpha^6 x^2 + x \quad \alpha^3 x^2]$$

$$= [\alpha^3 x^4 + \alpha^6 x \quad \alpha x] + [\alpha^6 x^2 + x \quad \alpha^3 x^2]$$

$$= [\alpha^3 x^4 + \alpha^6 x^2 + \alpha^2 x \quad \alpha^3 x^2 + \alpha x]$$

Symbolic division:

$$\alpha^3 x^4 + \alpha^6 x^2 + \alpha^2 x = (\alpha^3 x^2 + \alpha x) \circ (x^2 + \alpha x)$$

message polynomial
We get divisibility for all $a_0 \in \mathbb{F}_{2^3}\backslash\{0\}$. Thus our list decoding algorithm finds the following list of message polynomials and corresponding codewords:

\[
\begin{align*}
m_1(x) &= x^2 + \alpha x & c_1 &= (\alpha + 1 \ 0 \ \alpha^2 + 1), \\
m_2(x) &= \alpha^5 x^2 + \alpha^2 x & c_2 &= (\alpha + 1 \ \alpha \ \alpha), \\
m_3(x) &= \alpha^3 x^2 + \alpha^4 x & c_3 &= (\alpha^2 + 1 \ 0 \ \alpha^2), \\
m_4(x) &= \alpha^4 x^2 & c_4 &= (\alpha^2 + \alpha \ \alpha^2 + 1 \ \alpha), \\
m_5(x) &= \alpha^6 x^2 + \alpha^6 x & c_5 &= (0 \ \alpha + 1 \ 1), \\
m_6(x) &= \alpha^2 x^2 + \alpha^3 x & c_6 &= (\alpha^2 + \alpha + 1 \ 0 \ \alpha), \\
m_7(x) &= \alpha x^2 + x & c_7 &= (\alpha + 1 \ 1 \ \alpha + 1).
\end{align*}
\]

All these codewords are rank distance 1 away from

\[
r = (\alpha + 1 \ 0 \ \alpha).
\]
We get divisibility for all $a_0 \in \mathbb{F}_{2^3}\{0\}$. Thus our list decoding algorithm finds the following list of message polynomials and corresponding codewords:

\[
\begin{align*}
m_1(x) &= x^2 + \alpha x & c_1 &= (\alpha + 1 \ 0 \ \alpha^2 + 1), \\
m_2(x) &= \alpha^5 x^2 + \alpha^2 x & c_2 &= (\alpha + 1 \ \alpha \ \alpha), \\
m_3(x) &= \alpha^3 x^2 + \alpha^4 x & c_3 &= (\alpha^2 + 1 \ 0 \ \alpha^2), \\
m_4(x) &= \alpha^4 x^2 & c_4 &= (\alpha^2 + \alpha \ \alpha^2 + 1 \ \alpha), \\
m_5(x) &= \alpha^6 x^2 + \alpha^6 x & c_5 &= (0 \ \alpha + 1 \ 1), \\
m_6(x) &= \alpha^2 x^2 + \alpha^3 x & c_6 &= (\alpha^2 + \alpha + 1 \ 0 \ \alpha), \\
m_7(x) &= \alpha x^2 + x & c_7 &= (\alpha + 1 \ 1 \ \alpha + 1).
\end{align*}
\]

All these codewords are rank distance 1 away from

\[
r = (\alpha + 1 \ 0 \ \alpha).
\]

Note: Hamming distance can be 1, 2 or 3.
Complexity:

- Computing $\Lambda_{g,r}(x)$: $O_{qm}(n^2)$
- Computing the minimal basis of $M(r)$ with Euclidean algorithm: $O_{qm}(n^3)$
- Computing the minimal basis of $M(r)$ iteratively (not in this talk): $O_{qm}(n^2)$
Complexity:

- Computing $\Lambda_{g,r}(x)$: $O_{q^m}(n^2)$
- Computing the minimal basis of $\mathcal{M}(r)$ with Euclidean algorithm: $O_{q^m}(n^3)$
- Computing the minimal basis of $\mathcal{M}(r)$ iteratively (not in this talk): $O_{q^m}(n^2)$

- Parametrization: $O_{q^m}((q^{m(2t+k-n)} + q)n^2)$
  - If $t \leq (n - k)/2$ (unique decoding), then polynomial.
  
  - If $t > (n - k)/2$, then exponential.
Idea to improve parametrization (open problem):

- When finding all \([N(x) - D(x)] \in \mathcal{M}(r)\) with the degree restrictions we can impose extra condition that the error span polynomial \(D(x)\) has only distinct roots.
Idea to improve parametrization (open problem):

- When finding all \([N(x) - D(x)] \in \mathcal{M}(r)\) with the degree restrictions we can impose extra condition that the error span polynomial \(D(x)\) has only distinct roots.
- **Open problem**: How to parametrize this condition?
- In Reed-Solomon case it can be done with a curve fitting algorithm (based on Wu’s algorithm). This idea does not work in the linearized case.
1 Linearized Polynomials
   - The Ring $\mathcal{L}_q(x, q^m)$
   - Modules over $\mathcal{L}_q(x, q^m)$

2 Network Coding and Gabidulin Codes
   - Introduction
   - Gabidulin Codes and Interpolation Decoding

3 Summary and Conclusion
Summary and Conclusion

- $\mathcal{L}_q(x, q^m)$ is non-commutative ring with Euclidean algorithm
- $\mathcal{L}_q(x, q^m)^\ell$, as left module, can be equipped with monomial order (e.g. $(k, \ldots, k\ell)$-weighted TOP order)
- Minimal basis = basis with all distinct leading positions
- Predictable Leading Monomial Property holds for minimal bases
- PLMP gives rise to parametrizations
Summary and Conclusion

- $\mathcal{L}_q(x, q^m)$ is a non-commutative ring with Euclidean algorithm
- $\mathcal{L}_q(x, q^m)^\ell$, as a left module, can be equipped with a monomial order (e.g. $(k, \ldots, k_\ell)$-weighted TOP order)
- Minimal basis = basis with all distinct leading positions
- Predictable Leading Monomial Property holds for minimal bases
- PLMP gives rise to parametrizations

Remark: Linearized polynomials are skew polynomials, many statements can be proven in this setting, as well.
Decoding in the network coding setting (Gabidulin codes) can be translated to a parametrization in the interpolation module.

Set up algebraic decoding algorithm, that finds all codewords within the ball of radius $t$ around a given received word, for any decoding radius $t$.

Can easily be altered to find all closest codewords to a given received word.

Complexity is exponential in code length iff the decoding radius is beyond the unique decoding radius.

Nonetheless, it is still feasible for radii close to the unique decoding radius.
• Decoding in the network coding setting (Gabidulin codes) can be translated to a parametrization in the interpolation module.
• Set up algebraic decoding algorithm, that finds all codewords within the ball of radius \( t \) around a given received word, for any decoding radius \( t \).
• Can easily be altered to find all closest codewords to a given received word.
• Complexity is exponential in code length iff the decoding radius is beyond the unique decoding radius.
• Nonetheless, it is still feasible for radii close to the unique decoding radius.

Thank you for your attention!