Residues of skew rational functions and linearized Goppa codes

Xavier Caruso

University of Bordeaux

xavier.caruso@normalesup.org

SpecFun seminar

October 28, 2019

Skew polynomials and skew rational functions

Definition of skew polynomials

Definition of skew polynomials

Notations

Definition of skew polynomials

Notations

K — a field

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition

A skew polynomial is an expression of the form:

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$$

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition

A skew polynomial is an expression of the form:

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$$

Multiplication of skew polynomials is governed by the rule:

$$Xa = \theta(a)X$$

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition

A skew polynomial is an expression of the form:

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$$

Multiplication of skew polynomials is governed by the rule:

$$Xa = \theta(a)X$$

The ring of skew polynomials is denoted by $K[X;\theta]$

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition

A skew polynomial is an expression of the form:

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$$

Multiplication of skew polynomials is governed by the rule:

$$Xa = \theta(a)X$$

The ring of skew polynomials is denoted by $K[X;\theta]$

We set $Y = X^r$

Definition of skew polynomials

Notations

K — a field

$\theta : K \to K$ — a ring automorphism of finite order r

F — the subfield of K fixed by θ

Definition

A skew polynomial is an expression of the form:

$$a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$$

Multiplication of skew polynomials is governed by the rule:

$$Xa = \theta(a)X$$

The ring of skew polynomials is denoted by $K[X;\theta]$

We set $Y = X^r$; it is a central element

Definition of skew rational functions

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

☞ The centre of $K[X;\theta]$ is $F[Y]$

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

☞ The centre of $K[X;\theta]$ is $F[Y]$; it has finite index

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

- ☞ The centre of $K[X;\theta]$ is $F[Y]$; it has finite index
- ☞ Each skew polynomial has a multiple in the centre

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

- ☞ The centre of $K[X;\theta]$ is $F[Y]$; it has finite index
- ☞ Each skew polynomial has a multiple in the centre
- ☞ Skew rational functions can be written $\frac{P}{D}$ with D central

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

- ☞ The centre of $K[X;\theta]$ is $F[Y]$; it has finite index
- ☞ Each skew polynomial has a multiple in the centre
- ☞ Skew rational functions can be written $\frac{P}{D}$ with D central

$$\textit{i.e.} \quad \mathrm{Frac}\big(K[X;\theta]\big) = \mathrm{Frac}\big(F[Y]\big) \otimes_{F[Y]} K[X;\theta]$$

Definition of skew rational functions

Definition

A skew rational function is an element of $\mathrm{Frac}\big(K[X;\theta]\big)$

Observations

- ☞ The centre of $K[X;\theta]$ is $F[Y]$; it has finite index
- ☞ Each skew polynomial has a multiple in the centre
- ☞ Skew rational functions can be written $\frac{P}{D}$ with D central

$$\textit{i.e.} \quad \mathrm{Frac}\big(K[X;\theta]\big) = \mathrm{Frac}\big(F[Y]\big) \otimes_{F[Y]} K[X;\theta]$$

- ☞ With this representation, we have

$$\frac{P_1}{D_1} + \frac{P_2}{D_2} = \frac{P_1 D_2 + P_2 D_1}{D_1 D_2} \quad \text{and} \quad \frac{P_1}{D_1} \cdot \frac{P_2}{D_2} = \frac{P_1 P_2}{D_1 D_2}$$

A theory of residues

A theory of residues

Throughout this section, for simplicity,
we assume that the characteristic of K does not divide r

Derivation of skew polynomials

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r}$$

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r} \quad \in K[X^{\pm 1}; \theta]$$

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r} \quad \in K[X^{\pm 1}; \theta]$$

$$X^{-1} a = \theta^{-1}(a) X^{-1}$$

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r} \quad \in K[X^{\pm 1}; \theta]$$

$$X^{-1} a = \theta^{-1}(a) X^{-1}$$

Proposition

$\frac{d}{dY}$ is a K-linear derivation on $K[X^{\pm 1}; \theta]$

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r} \quad \in K[X^{\pm 1}; \theta]$$

$$X^{-1} a = \theta^{-1}(a) X^{-1}$$

Proposition

$\frac{d}{dY}$ is a K-linear derivation on $K[X^{\pm 1}; \theta]$

$$\textit{i.e.} \qquad \frac{d}{dY}(PQ) = \frac{dP}{dY}\, Q + P\, \frac{dQ}{dY}$$

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r} \quad \in K[X^{\pm 1}; \theta]$$

$$X^{-1} a = \theta^{-1}(a) X^{-1}$$

Proposition

$\frac{d}{dY}$ is a K-linear derivation on $K[X^{\pm 1}; \theta]$

$$\textit{i.e.} \qquad \frac{d}{dY}(PQ) = \frac{dP}{dY}\, Q + P\, \frac{dQ}{dY}$$

Consequence

$\frac{d}{dY}$ extends to a K-linear derivation on $\mathrm{Frac}\big(K[X; \theta]\big)$

Derivation of skew polynomials

For a skew polynomial $P = \sum_i a_i X^i$, we define:

$$\frac{dP}{dY} = \frac{1}{r} \cdot \sum_i i\, a_i\, X^{i-r} \quad \in K[X^{\pm 1}; \theta]$$

$$X^{-1} a = \theta^{-1}(a) X^{-1}$$

Proposition

$\frac{d}{dY}$ is a K-linear derivation on $K[X^{\pm 1}; \theta]$

$$\textit{i.e.} \qquad \frac{d}{dY}(PQ) = \frac{dP}{dY}\, Q + P\, \frac{dQ}{dY}$$

Consequence

$\frac{d}{dY}$ extends to a K-linear derivation on $\mathrm{Frac}\big(K[X; \theta]\big)$

$$\frac{d}{dY}\left(\frac{P}{D}\right) = \frac{\frac{dP}{dY} D - P \frac{dD}{dY}}{D^2}$$

Taylor expansion of skew rational functions

Taylor expansion of skew rational functions

Definition

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$, we define:

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \frac{d^n f}{dY^n} \right)_{|Y=z} T^n$$

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$, we define:

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \frac{d^n f}{dY^n} \right)_{|Y=z} T^n$$

reduction modulo $Y-z$

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$, we define:

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \frac{d^n f}{dY^n} \right)_{|Y=z} T^n \quad \in \quad \frac{K[X;\theta]}{(Y-z)}[\![T]\!]$$

reduction modulo $Y-z$

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$, we define:

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \frac{d^n f}{dY^n} \right)_{|Y=z} T^n \quad \in \quad \frac{K[X;\theta]}{(Y-z)}[\![T]\!]$$

reduction modulo $Y-z$

☞ Otherwise, if z is a zero of D of order m, we define:

$$\mathrm{TS}_z(f) = T^{-m} \cdot \mathrm{TS}_z\big((Y-z)^m f\big)$$

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$, we define:

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \frac{d^n f}{dY^n} \right)_{|Y=z} T^n \quad \in \quad \frac{K[X;\theta]}{(Y-z)}[\![T]\!]$$

reduction modulo $Y-z$

☞ Otherwise, if z is a zero of D of order m, we define:

$$\mathrm{TS}_z(f) = T^{-m} \cdot \mathrm{TS}_z\big((Y-z)^m f\big) \quad \in \quad \frac{K[X;\theta]}{(Y-z)}(\!(T)\!)$$

Taylor expansion of skew rational functions

Definition

Let $z \in F^\times$; let $f = \frac{P}{D}$ be a skew rational function

☞ If $D_{|Y=z} \neq 0$, we define:

$$\mathrm{TS}_z(f) = \sum_{n=0}^{\infty} \left(\frac{1}{n!} \frac{d^n f}{dY^n} \right)_{|Y=z} T^n \quad \in \quad \frac{K[X;\theta]}{(Y-z)}[\![T]\!]$$

reduction modulo $Y-z$

☞ Otherwise, if z is a zero of D of order m, we define:

$$\mathrm{TS}_z(f) = T^{-m} \cdot \mathrm{TS}_z\big((Y-z)^m f\big) \quad \in \quad \frac{K[X;\theta]}{(Y-z)}(\!(T)\!)$$

Theorem

The function $\mathrm{TS}_z : \mathrm{Frac}\big(K[X;\theta]\big) \longrightarrow \frac{K[X;\theta]}{(Y-z)}(\!(T)\!)$

is a homomorphism of K-algebras

Skew residues

Skew residues

Definition

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Generalization

One can also define partial skew residues
when z lies in a separable closure F^{sep} of F or $z = \infty$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Generalization

One can also define partial skew residues
when z lies in a separable closure F^{sep} of F or $z = \infty$

$$\mathrm{sres}_{z,j}(f)$$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Generalization

One can also define partial skew residues
when z lies in a separable closure F^{sep} of F or $z = \infty$

$$\mathrm{sres}_{z,j}(f) = [\ldots]$$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Generalization

One can also define partial skew residues
when z lies in a separable closure F^{sep} of F or $z = \infty$

$$\mathrm{sres}_{z,j}(f) = [\ \ldots\ ] \quad \in F[z] \otimes_F K$$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Generalization

One can also define partial skew residues
when z lies in a separable closure F^{sep} of F or $z = \infty$

$$\mathrm{sres}_{z,j}(f) = [\ \ldots\ ] \quad \in F[z] \otimes_F K \subset F^{\mathrm{sep}} \otimes_F K$$

Skew residues

Definition

Let $z \in F^\times$; let f be a skew rational function

☞ The skew residue of f at z is:

$$\mathrm{sres}_z(f) = \text{coefficient of } T^{-1} \text{ in } \mathrm{TS}_z(f) \quad \in \frac{K[X;\theta]}{(Y-z)}$$

☞ For $j \in \{0, 1, \ldots, r-1\}$,
the j-th partial skew residue of f at z is:

$$\mathrm{sres}_{z,j}(f) = \text{coefficient of } X^j \text{ in } \mathrm{sres}_z(f) \quad \in K$$

Generalization

One can also define partial skew residues
when z lies in a separable closure F^{sep} of F or $z = \infty$

$$\mathrm{sres}_{z,j}(f) = [\ \ldots\ ] \quad \in F[z] \otimes_F K \subset F^{\mathrm{sep}} \otimes_F K \simeq (F^{\mathrm{sep}})^r$$

A residue formula

A residue formula

Theorem

A residue formula

Theorem

☞ For all skew rational function f, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,0}(f) = 0$$

A residue formula

Theorem

- For all skew rational function f, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,0}(f) = 0$$

- If f has only simple poles, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,j}(f) = 0, \qquad \forall j \in \{0, 1, \ldots, r-1\}$$

A residue formula

Theorem

- For all skew rational function f, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,0}(f) = 0$$

- If f has only simple poles, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,j}(f) = 0, \qquad \forall j \in \{0, 1, \ldots, r-1\}$$

Remarks

A residue formula

Theorem

- For all skew rational function f, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,0}(f) = 0$$

- If f has only simple poles, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,j}(f) = 0, \qquad \forall j \in \{0, 1, \ldots, r-1\}$$

Remarks

The main ingredient of the proof is a formula relating $\mathrm{sres}_{z,j}(f)$ to a residue of a classical rational function

A residue formula

Theorem

- For all skew rational function f, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,0}(f) = 0$$

- If f has only simple poles, we have:

$$\sum_{z \in F^{\mathrm{sep}} \sqcup \{\infty\}} \mathrm{sres}_{z,j}(f) = 0, \qquad \forall j \in \{0, 1, \ldots, r-1\}$$

Remarks

The main ingredient of the proof is a formula relating $\mathrm{sres}_{z,j}(f)$ to a residue of a classical rational function

The second part of the theorem admits generalizations when f has multiple poles, but they are much more difficult to state

Change of variables

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

☞ $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$

i.e. γ stabilizes $\mathrm{Frac}\big(K[Y]\big)$ and acts on it
as the change of variables $Y \mapsto NY$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$

i.e. γ stabilizes $\mathrm{Frac}\big(K[Y]\big)$ and acts on it as the change of variables $Y \mapsto NY$

- If $f \in \mathrm{Frac}\big(K[Y]\big)$,

$$\mathrm{res}_{\gamma\star z}\big(f\, dY\big) = \mathrm{res}_z\big(\gamma(f)\, d\gamma(Y)\big) = \mathrm{res}_z\left(\gamma(f)\, \frac{d\gamma(Y)}{dY}\, dY\right)$$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$

i.e. γ stabilizes $\mathrm{Frac}\big(K[Y]\big)$ and acts on it as the change of variables $Y \mapsto NY$

- If $f \in \mathrm{Frac}\big(K[Y]\big)$,

$$\mathrm{res}_{\gamma\star z}\big(f\,dY\big) = \mathrm{res}_z\big(\gamma(f)\,d\gamma(Y)\big) = \mathrm{res}_z\left(\gamma(f)\,\frac{d\gamma(Y)}{dY}\,dY\right)$$

$\gamma\star z = \gamma(Y)_{|Y=z}$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$

i.e. γ stabilizes $\mathrm{Frac}\big(K[Y]\big)$ and acts on it as the change of variables $Y \mapsto NY$

- If $f \in \mathrm{Frac}\big(K[Y]\big)$,

$$\mathrm{res}_{\gamma_\star z}\big(f\,dY\big) = \mathrm{res}_z\big(\gamma(f)\,d\gamma(Y)\big) = \mathrm{res}_z\left(\gamma(f)\,\frac{d\gamma(Y)}{dY}\,dY\right)$$

$\gamma_\star z = \gamma(Y)_{|Y=z}$

Objective

Generalize this formula to any skew rational function f

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$
- By Hilbert's Theorem 90, there exists U such that:

$$\frac{\theta(U)}{U} = \frac{C}{\sqrt[r]{N}}$$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$
- By Hilbert's Theorem 90, there exists U such that:

$$\frac{\theta(U)}{U} = \frac{C}{\sqrt[r]{N}} \quad \in \mathrm{Frac}\big(F[Y]\big)\big[\sqrt[r]{N}\,\big] \otimes_F K$$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$
- By Hilbert's Theorem 90, there exists U such that:

$$\frac{\theta(U)}{U} = \frac{C}{\sqrt[r]{N}} \in \mathrm{Frac}\big(F[Y]\big)\big[\sqrt[r]{N}\,\big] \otimes_F K \subset \mathrm{Frac}\big(F[Y]\big)\big[\sqrt[r]{N}\,\big] \otimes_{F[Y]} K[X;\theta]$$

Change of variables

Let $\gamma : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$
be an endormorphism of K-algebras

Change of variables $X \mapsto \gamma(X)$

Facts

- $\gamma(X) = CX$ with $C \in \mathrm{Frac}\big(K[Y]\big)$
- $\gamma(Y) = NY$ with $N = \mathrm{N}_{K/F}(C) \in \mathrm{Frac}\big(F[Y]\big)$
- By Hilbert's Theorem 90, there exists U such that:

$$\frac{\theta(U)}{U} = \frac{C}{\sqrt[r]{N}} \quad \in \mathrm{Frac}\big(F[Y]\big)\big[\sqrt[r]{N}\,\big] \otimes_F K$$
$$\subset \mathrm{Frac}\big(F[Y]\big)\big[\sqrt[r]{N}\,\big] \otimes_{F[Y]} K[X;\theta]$$

Theorem

For all skew rational function f, we have:

$$\mathrm{sres}_{\gamma_\star z}\big(f\big) = U^{-1} \cdot \mathrm{sres}_z\left(U\,\gamma(f)\,U^{-1}\,\frac{d\gamma(Y)}{dY}\right) \cdot U$$

$\gamma_\star z = \gamma(Y)_{|Y=z}$

When p divides r

When p divides r

- ☞ There is no analogue of the derivation $\frac{d}{dY}$ on $\mathrm{Frac}\big(K[X;\theta]\big)$

When p divides r

- ☞ There is no analogue of the derivation $\frac{d}{dY}$ on $\mathrm{Frac}\big(K[X;\theta]\big)$

Proposition

There is no derivation $\partial : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$ such that $\partial = \frac{d}{dY}$ on $\mathrm{Frac}\big(K[Y]\big)$ and $\partial^p = 0$

When p divides r

- There is no analogue of the derivation $\frac{d}{dY}$ on $\mathrm{Frac}\big(K[X;\theta]\big)$

  Proposition

  There is no derivation $\partial : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$ such that $\partial = \frac{d}{dY}$ on $\mathrm{Frac}\big(K[Y]\big)$ and $\partial^p = 0$

- But there do exist morphisms of K-algebras

$$\mathrm{TS}_z : K[X;\theta] \longrightarrow \frac{K[X;\theta]}{(Y-z)}[\![T]\!]$$

When p divides r

- There is no analogue of the derivation $\frac{d}{dY}$ on $\mathrm{Frac}\big(K[X;\theta]\big)$

  Proposition

  There is no derivation $\partial : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$ such that $\partial = \frac{d}{dY}$ on $\mathrm{Frac}\big(K[Y]\big)$ and $\partial^p = 0$

- But there do exist morphisms of K-algebras

$$\begin{array}{ccc} \mathrm{TS}_z : K[X;\theta] & \longrightarrow & \dfrac{K[X;\theta]}{(Y-z)}[\![T]\!] \\ \downarrow & \nearrow & \\ \varprojlim_{m>1} \dfrac{K[X;\theta]}{(Y-z)^m} & & \end{array}$$

When p divides r

- There is no analogue of the derivation $\frac{d}{dY}$ on $\mathrm{Frac}\big(K[X;\theta]\big)$

  Proposition

  There is no derivation $\partial : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$ such that $\partial = \frac{d}{dY}$ on $\mathrm{Frac}\big(K[Y]\big)$ and $\partial^p = 0$

- But there do exist morphisms of K-algebras

$$\begin{array}{ccc} \mathrm{TS}_z : K[X;\theta] & \longrightarrow & \dfrac{K[X;\theta]}{(Y-z)}[\![T]\!] \\ \downarrow & \nearrow_{\sim} & \\ \varprojlim_{m>1} \dfrac{K[X;\theta]}{(Y-z)^m} & & \end{array}$$

When p divides r

- There is no analogue of the derivation $\frac{d}{dY}$ on $\mathrm{Frac}\big(K[X;\theta]\big)$

  Proposition

  There is no derivation $\partial : \mathrm{Frac}\big(K[X;\theta]\big) \to \mathrm{Frac}\big(K[X;\theta]\big)$ such that $\partial = \frac{d}{dY}$ on $\mathrm{Frac}\big(K[Y]\big)$ and $\partial^p = 0$

- But there do exist morphisms of K-algebras

$$\begin{array}{ccc} \mathrm{TS}_z : K[X;\theta] & \longrightarrow & \dfrac{K[X;\theta]}{(Y-z)}[\![T]\!] \\ \downarrow & \nearrow_{\sim} & \\ \varprojlim_{m>1} \dfrac{K[X;\theta]}{(Y-z)^m} & & \end{array}$$

- The main issue is that
  there is no canonical choice of such a morphism

When p divides r (cont.)

When p divides r (cont.)

- ☞ One can define skew residues and partial skew residues

When p divides r (cont.)

- ☞ One can define skew residues and partial skew residues but there are not canonical

When p divides r (cont.)

- ☞ One can define skew residues and partial skew residues
  but there are not canonical (They depend upon a choice of TS_z)

When p divides r (cont.)

- One can define skew residues and partial skew residues but there are not canonical (They depend upon a choice of TS_z)
- However are defined without ambiguity:

When p divides r (cont.)

- One can define skew residues and partial skew residues but there are not canonical (They depend upon a choice of TS_z)
- However are defined without ambiguity:
  - $\mathrm{sres}_{z,0}(f)$ for any $f \in \mathrm{Frac}\big(K[X;\theta]\big)$ and any $z \in F^{\mathrm{sep}}$

When p divides r (cont.)

- One can define skew residues and partial skew residues
  but there are not canonical (They depend upon a choice of TS_z)

- However are defined without ambiguity:
  - $\mathrm{sres}_{z,0}(f)$ for any $f \in \mathrm{Frac}\big(K[X;\theta]\big)$ and any $z \in F^{\mathrm{sep}}$
  - $\mathrm{sres}_z(f)$ if f has (at most) a simple pole at z

When p divides r (cont.)

- One can define skew residues and partial skew residues
  but there are not canonical (They depend upon a choice of TS_z)
- However are defined without ambiguity:
  - $\mathrm{sres}_{z,0}(f)$ for any $f \in \mathrm{Frac}\big(K[X;\theta]\big)$ and any $z \in F^{\mathrm{sep}}$
  - $\mathrm{sres}_z(f)$ if f has (at most) a simple pole at z
- The residue formulas hold without any modification

When p divides r (cont.)

- One can define skew residues and partial skew residues
  but there are not canonical (They depend upon a choice of TS_z)

- However are defined without ambiguity:
  - $\mathrm{sres}_{z,0}(f)$ for any $f \in \mathrm{Frac}\big(K[X;\theta]\big)$ and any $z \in F^{\mathrm{sep}}$
  - $\mathrm{sres}_z(f)$ if f has (at most) a simple pole at z

- The residue formulas hold without any modification

- The formula of change of variables reads as follows:

  For any choice of $\mathrm{sres}_{\gamma\star z}$,
  there exists a choice of sres_z such that

$$\mathrm{sres}_{\gamma\star z}\big(f\big) = \mathrm{sres}_z\left(\gamma(f)\,\frac{d\gamma(Y)}{dY}\right)$$

Linearized Goppa codes

Evaluation morphisms

Evaluation morphisms

Definition

Given a K-linear vector space V, a semi-linear homomorphism $\varphi : V \to V$ is an additive mapping such that:

$$\forall a \in K,\ \forall v \in V, \quad \varphi(av) = \theta(a) \cdot \varphi(v)$$

Evaluation morphisms

Definition

Given a K-linear vector space V, a semi-linear homomorphism $\varphi : V \to V$ is an additive mapping such that:

$$\forall a \in K,\ \forall v \in V, \quad \varphi(av) = \theta(a) \cdot \varphi(v)$$

Proposition

☞ If $\varphi : V \to V$ is a semi-linear endomorphism, the function

$$\begin{array}{rccc} \varepsilon_\varphi : & K[X;\theta] & \longrightarrow & \mathrm{End}_F(V) \\ & \sum a_i X^i & \mapsto & \sum a_i \varphi^i \end{array}$$

is a homomorphism of K-algebras

Evaluation morphisms

Definition

Given a K-linear vector space V, a semi-linear homomorphism $\varphi : V \to V$ is an additive mapping such that:

$$\forall a \in K,\ \forall v \in V, \quad \varphi(av) = \theta(a) \cdot \varphi(v)$$

Proposition

- ☞ If $\varphi : V \to V$ is a semi-linear endomorphism, the function

$$\begin{array}{rccc} \varepsilon_\varphi : & K[X;\theta] & \longrightarrow & \mathrm{End}_F(V) \\ & \sum a_i X^i & \mapsto & \sum a_i \varphi^i \end{array}$$

  is a homomorphism of K-algebras

- ☞ The semi-linear endomorphisms of K are the $c\theta$, $c \in K$

Evaluation morphisms

Definition

Given a K-linear vector space V, a semi-linear homomorphism $\varphi : V \to V$ is an additive mapping such that:

$$\forall a \in K,\ \forall v \in V, \quad \varphi(av) = \theta(a) \cdot \varphi(v)$$

Proposition

- ☞ If $\varphi : V \to V$ is a semi-linear endomorphism, the function

$$\begin{array}{rccc} \varepsilon_\varphi : & K[X;\theta] & \longrightarrow & \mathrm{End}_F(V) \\ & \sum a_i X^i & \mapsto & \sum a_i \varphi^i \end{array}$$

  is a homomorphism of K-algebras

- ☞ The semi-linear endomorphisms of K are the $c\theta$, $c \in K$
- ☞ For $c \in K^\star$, ε_c is surjective

Evaluation morphisms

Definition

Given a K-linear vector space V, a semi-linear homomorphism $\varphi : V \to V$ is an additive mapping such that:

$$\forall a \in K,\ \forall v \in V, \quad \varphi(av) = \theta(a) \cdot \varphi(v)$$

Proposition

- ☞ If $\varphi : V \to V$ is a semi-linear endomorphism, the function

$$\begin{array}{rccc} \varepsilon_\varphi : & K[X;\theta] & \longrightarrow & \mathrm{End}_F(V) \\ & \sum a_i X^i & \mapsto & \sum a_i \varphi^i \end{array}$$

  is a homomorphism of K-algebras

- ☞ The semi-linear endomorphisms of K are the $c\theta$, $c \in K$
- ☞ For $c \in K^\star$, ε_c is surjective and $\ker \varepsilon_c = \left(Y - \mathrm{N}_{K/F}(c)\right)$

Linearized Reed–Solomon codes

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

☞ $$\begin{array}{rcl} \rho_{\underline{c},\underline{V}} : K[X;\theta] & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ f & \mapsto & \left(\varepsilon_{c_1}(f)_{|V_1}, \ldots, \varepsilon_{c_m}(f)_{|V_m}\right) \end{array}$$

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

☞ $$\begin{array}{rccl} \rho_{\underline{c},\underline{V}} : K[X;\theta] & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ f & \mapsto & \left(\varepsilon_{c_1}(f)_{|V_1}, \ldots, \varepsilon_{c_m}(f)_{|V_m}\right) \end{array}$$

☞ $$\mathrm{LRS}(k, \underline{c}, \underline{V}) = \rho_{\underline{c},\underline{V}}\left(K[X;\theta]_{<k}\right)$$

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

☞ $$\begin{array}{rcl} \rho_{\underline{c},\underline{V}} : K[X;\theta] & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ f & \mapsto & \left(\varepsilon_{c_1}(f)_{|V_1}, \ldots, \varepsilon_{c_m}(f)_{|V_m}\right) \end{array}$$

☞ $$\mathrm{LRS}(k, \underline{c}, \underline{V}) = \rho_{\underline{c},\underline{V}}\left(K[X;\theta]_{<k}\right)$$

Theorem

The parameters of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ are:
length n, dimension k, minimal distance $d = n - k + 1$

Linearized Reed–Solomon codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

☞ $$\begin{array}{rcl} \rho_{\underline{c},\underline{V}} : K[X;\theta] & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ f & \mapsto & \left(\varepsilon_{c_1}(f)_{|V_1}, \ldots, \varepsilon_{c_m}(f)_{|V_m}\right) \end{array}$$

☞ $$\mathrm{LRS}(k, \underline{c}, \underline{V}) = \rho_{\underline{c},\underline{V}}\left(K[X;\theta]_{<k}\right)$$

Theorem

The parameters of $\mathrm{LRS}(k, \underline{c}, \underline{V})$ are:
length n, dimension k, minimal distance $d = n - k + 1$

for the sum-rank weight: $w_{\text{s-rk}}(\underline{\varphi}) = \mathrm{rank}(\varphi_1) + \cdots + \mathrm{rank}(\varphi_m)$

Linearized Goppa codes

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \mathrm{codim}_F V_1 + \cdots + \mathrm{codim}_F V_m$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

☞ There exists $D \in K[X;\theta]$ of degree n with $\operatorname{im} \varepsilon_{c_i}(D) = V_i$, $\forall i$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

- There exists $D \in K[X;\theta]$ of degree n with $\operatorname{im} \varepsilon_{c_i}(D) = V_i$, $\forall i$
- For $f = gD^{-1}$ with $g \in K[X^{\pm 1};\theta]$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

- There exists $D \in K[X;\theta]$ of degree n with $\operatorname{im} \varepsilon_{c_i}(D) = V_i$, $\forall i$
- For $f = gD^{-1}$ with $g \in K[X^{\pm 1};\theta]$:
  - f has a simple pole at each $z_i = \mathrm{N}_{K/F}(c_i)$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

- There exists $D \in K[X;\theta]$ of degree n with $\operatorname{im} \varepsilon_{c_i}(D) = V_i$, $\forall i$
- For $f = gD^{-1}$ with $g \in K[X^{\pm 1};\theta]$:
  - f has a simple pole at each $z_i = \mathrm{N}_{K/F}(c_i)$
  - $\varepsilon_{c_i}\big(\operatorname{sres}_{z_i}(f)\big)$ vanishes on V_i

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

- There exists $D \in K[X;\theta]$ of degree n with $\operatorname{im} \varepsilon_{c_i}(D) = V_i$, $\forall i$
- For $f = gD^{-1}$ with $g \in K[X^{\pm 1};\theta]$:
  - f has a simple pole at each $z_i = \mathrm{N}_{K/F}(c_i)$
  - $\varepsilon_{c_i}\big(\operatorname{sres}_{z_i}(f)\big)$ vanishes on V_i
    and then induces a F-linear mapping $K/V_i \to K$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Preparation

- There exists $D \in K[X;\theta]$ of degree n with $\operatorname{im} \varepsilon_{c_i}(D) = V_i$, $\forall i$
- For $f = gD^{-1}$ with $g \in K[X^{\pm 1};\theta]$:
  - f has a simple pole at each $z_i = \mathrm{N}_{K/F}(c_i)$
  - $\varepsilon_{c_i}\big(\operatorname{sres}_{z_i}(f)\big)$ vanishes on V_i
    and then induces a F-linear mapping $K/V_i \to K$

Note: $\varepsilon_{c_i}\big(\operatorname{sres}_{z_i}(f)\big) = \varepsilon_{c_i}\big((Y - z_i) \cdot f\big)$

Linearized Goppa codes

Let $\underline{c} = (c_1, \ldots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \ldots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

Linearized Goppa codes

Let $\underline{c} = (c_1, \dots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \dots, V_m)$ be F-linear subspaces of K

Set $n = \mathrm{codim}_F V_1 + \cdots + \mathrm{codim}_F V_m$ and let $k \leq n$

☞ $\gamma_{\underline{c},\underline{V}} : K[X^{\pm 1}; \theta]\, D^{-1} \longrightarrow \mathrm{Hom}_F(K/V_1, K) \times \cdots$

$$f \mapsto \left(\varepsilon_{c_1}(\mathrm{sres}_{z_1}(f)), \dots\right)$$

Linearized Goppa codes

Let $\underline{c} = (c_1, \dots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \dots, V_m)$ be F-linear subspaces of K

Set $n = \mathrm{codim}_F V_1 + \cdots + \mathrm{codim}_F V_m$ and let $k \leq n$

☞ $\gamma_{\underline{c},\underline{V}} : K[X^{\pm 1}; \theta]\, D^{-1} \longrightarrow \mathrm{Hom}_F(K/V_1, K) \times \cdots$

$$f \mapsto \left(\varepsilon_{c_1}(\mathrm{sres}_{z_1}(f)), \dots\right)$$

☞ $\mathrm{LG}(k, \underline{c}, \underline{V}) = \gamma_{\underline{c},\underline{V}}\left(K[X; \theta]_{<k}\, X^{n-k-r(m+1)}\, D^{-1}\right)$

Linearized Goppa codes

Let $\underline{c} = (c_1, \dots, c_m)$ be elements of $K^\star$
such that the $\mathrm{N}_{K/F}(c_i)$'s are pairwise distinct

Let $\underline{V} = (V_1, \dots, V_m)$ be F-linear subspaces of K

Set $n = \dim_F V_1 + \cdots + \dim_F V_m$ and let $k \leq n$

☞ $\gamma_{\underline{c},\underline{V}} : K[X^{\pm 1}; \theta]\, D^{-1} \longrightarrow \mathrm{Hom}_F(K/V_1, K) \times \cdots$

$$f \mapsto \left(\varepsilon_{c_1}(\mathrm{sres}_{z_1}(f)), \dots\right)$$

☞ $\mathrm{LG}(k, \underline{c}, \underline{V}) = \gamma_{\underline{c},\underline{V}}\left(K[X; \theta]_{<k}\, X^{n-k-r(m+1)}\, D^{-1}\right)$

Theorem

The parameters of $\mathrm{LG}(k, \underline{c}, \underline{V})$ are:
length n, dimension k, minimal distance $d = n - k + 1$

for the sum-rank weight: $w_{\text{s-rk}}(\underline{\varphi}) = \mathrm{rank}(\varphi_1) + \cdots + \mathrm{rank}(\varphi_m)$

Main ingredient of the proof: Comparison with Reed–Solomon codes

Main ingredient of the proof: Comparison with Reed–Solomon codes

1. There exists a skew polynomial D' such that:

$$D'D = (Y - z_1)(Y - z_2)\cdots(Y - z_m)$$

Main ingredient of the proof: Comparison with Reed–Solomon codes

1. There exists a skew polynomial D' such that:

$$D'D = (Y - z_1)(Y - z_2)\cdots(Y - z_m)$$

2. Set $v = n - k - r\,(m+1)$. For all i:

$$\ker \varepsilon_{c_i}(D') = \ker \varepsilon_{c_i}(X^v D') = V_i$$

Main ingredient of the proof: Comparison with Reed–Solomon codes

1. There exists a skew polynomial D' such that:
$$D'D = (Y - z_1)(Y - z_2)\cdots(Y - z_m)$$

2. Set $v = n - k - r\,(m+1)$. For all i:
$$\ker \varepsilon_{c_i}(D') = \ker \varepsilon_{c_i}(X^v D') = V_i$$

3. $\displaystyle\prod_{j\neq i}(z_i - z_j)^{-1} \cdot \varepsilon_{c_i}(X^v D')$ induces isomorphisms:
$$\tau_i : \quad K/V_i \xrightarrow{\sim} \operatorname{im} \varepsilon_{c_i}(X^v D') = W_i$$

Main ingredient of the proof: Comparison with Reed–Solomon codes

1. There exists a skew polynomial D' such that:
$$D'D = (Y - z_1)(Y - z_2)\cdots(Y - z_m)$$

2. Set $v = n - k - r\,(m+1)$. For all i:
$$\ker \varepsilon_{c_i}(D') = \ker \varepsilon_{c_i}(X^v D') = V_i$$

3. $\displaystyle\prod_{j\neq i}(z_i - z_j)^{-1} \cdot \varepsilon_{c_i}(X^v D')$ induces isomorphisms:
$$\tau_i : \quad K/V_i \xrightarrow{\sim} \operatorname{im} \varepsilon_{c_i}(X^v D') = W_i$$
$$\tau_i^\star : \quad \operatorname{Hom}_F(W_i, K) \xrightarrow{\sim} \operatorname{Hom}_F(K/V_i, K)$$

Main ingredient of the proof: Comparison with Reed–Solomon codes

1. There exists a skew polynomial D' such that:
$$D'D = (Y - z_1)(Y - z_2)\cdots(Y - z_m)$$

2. Set $v = n - k - r\,(m+1)$. For all i:
$$\ker \varepsilon_{c_i}(D') = \ker \varepsilon_{c_i}(X^v D') = V_i$$

3. $\displaystyle\prod_{j\neq i}(z_i - z_j)^{-1} \cdot \varepsilon_{c_i}(X^v D')$ induces isomorphisms:
$$\tau_i : \quad K/V_i \xrightarrow{\sim} \operatorname{im} \varepsilon_{c_i}(X^v D') = W_i$$
$$\tau_i^\star : \quad \operatorname{Hom}_F(W_i, K) \xrightarrow{\sim} \operatorname{Hom}_F(K/V_i, K)$$

4. $\underline{\tau}^\star = (\tau_1^\star, \ldots, \tau_m^\star)$ identifies $\mathrm{LRS}(k, \underline{c}, \underline{W})$ with $\mathrm{LG}(k, \underline{c}, \underline{V})$

Main ingredient of the proof: Comparison with Reed–Solomon codes

1. There exists a skew polynomial D' such that:
$$D'D = (Y - z_1)(Y - z_2)\cdots(Y - z_m)$$

2. Set $v = n - k - r\,(m+1)$. For all i:
$$\ker \varepsilon_{c_i}(D') = \ker \varepsilon_{c_i}(X^v D') = V_i$$

3. $\displaystyle\prod_{j\neq i}(z_i - z_j)^{-1} \cdot \varepsilon_{c_i}(X^v D')$ induces isomorphisms:
$$\tau_i : \quad K/V_i \xrightarrow{\sim} \operatorname{im} \varepsilon_{c_i}(X^v D') = W_i$$
$$\tau_i^\star : \quad \operatorname{Hom}_F(W_i, K) \xrightarrow{\sim} \operatorname{Hom}_F(K/V_i, K)$$

4. $\underline{\tau}^\star = (\tau_1^\star, \ldots, \tau_m^\star)$ identifies $\mathrm{LRS}(k, \underline{c}, \underline{W})$ with $\mathrm{LG}(k, \underline{c}, \underline{V})$

5. $\underline{\tau}^\star$ preserves the sum-rank weight

A theorem of duality

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

Pairing

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

Pairing

☞ K is equipped with the pairing $\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

Pairing

- K is equipped with the pairing $\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$
- $\mathrm{End}_F(K)$ is equipped with the pairing $\langle \varphi, \psi \rangle_K = \mathrm{Tr}(\varphi^\star \psi)$

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

Pairing

- K is equipped with the pairing $\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$
- $\mathrm{End}_F(K)$ is equipped with the pairing $\langle \varphi, \psi \rangle_K = \mathrm{Tr}(\varphi^\star \psi)$

  $\varphi^\star$ is the adjoint of φ: $\langle \varphi^\star(x), y \rangle_K = \langle x, \varphi(y) \rangle_K$

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

Pairing

- K is equipped with the pairing $\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$
- $\mathrm{End}_F(K)$ is equipped with the pairing $\langle \varphi, \psi \rangle_K = \mathrm{Tr}(\varphi^\star \psi)$

  $\varphi^\star$ is the adjoint of φ: $\langle \varphi^\star(x), y \rangle_K = \langle x, \varphi(y) \rangle_K$
- More generally, the same formula defines a perfect pairing:

$$\mathrm{Hom}_F(K/V, K) \times \mathrm{Hom}_F(V^\perp, K) \longrightarrow F$$

A theorem of duality

Recall that:

$$\begin{aligned} \mathrm{LRS}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ \mathrm{LG}(k, \underline{c}, \underline{V}) &\subset \mathrm{Hom}_F(K/V_1, K) \times \cdots \times \mathrm{Hom}_F(K/V_m, K) \end{aligned}$$

Pairing

- K is equipped with the pairing $\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$
- $\mathrm{End}_F(K)$ is equipped with the pairing $\langle \varphi, \psi \rangle_K = \mathrm{Tr}(\varphi^\star \psi)$

  $\varphi^\star$ is the adjoint of φ: $\langle \varphi^\star(x), y \rangle_K = \langle x, \varphi(y) \rangle_K$
- More generally, the same formula defines a perfect pairing:

$$\mathrm{Hom}_F(K/V, K) \times \mathrm{Hom}_F(V^\perp, K) \longrightarrow F$$

Theorem

$$\mathrm{LG}\big(k, \underline{c}, \underline{V}\big)^\perp = \mathrm{LRS}\big(n-k, \underline{c}^{-1}, \underline{V}^\perp\big)$$

Decoding algorithm

Decoding algorithm

Decoding linearized Reed–Solomon codes

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

1. Compute $g \in K[X;\theta]$ with $\varepsilon_{c_i}(g) = \underline{\varphi}$

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

1. Compute $g \in K[X;\theta]$ with $\varepsilon_{c_i}(g) = \underline{\varphi}$

2. Compute $U, V, R \in K[X;\theta]$ with

$Ug + VP = R$ and $\deg U \leq w$, $\deg R < w+k$

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

1. Compute $g \in K[X;\theta]$ with $\varepsilon_{c_i}(g) = \underline{\varphi}$

2. Compute $U, V, R \in K[X;\theta]$ with
$Ug + VP = R$ and $\deg U \leq w$, $\deg R < w+k$

3. **Return** the quotient in the left division of R by U

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

1. Compute $g \in K[X;\theta]$ with $\varepsilon_{c_i}(g) = \underline{\varphi}$

2. Compute $U, V, R \in K[X;\theta]$ with
$Ug + VP = R$ and $\deg U \leq w$, $\deg R < w+k$

3. **Return** the quotient in the left division of R by U

Complexity: $\tilde{O}\left(\min\left(n^{\frac{\omega+1}{2}} r,\ n\, r^{\frac{4}{5-\omega}}\right)\right)$ operations in F

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{v}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

1. Compute $g \in K[X;\theta]$ with $\varepsilon_{c_i}(g) = \underline{\varphi}$

2. Compute $U, V, R \in K[X;\theta]$ with
$Ug + VP = R$ and $\deg U \leq w$, $\deg R < w+k$

3. **Return** the quotient in the left division of R by U

Complexity: $\tilde{O}\left(\min\left(n^{\frac{\omega+1}{2}} r,\ n\, r^{\frac{4}{5-\omega}}\right)\right)$ operations in F

Decoding linearized Goppa codes

Decoding algorithm

Decoding linearized Reed–Solomon codes

Input: $\underline{\varphi} = \rho_{\underline{c},\underline{V}}(f) + \underline{e}$ with $w_{\text{s-rk}}(\underline{e}) \leq \dfrac{n-k}{2} = w$

Output: f

0. Compute $P \in K[X;\theta]$ of degree n with $\varepsilon_{c_i}(P) = 0$

1. Compute $g \in K[X;\theta]$ with $\varepsilon_{c_i}(g) = \underline{\varphi}$

2. Compute $U, V, R \in K[X;\theta]$ with
$Ug + VP = R$ and $\deg U \leq w$, $\deg R < w+k$

3. **Return** the quotient in the left division of R by U

Complexity: $\tilde{O}\left(\min\left(n^{\frac{\omega+1}{2}} r,\ n\, r^{\frac{4}{5-\omega}}\right)\right)$ operations in F

Decoding linearized Goppa codes

Use the isomorphism of codes $\mathrm{LG}(k, \underline{c}, \underline{V}) \simeq \mathrm{LRS}(k, \underline{c}, \underline{W})$

Thanks

for your attention