Ore polynomials and application to coding theory

Xavier Caruso
University of Bordeaux
xavier.caruso@normalesup.org

Arithmetic, Geometry,
Cryptography and Coding Theory

June 13, 2019

Ore polynomials

What are Ore polynomials?

What are Ore polynomials?

Setting

What are Ore polynomials?

Setting

Let K be a field

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

i.e. ∂ additive and $\forall a, b \in K, \quad \partial(ab) = \varphi(a)\,\partial(b) + \partial(a)\,b$

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

i.e. ∂ additive and $\forall a, b \in K, \quad \partial(ab) = \varphi(a)\,\partial(b) + \partial(a)\,b$

Definition

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

i.e. ∂ additive and $\forall a, b \in K, \quad \partial(ab) = \varphi(a)\,\partial(b) + \partial(a)\,b$

Definition

The Ore ring $K[x; \varphi, \partial]$ is described as follows

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

i.e. ∂ additive and $\forall a, b \in K, \quad \partial(ab) = \varphi(a)\,\partial(b) + \partial(a)\,b$

Definition

The Ore ring $K[x; \varphi, \partial]$ is described as follows

☞ elements: usual univariate polynomials over K

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

i.e. ∂ additive and $\forall a, b \in K, \quad \partial(ab) = \varphi(a)\,\partial(b) + \partial(a)\,b$

Definition

The Ore ring $K[x; \varphi, \partial]$ is described as follows

☞ elements: usual univariate polynomials over K

☞ addition: standard addition

What are Ore polynomials?

Setting

Let K be a field

Let $\varphi : K \to K$ be a morphism of rings

Let $\partial : K \to K$ be a φ-derivation

i.e. ∂ additive and $\forall a, b \in K, \quad \partial(ab) = \varphi(a)\,\partial(b) + \partial(a)\,b$

Definition

The Ore ring $K[x; \varphi, \partial]$ is described as follows

- ☞ elements: usual univariate polynomials over K
- ☞ addition: standard addition
- ☞ multiplication: driven by $x\,a = \varphi(a)\,x + \partial(a), \quad \forall a \in K$

Example of computations

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$x^2 a$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\mathbf{x}^2\mathbf{a} = \mathbf{x}\cdot\mathbf{x}\,\mathbf{a}$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\mathbf{x}^2\mathbf{a} = \mathbf{x}\cdot\mathbf{x}\,\mathbf{a}$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\begin{aligned}\mathbf{x}^2\mathbf{a} &= \mathbf{x}\cdot\mathbf{x}\,\mathbf{a}\\ &= \mathbf{x}\cdot\left(\varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})\right)\end{aligned}$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\begin{aligned}
\mathbf{x}^2\mathbf{a} &= \mathbf{x}\cdot\mathbf{x}\,\mathbf{a} \\
&= \mathbf{x}\cdot\left(\varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})\right) \\
&= \mathbf{x}\,\varphi(\mathbf{a})\cdot\mathbf{x} + \mathbf{x}\,\partial(\mathbf{a})
\end{aligned}$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\begin{aligned}
\mathbf{x}^2\mathbf{a} &= \mathbf{x}\cdot\mathbf{x}\,\mathbf{a} \\
&= \mathbf{x}\cdot\left(\varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})\right) \\
&= \mathbf{x}\,\varphi(\mathbf{a})\cdot\mathbf{x} + \mathbf{x}\,\partial(\mathbf{a})
\end{aligned}$$

Example of computations

$$\mathbf{x}\,a = \varphi(a)\,\mathbf{x} + \partial(a)$$

$$\begin{aligned}
\mathbf{x}^2 a &= \mathbf{x} \cdot \mathbf{x}\,a \\
&= \mathbf{x} \cdot \big(\varphi(a)\,\mathbf{x} + \partial(a)\big) \\
&= \mathbf{x}\,\varphi(a) \cdot \mathbf{x} + \mathbf{x}\,\partial(a) \\
&= \big(\varphi^2(a)\,\mathbf{x} + \partial\varphi(a)\big) \cdot \mathbf{x}
\end{aligned}$$

Example of computations

$$\mathbf{x}\,a = \varphi(a)\,\mathbf{x} + \partial(a)$$

$$\begin{aligned}
\mathbf{x}^2 a &= \mathbf{x} \cdot \mathbf{x}\,a \\
&= \mathbf{x} \cdot \big(\varphi(a)\,\mathbf{x} + \partial(a)\big) \\
&= \mathbf{x}\,\varphi(a) \cdot \mathbf{x} + \mathbf{x}\,\partial(a) \\
&= \big(\varphi^2(a)\,\mathbf{x} + \partial\varphi(a)\big) \cdot \mathbf{x}
\end{aligned}$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\begin{aligned}
\mathbf{x}^2\mathbf{a} &= \mathbf{x}\cdot\mathbf{x}\,\mathbf{a} \\
&= \mathbf{x}\cdot\big(\varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})\big) \\
&= \mathbf{x}\,\varphi(\mathbf{a})\cdot\mathbf{x} + \mathbf{x}\,\partial(\mathbf{a}) \\
&= \big(\varphi^2(\mathbf{a})\,\mathbf{x} + \partial\varphi(\mathbf{a})\big)\cdot\mathbf{x} \;+\; \varphi\partial(\mathbf{a})\,\mathbf{x} + \partial^2(\mathbf{a})
\end{aligned}$$

Example of computations

$$\mathbf{x}\,\mathbf{a} = \varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})$$

$$\begin{aligned}
\mathbf{x}^2\mathbf{a} &= \mathbf{x}\cdot\mathbf{x}\,\mathbf{a} \\
&= \mathbf{x}\cdot\big(\varphi(\mathbf{a})\,\mathbf{x} + \partial(\mathbf{a})\big) \\
&= \mathbf{x}\,\varphi(\mathbf{a})\cdot\mathbf{x} + \mathbf{x}\,\partial(\mathbf{a}) \\
&= \big(\varphi^2(\mathbf{a})\,\mathbf{x} + \partial\varphi(\mathbf{a})\big)\cdot\mathbf{x} \;+\; \varphi\partial(\mathbf{a})\,\mathbf{x} + \partial^2(\mathbf{a}) \\
&= \varphi^2(\mathbf{a})\,\mathbf{x}^2 \;+\; (\partial\varphi + \varphi\partial)(\mathbf{a})\,\mathbf{x} \;+\; \partial^2(\mathbf{a})
\end{aligned}$$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned}
x^2 a &= x \cdot x\,a \\
&= x \cdot \big(\varphi(a)\,x + \partial(a)\big) \\
&= x\,\varphi(a) \cdot x + x\,\partial(a) \\
&= \big(\varphi^2(a)\,x + \partial\varphi(a)\big) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\
&= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a)
\end{aligned}$$

$$(x^2 + ax + b) \cdot (x^2 + cx + d)$$

Example of computations

$$\mathrm{x}\,a = \varphi(a)\,\mathrm{x} + \partial(a)$$

$$\begin{aligned}
\mathrm{x}^2 a &= \mathrm{x} \cdot \mathrm{x}\,a \\
&= \mathrm{x} \cdot \big(\varphi(a)\,\mathrm{x} + \partial(a)\big) \\
&= \mathrm{x}\,\varphi(a) \cdot \mathrm{x} + \mathrm{x}\,\partial(a) \\
&= \big(\varphi^2(a)\,\mathrm{x} + \partial\varphi(a)\big) \cdot \mathrm{x} \;+\; \varphi\partial(a)\,\mathrm{x} + \partial^2(a) \\
&= \varphi^2(a)\,\mathrm{x}^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,\mathrm{x} \;+\; \partial^2(a)
\end{aligned}$$

$$\begin{aligned}
&(\mathrm{x}^2 + a\mathrm{x} + b) \cdot (\mathrm{x}^2 + c\mathrm{x} + d) \\
&\quad = \mathrm{x}^4 + \mathrm{x}^2 c\mathrm{x} + \mathrm{x}^2 d + a\mathrm{x}^3 + a\mathrm{x}c\mathrm{x} + a\mathrm{x}d + b\mathrm{x}^2 + bc\mathrm{x} + d
\end{aligned}$$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned}
x^2 a &= x \cdot x\,a \\
&= x \cdot \big(\varphi(a)\,x + \partial(a)\big) \\
&= x\,\varphi(a) \cdot x + x\,\partial(a) \\
&= \big(\varphi^2(a)\,x + \partial\varphi(a)\big) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\
&= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a)
\end{aligned}$$

$$\begin{aligned}
&(x^2 + ax + b) \cdot (x^2 + cx + d) \\
&\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d
\end{aligned}$$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned}
x^2 a &= x \cdot x\,a \\
&= x \cdot (\varphi(a)\,x + \partial(a)) \\
&= x\,\varphi(a) \cdot x + x\,\partial(a) \\
&= (\varphi^2(a)\,x + \partial\varphi(a)) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\
&= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a)
\end{aligned}$$

$$\begin{aligned}
&(x^2 + ax + b) \cdot (x^2 + cx + d) \\
&\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d \\
&\quad = x^4
\end{aligned}$$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned}
x^2 a &= x \cdot x\,a \\
&= x \cdot (\varphi(a)\,x + \partial(a)) \\
&= x\,\varphi(a) \cdot x + x\,\partial(a) \\
&= (\varphi^2(a)\,x + \partial\varphi(a)) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\
&= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a)
\end{aligned}$$

$$\begin{aligned}
&(x^2 + ax + b) \cdot (x^2 + cx + d) \\
&\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d \\
&\quad = x^4
\end{aligned}$$

Example of computations

$$\mathrm{x}\,a = \varphi(a)\,\mathrm{x} + \partial(a)$$

$$\begin{aligned}
\mathrm{x}^2 a &= \mathrm{x}\cdot \mathrm{x}\,a \\
&= \mathrm{x}\cdot\big(\varphi(a)\,\mathrm{x} + \partial(a)\big) \\
&= \mathrm{x}\,\varphi(a)\cdot \mathrm{x} + \mathrm{x}\,\partial(a) \\
&= \big(\varphi^2(a)\,\mathrm{x} + \partial\varphi(a)\big)\cdot \mathrm{x} \;+\; \varphi\partial(a)\,\mathrm{x} + \partial^2(a) \\
&= \varphi^2(a)\,\mathrm{x}^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,\mathrm{x} \;+\; \partial^2(a)
\end{aligned}$$

$$\begin{aligned}
&(\mathrm{x}^2 + a\mathrm{x} + b)\cdot(\mathrm{x}^2 + c\mathrm{x} + d) \\
&\quad= \mathrm{x}^4 + \mathrm{x}^2 c\mathrm{x} + \mathrm{x}^2 d + a\mathrm{x}^3 + a\mathrm{x}c\mathrm{x} + a\mathrm{x}d + b\mathrm{x}^2 + bc\mathrm{x} + d \\
&\quad= \mathrm{x}^4 \;+\; \varphi^2(c)\,\mathrm{x}^3 + (\partial\varphi + \varphi\partial)(c)\,\mathrm{x}^2 + \partial^2(c)\mathrm{x}
\end{aligned}$$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned}
x^2 a &= x \cdot x\,a \\
&= x \cdot (\varphi(a)\,x + \partial(a)) \\
&= x\,\varphi(a) \cdot x + x\,\partial(a) \\
&= (\varphi^2(a)\,x + \partial\varphi(a)) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\
&= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a)
\end{aligned}$$

$$\begin{aligned}
&(x^2 + ax + b) \cdot (x^2 + cx + d) \\
&\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d \\
&\quad = x^4 \;+\; \varphi^2(c)\,x^3 + (\partial\varphi + \varphi\partial)(c)\,x^2 + \partial^2(c)x \;+\; \text{etc}
\end{aligned}$$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned} x^2 a &= x \cdot x\,a \\ &= x \cdot (\varphi(a)\,x + \partial(a)) \\ &= x\,\varphi(a) \cdot x + x\,\partial(a) \\ &= (\varphi^2(a)\,x + \partial\varphi(a)) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\ &= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a) \end{aligned}$$

$$\begin{aligned} &(x^2 + ax + b) \cdot (x^2 + cx + d) \\ &\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d \\ &\quad = x^4 \;+\; \varphi^2(c)\,x^3 + (\partial\varphi + \varphi\partial)(c)\,x^2 + \partial^2(c)x \;+\; \text{etc} \end{aligned}$$

In $\mathbb{C}[x;\, z \mapsto \bar{z}]$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned} x^2 a &= x \cdot x\,a \\ &= x \cdot (\varphi(a)\,x + \partial(a)) \\ &= x\,\varphi(a) \cdot x + x\,\partial(a) \\ &= (\varphi^2(a)\,x + \partial\varphi(a)) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\ &= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a) \end{aligned}$$

$$\begin{aligned} &(x^2 + ax + b) \cdot (x^2 + cx + d) \\ &\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d \\ &\quad = x^4 \;+\; \varphi^2(c)\,x^3 + (\partial\varphi + \varphi\partial)(c)\,x^2 + \partial^2(c)x \;+\; \text{etc} \end{aligned}$$

In $\mathbb{C}[x;\, z \mapsto \bar{z}]$: $\quad (x + a) \cdot (x - \bar{a}) = x^2 - |a|^2$

Example of computations

$$x\,a = \varphi(a)\,x + \partial(a)$$

$$\begin{aligned} x^2 a &= x \cdot x\,a \\ &= x \cdot (\varphi(a)\,x + \partial(a)) \\ &= x\,\varphi(a) \cdot x + x\,\partial(a) \\ &= (\varphi^2(a)\,x + \partial\varphi(a)) \cdot x \;+\; \varphi\partial(a)\,x + \partial^2(a) \\ &= \varphi^2(a)\,x^2 \;+\; (\partial\varphi + \varphi\partial)(a)\,x \;+\; \partial^2(a) \end{aligned}$$

$$\begin{aligned} &(x^2 + ax + b) \cdot (x^2 + cx + d) \\ &\quad = x^4 + x^2cx + x^2d + ax^3 + axcx + axd + bx^2 + bcx + d \\ &\quad = x^4 \;+\; \varphi^2(c)\,x^3 + (\partial\varphi + \varphi\partial)(c)\,x^2 + \partial^2(c)x \;+\; \text{etc} \end{aligned}$$

In $\mathbb{C}[x;\, z \mapsto \bar{z}]$: $\quad (x + a) \cdot (x - \bar{a}) = x^2 - |a|^2$

$\Longrightarrow$ Ore polynomials can admit many factorizations

But... Ore polynomials look like polynomials

But... Ore polynomials look like polynomials

There is a well defined notion of degree

But... Ore polynomials look like polynomials

There is a well defined notion of **degree**, and:

$$\forall f, g \in K[x; \varphi, \partial], \quad \deg(f+g) \leq \max(\deg f, \deg g)$$
$$\deg(fg) = \deg f + \deg g$$

But... Ore polynomials look like polynomials

There is a well defined notion of **degree**, and:

$$\forall f, g \in K[x; \varphi, \partial], \quad \deg(f+g) \leq \max(\deg f, \deg g)$$
$$\deg(fg) = \deg f + \deg g$$

Proposition

$K[x; \varphi, \partial]$ is a right Euclidean ring

But... Ore polynomials look like polynomials

There is a well defined notion of degree, and:

$$\forall f, g \in K[x; \varphi, \partial], \quad \deg(f+g) \leq \max(\deg f, \deg g)$$
$$\deg(fg) = \deg f + \deg g$$

Proposition

$K[x; \varphi, \partial]$ is a right Euclidean ring

Given $A, B \in K[x; \varphi, \partial]$ with $B \neq 0$
there exist unique $Q, R \in K[x; \varphi, \partial]$
such that $A = QB + R$ and $\deg R < \deg B$

But... Ore polynomials look like polynomials

There is a well defined notion of **degree**, and:

$$\forall f, g \in K[x; \varphi, \partial], \quad \deg(f+g) \leq \max(\deg f, \deg g)$$
$$\deg(fg) = \deg f + \deg g$$

Proposition

$K[x; \varphi, \partial]$ is a right Euclidean ring

Given $A, B \in K[x; \varphi, \partial]$ with $B \neq 0$
there exist unique $Q, R \in K[x; \varphi, \partial]$
such that $A = QB + R$ and $\deg R < \deg B$

Corollary

$K[x; \varphi, \partial]$ is left principal

But... Ore polynomials look like polynomials

There is a well defined notion of **degree**, and:

$$\forall f, g \in K[x; \varphi, \partial], \quad \deg(f+g) \leq \max(\deg f, \deg g)$$
$$\deg(fg) = \deg f + \deg g$$

Proposition

$K[x; \varphi, \partial]$ is a right Euclidean ring

Given $A, B \in K[x; \varphi, \partial]$ with $B \neq 0$
there exist unique $Q, R \in K[x; \varphi, \partial]$
such that $A = QB + R$ and $\deg R < \deg B$

Corollary

$K[x; \varphi, \partial]$ is left principal

$K[x; \varphi, \partial]$ admits right gcd and left lcm

Application to coding theory

Notion of linear code

Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Its *length* is n

Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Its *length* is n

Its *dimension* is $k = \dim_K C$

Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Its *length* is n

Its *dimension* is $k = \dim_K C$

Its *minimal distance* is $d = \min_{\substack{x \in C \\ x \neq 0}} w(x)$

where $w(x) =$ number of nonzero coordinates of x

Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Its *length* is n

Its *dimension* is $k = \dim_K C$

Its *minimal distance* is $d = \min_{\substack{x \in C \\ x \neq 0}} w(x)$

where $w(x) =$ number of nonzero coordinates of x

(Hamming weight)

Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Its *length* is n

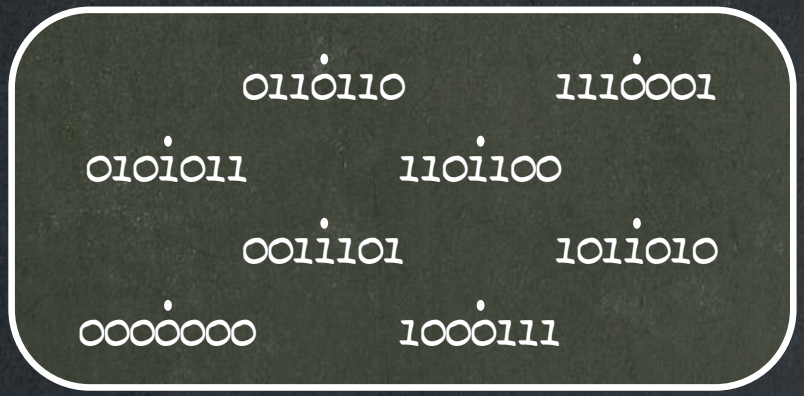
Its *dimension* is $k = \dim_K C$

Its *minimal distance* is $d = \min_{\substack{x \in C \\ x \neq 0}} w(x)$

where $w(x) =$ number of nonzero coordinates of x

(Hamming weight)

Example



Notion of linear code

Definition

A *linear code* is a sub-K-vector space C of K^n

Its *length* is n

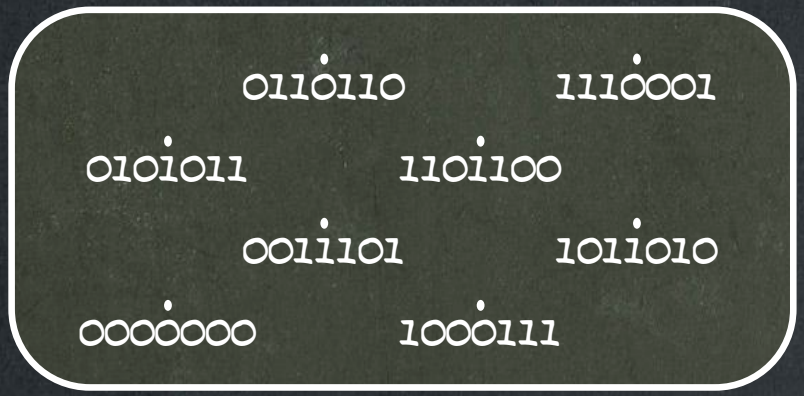
Its *dimension* is $k = \dim_K C$

Its *minimal distance* is $d = \min_{\substack{x \in C \\ x \neq 0}} w(x)$

where $w(x) =$ number of nonzero coordinates of x

(Hamming weight)

Example



Theorem
(Singleton bound)

For any linear code:
$d + k \leq n + 1$

Reed Solomon codes and Gabidulin codes

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be pairwise distinct elements of K

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be pairwise distinct elements of K

The associated Reed Solomon code $RS(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be pairwise distinct elements of K

The associated Reed Solomon code $RS(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be [redacted] elements of K

The associated Reed Solomon code $RS(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of K

The associated Reed Solomon code $RS(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Reed Solomon code $RS(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated code $RS(k; a_1, \ldots, a_n)$

is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $RS(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{rcl} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

$$\left\{ c_0 x + c_1 x^p + \cdots + c_{k-1} x^{p^{k-1}} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

$$\left\{ c_0 x + c_1 x^p + \cdots + c_{k-1} x^{p^{k-1}} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

$$\left\{ c_0 x + c_1 x^p + \cdots + c_{k-1} x^{p^{k-1}} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(a_1), \ldots, f(a_n)) \end{array}$$

$$\left\{ c_0 x + c_1 x^p + \cdots + c_{k-1} x^{p^{k-1}} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & \end{array}$$

$$\left\{ c_0 x + c_1 x^p + \cdots + c_{k-1} x^{p^{k-1}} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(\varphi)(a_1), \ldots, f(\varphi)(a_n)) \end{array}$$

$$\left\{ c_0 x + c_1 x^p + \cdots + c_{k-1} x^{p^{k-1}} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(\varphi)(a_1), \ldots, f(\varphi)(a_n)) \end{array}$$

Theorem

$\{$ [redacted] $\}$ $(c_i \in K)$

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(\varphi)(a_1), \ldots, f(\varphi)(a_n)) \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \quad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x]^{\mathrm{lin}}_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(\varphi)(a_1), \ldots, f(\varphi)(a_n)) \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\longrightarrow K^n$$

$$f(x) \mapsto (f(\varphi)(a_1), \ldots, f(\varphi)(a_n))$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & (f(\varphi)(a_1), \ldots, f(\varphi)(a_n)) \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$x a = a^p x$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$

is the image of

$$K[x;\varphi]_{<k} \longrightarrow K^n$$

$$f(x) \mapsto$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & K^n \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$

is the image of

$$K[x;\varphi]_{<k} \longrightarrow$$

$$f(x) \mapsto f(\varphi)_{|V}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\}$$

$$\boxed{x a = a^p x} \qquad (c_i \in K)$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

Theorem

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(x) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

Theorem

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(\ ) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

Theorem

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(v) = \dim_{\mathbb{F}_p} \langle \text{coord. of } x \rangle \leq w(x)$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(U) =$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $a_1, \ldots, a_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\}$

$x a = a^p x$ $\quad (c_i \in K)$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let $g_1, \ldots, g_n$ be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; g_1, \ldots, g_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\}$$

$$\boxed{x a = a^p x} \qquad (c_i \in K)$$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let V be $\mathbb{F}_p$-linearly indep. elements of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let V be [redacted] of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x\,a = a^p\,x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let V be sub-$\mathbb{F}_p$-vector space of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; a_1, \ldots, a_n)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x a = a^p x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let V be sub-$\mathbb{F}_p$-vector space of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; \quad)$

is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x\,a = a^p\,x}$$

Theorem

length = n

dimension = k

minimal distance = $n - k + 1$

for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

Reed Solomon codes and Gabidulin codes

Let k, n be two positive integers with $k \leq n$

Let V be sub-$\mathbb{F}_p$-vector space of $K = \mathbb{F}_q$

The associated Gabidulin code $\mathrm{Gab}(k; V)$ is the image of

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_{\mathbb{F}_p}(V, K) \\ f(x) & \mapsto & f(\varphi)_{|V} \end{array}$$

$$\left\{ c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \right\} \qquad (c_i \in K)$$

$$\boxed{x\,a = a^p\,x}$$

Theorem

length = n

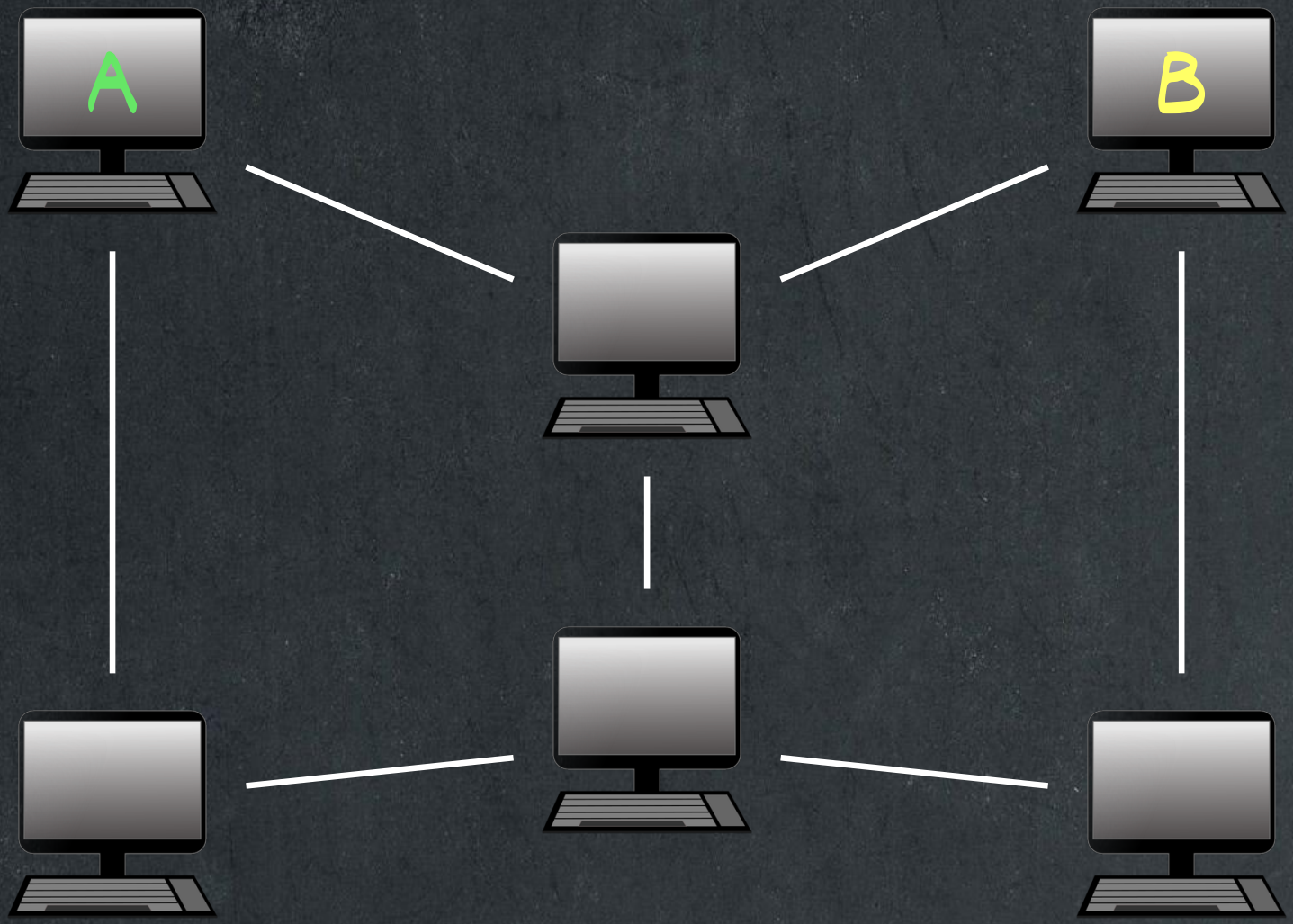
dimension = k

minimal distance = $n - k + 1$

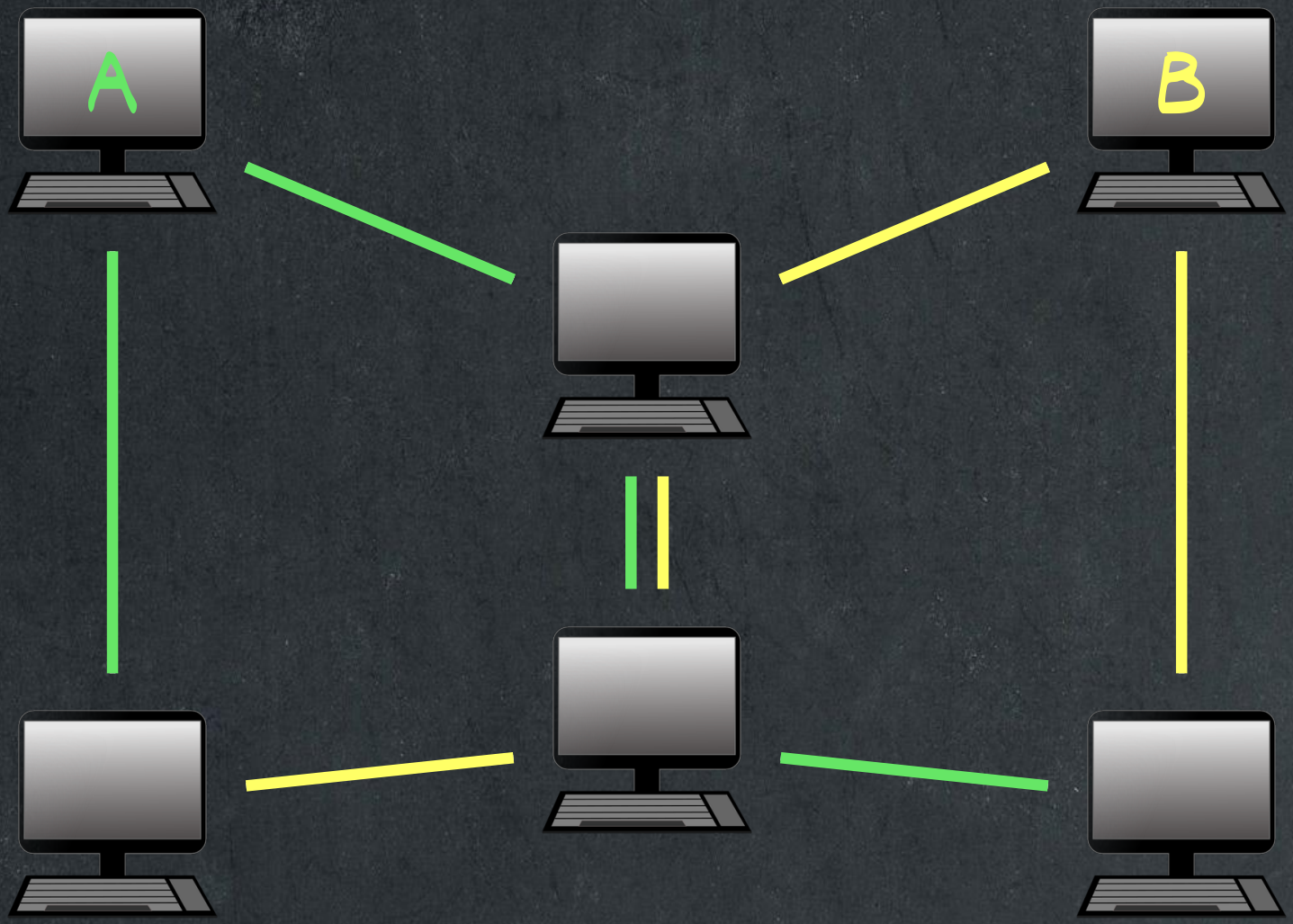
for the rank distance: $w_{rk}(u) = \mathrm{rank}\ u$

Why do we care about the rank distance?

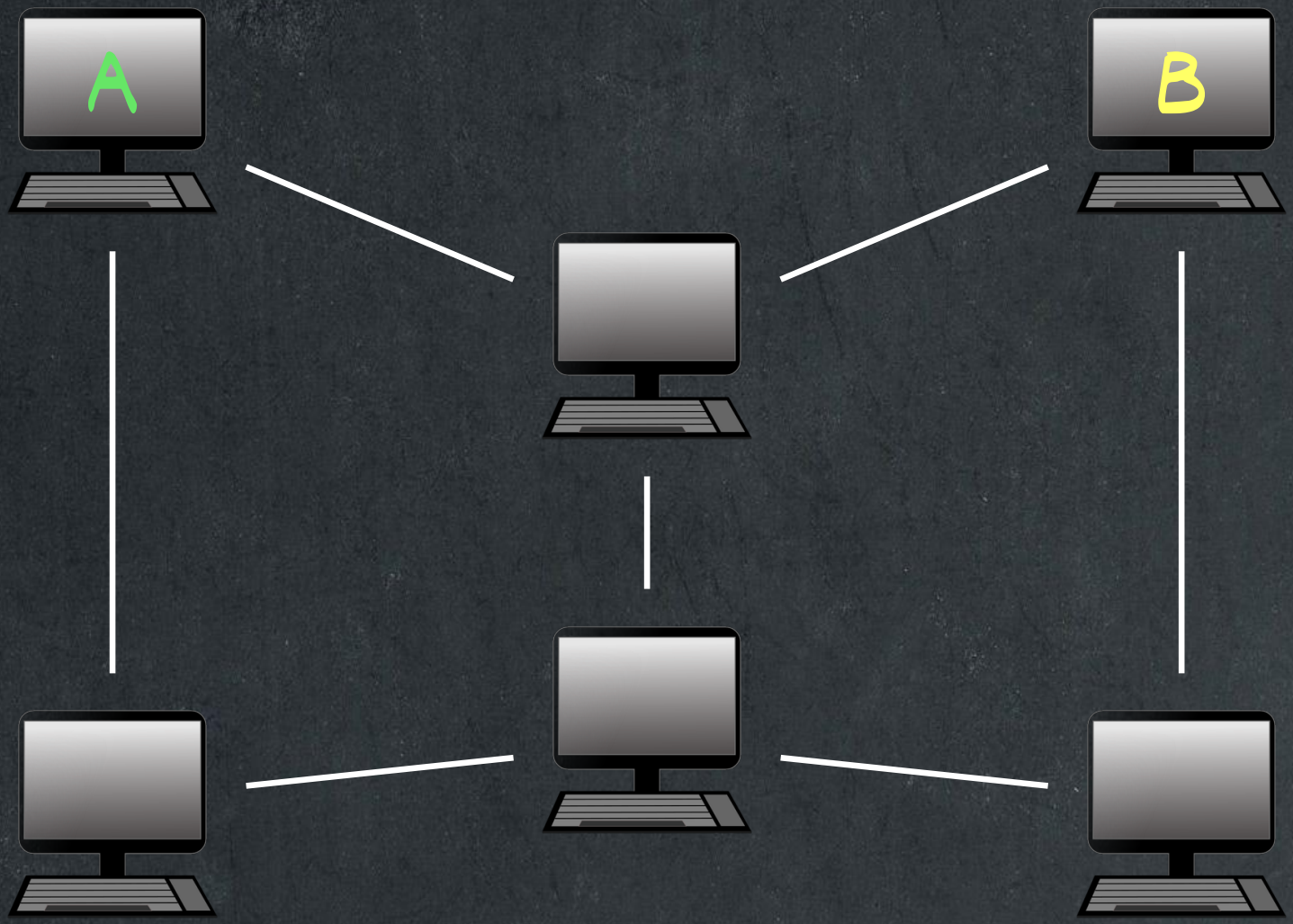
Why do we care about the rank distance?



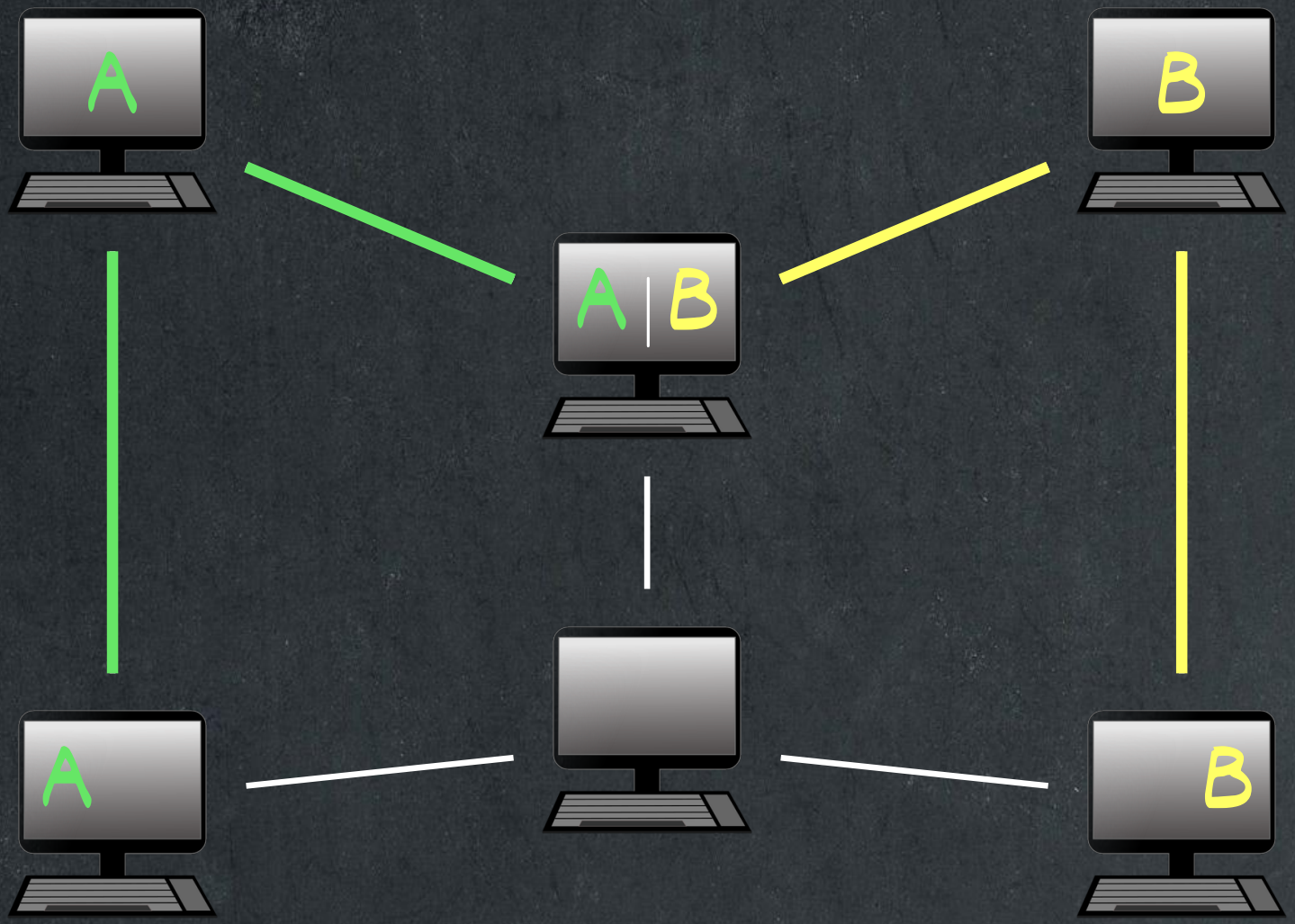
Why do we care about the rank distance?



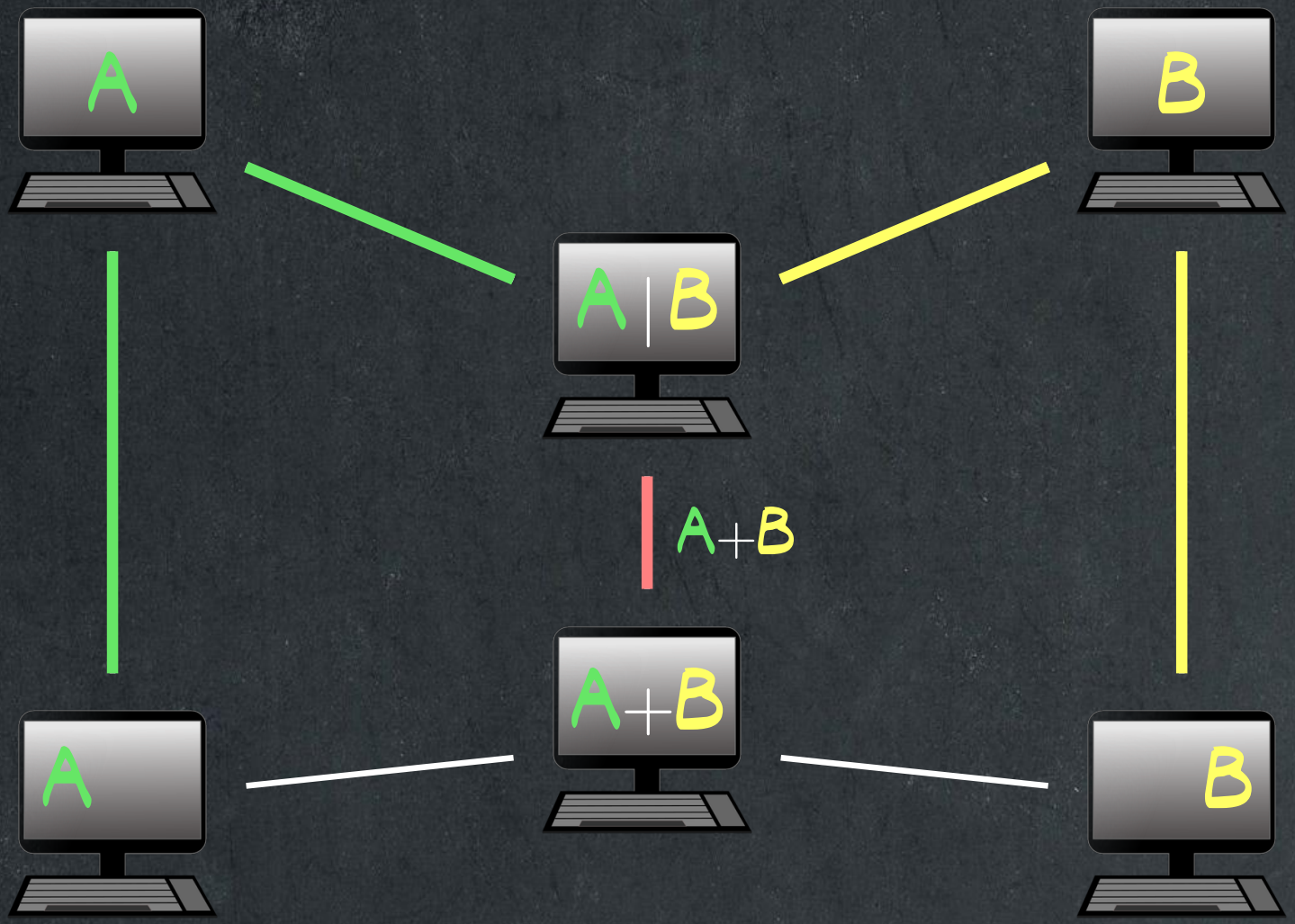
Why do we care about the rank distance?



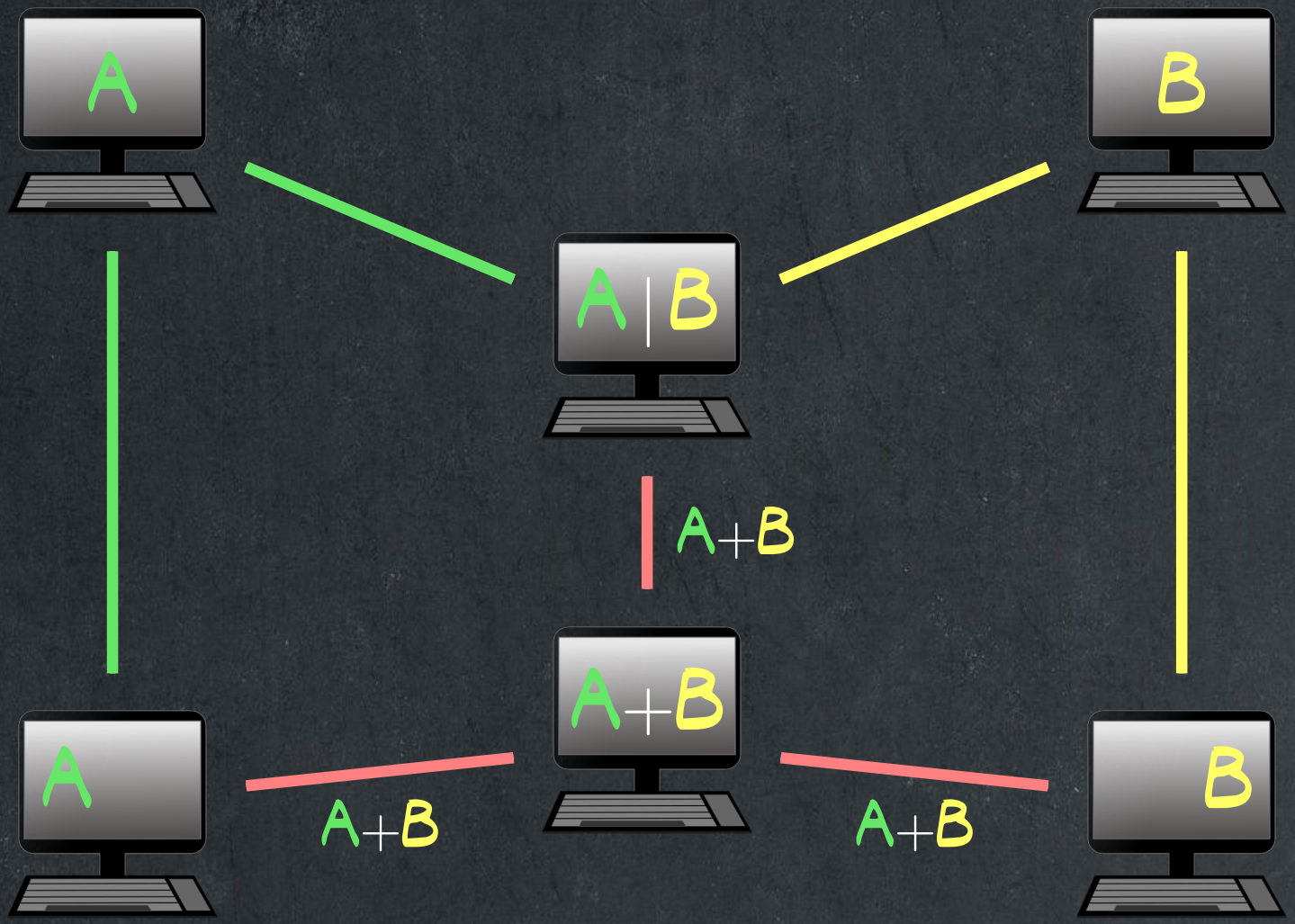
Why do we care about the rank distance?



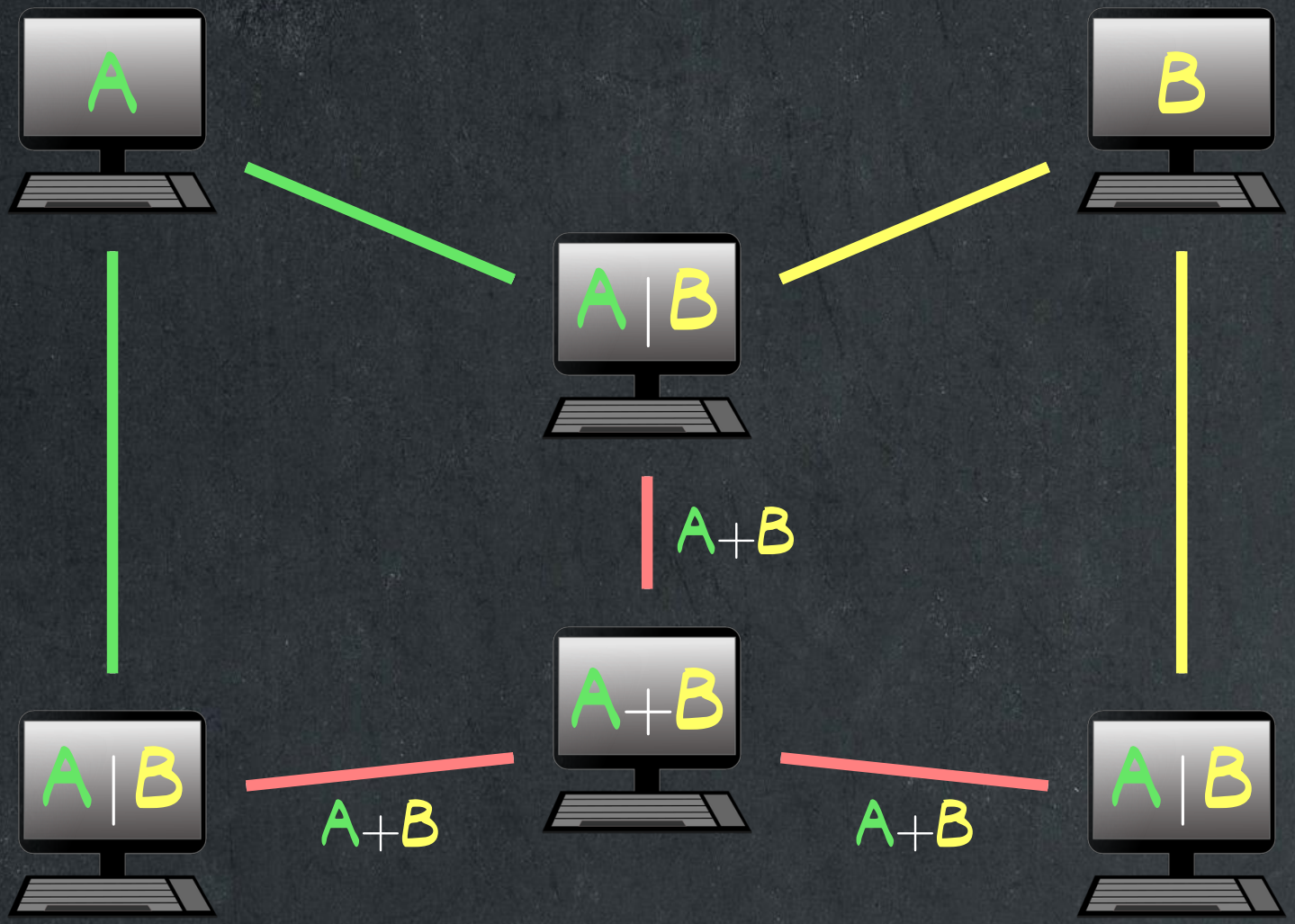
Why do we care about the rank distance?



Why do we care about the rank distance?



Why do we care about the rank distance?



More evaluation morphisms

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$ and assume that K/F is finite

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$ and assume that K/F is finite

In the definition of Gabidulin codes, we have encoutered

$$\begin{array}{rccc} ev_\varphi : & K[x;\varphi] & \to & End_F(K) \\ & f(x) & \mapsto & f(\varphi) \end{array}$$

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$ and assume that K/F is finite

In the definition of Gabidulin codes, we have encoutered

$$\begin{array}{rccc} ev_\varphi : & K[x;\varphi] & \to & End_F(K) \\ & f(x) & \mapsto & f(\varphi) \end{array}$$

More generally, if $\alpha : V \to V$ is any semi-linear mapping

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$ and assume that K/F is finite

In the definition of Gabidulin codes, we have encoutered

$$\begin{array}{rccc} ev_\varphi : & K[X;\varphi] & \to & End_F(K) \\ & f(X) & \mapsto & f(\varphi) \end{array}$$

More generally, if $\alpha : V \to V$ is any semi-linear mapping

i.e. α additive and $\forall a \in K,\ \forall x \in V,\ \alpha(ax) = \varphi(a)\,\alpha(x)$

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$ and assume that K/F is finite

In the definition of Gabidulin codes, we have encoutered

$$\begin{array}{rccc} ev_\varphi : & K[x;\varphi] & \to & End_F(K) \\ & f(x) & \mapsto & f(\varphi) \end{array}$$

More generally, if $\alpha : V \to V$ is any semi-linear mapping

i.e. α additive and $\forall a \in K,\ \forall x \in V,\ \alpha(ax) = \varphi(a)\,\alpha(x)$

we have a well-defined evaluation morphism

$$\begin{array}{rccc} ev_\alpha : & K[x;\varphi] & \to & End_F(V) \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

More evaluation morphisms

From now on, let K be a field equipped with $\varphi : K \to K$

Set $F = K^{\varphi=1}$ and assume that K/F is finite

In the definition of Gabidulin codes, we have encoutered

$$\begin{array}{rccc} ev_\varphi : & K[x;\varphi] & \to & End_F(K) \\ & f(x) & \mapsto & f(\varphi) \end{array}$$

More generally, if $\alpha : V \to V$ is any semi-linear mapping

i.e. α additive and $\forall a \in K,\ \forall x \in V,\ \alpha(ax) = \varphi(a)\,\alpha(x)$

we have a well-defined evaluation morphism

$$\begin{array}{rccc} ev_\alpha : & K[x;\varphi] & \to & End_F(V) \\ & f(x) & \mapsto & f(\alpha) \end{array}$$

Proposition

The semi-linear mappings $\alpha : K \to K$ are the $(a\varphi)$'s for $a \in K$

Linearized RS codes (after Martinez-Peñas)

Linearized RS codes (after Martinez-Peñas)

Let k, m be two integers

Linearized RS codes (after Martinez-Peñas)

Let k, m be two integers

Let $a_1, \ldots, a_m \in K^\times$ s.t. $N_{K/F}(a_i)$ are pairwise distinct

Linearized RS codes (after Martinez-Peñas)

Let k, m be two integers

Let $a_1, \ldots, a_m \in K^\times$ s.t. $N_{K/F}(a_i)$ are pairwise distinct

Let $V_1, \ldots, V_m$ be sub-F-vector spaces of K

Linearized RS codes (after Martinez-Peñas)

Let k, m be two integers

Let $a_1, \ldots, a_m \in K^\times$ s.t. $N_{K/F}(a_i)$ are pairwise distinct

Let $V_1, \ldots, V_m$ be sub-F-vector spaces of K

The associated linearized Reed Solomon code $LRS(k; a_1, V_1; \ldots; a_m, V_m)$ is the image of:

$$\begin{aligned} K[x;\varphi]_{<k} &\longrightarrow \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ f(x) &\mapsto \left(f(a_1\varphi)_{|V_1}, \ldots, f(a_m\varphi)_{|V_m}\right) \end{aligned}$$

Linearized RS codes (after Martinez-Peñas)

Let k, m be two integers

Let $a_1, \ldots, a_m \in K^X$ s.t. $N_{K/F}(a_i)$ are pairwise distinct

Let $V_1, \ldots, V_m$ be sub-F-vector spaces of K

The associated linearized Reed Solomon code $LRS(k; a_1, V_1; \ldots; a_m, V_m)$ is the image of:

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & Hom_F(V_1, K) \times \cdots \times Hom_F(V_m, K) \\ f(x) & \mapsto & (f(a_1\varphi)_{|V_1}, \ \ldots, \ f(a_m\varphi)_{|V_m}) \end{array}$$

Theorem

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

dimension $= k$

minimal distance $= n - k + 1$

Linearized RS codes (after Martinez-Peñas)

Let k, m be two integers

Let $a_1, \dots, a_m \in K^\times$ s.t. $N_{K/F}(a_i)$ are pairwise distinct

Let $V_1, \dots, V_m$ be sub-F-vector spaces of K

The associated linearized Reed Solomon code $LRS(k; a_1, V_1; \dots; a_m, V_m)$ is the image of:

$$\begin{array}{ccc} K[x;\varphi]_{<k} & \longrightarrow & \mathrm{Hom}_F(V_1, K) \times \cdots \times \mathrm{Hom}_F(V_m, K) \\ f(x) & \mapsto & (f(a_1\varphi)_{|V_1}, \dots, f(a_m\varphi)_{|V_m}) \end{array}$$

Theorem

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

dimension $= k$

minimal distance $= n - k + 1$

for the sum-rank distance: $w_{s\text{-}rk}(U_1, \dots, U_m) = \sum_{i=1}^{m} \mathrm{rank}(U_i)$

More on Ore polynomials

More on Ore polynomials

Define $r = \dim_F K$

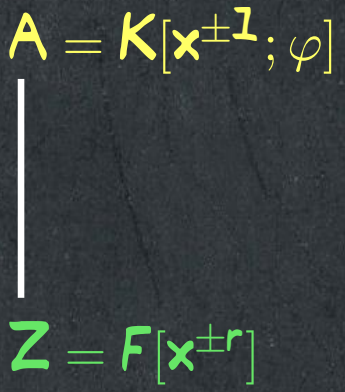
More on Ore polynomials

Define $r = \dim_F K$

$$A = K[x^{\pm 1}; \varphi]$$

More on Ore polynomials

Define $r = \dim_F K$



More on Ore polynomials

Define $r = \dim_F K$

$A = K[x^{\pm 1}; \varphi]$

|

$Z = F[x^{\pm r}]$ centre

More on Ore polynomials

Define $r = \dim_F K$

$$A = K[x^{\pm 1}; \varphi]$$
$$|$$
$$C = K[x^{\pm r}]$$
$$|$$
$$Z = F[x^{\pm r}] \qquad \text{centre}$$

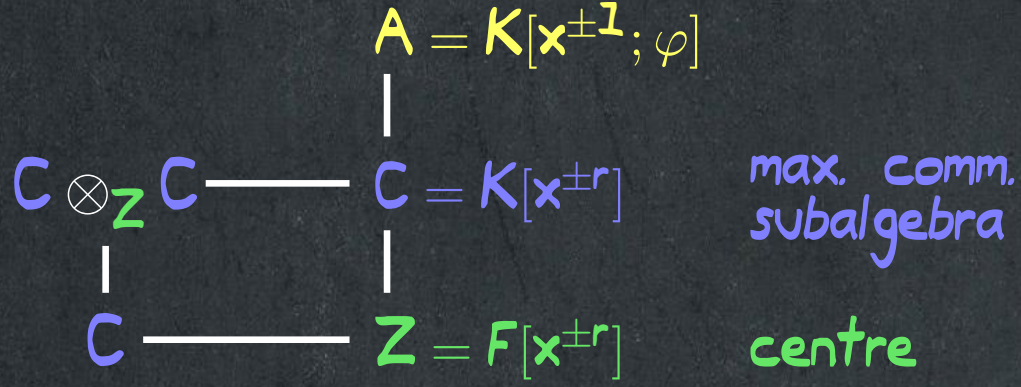
More on Ore polynomials

Define $r = \dim_F K$

$$A = K[x^{\pm 1}; \varphi]$$
$$|$$
$$C = K[x^{\pm r}] \qquad \text{max. comm. subalgebra}$$
$$|$$
$$Z = F[x^{\pm r}] \qquad \text{centre}$$

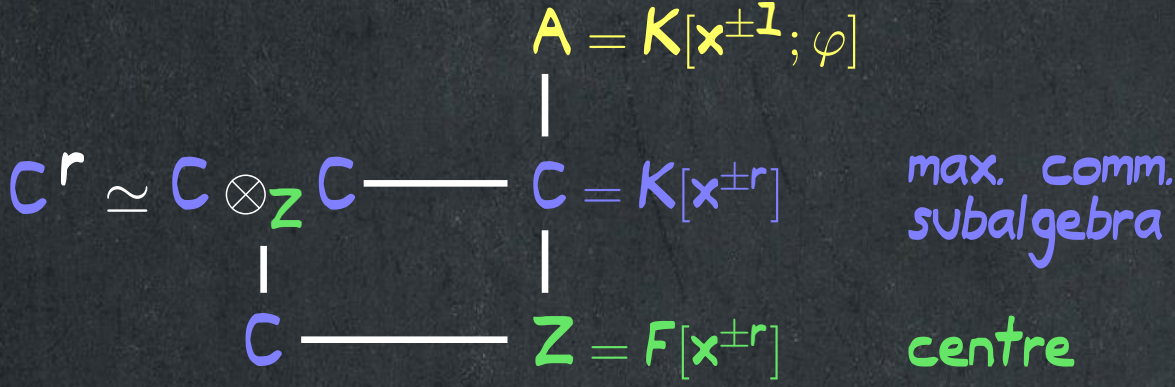
More on Ore polynomials

Define $r = \dim_F K$



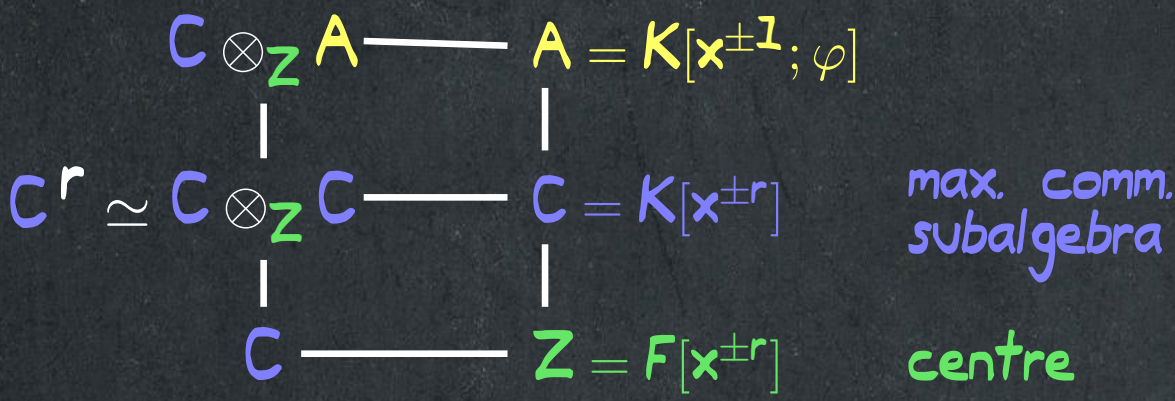
More on Ore polynomials

Define $r = \dim_F K$



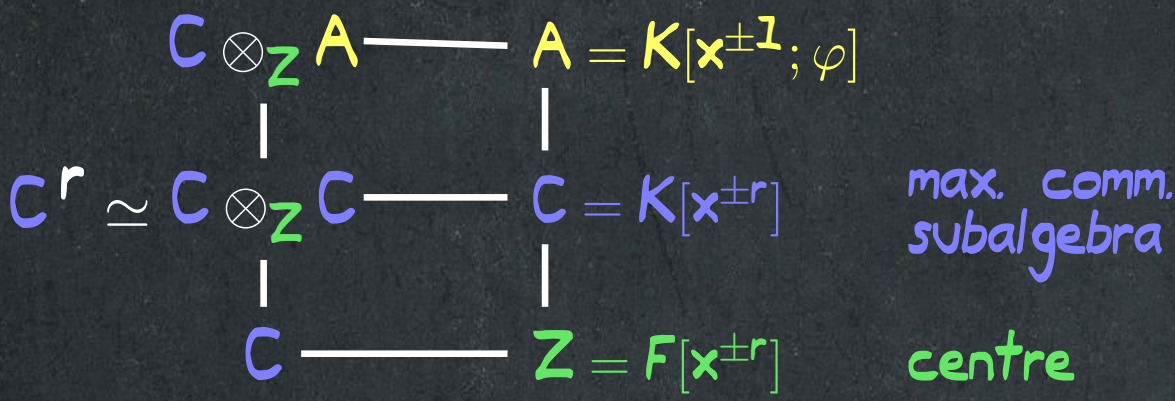
More on Ore polynomials

Define $r = \dim_F K$



More on Ore polynomials

Define $r = \dim_F K$

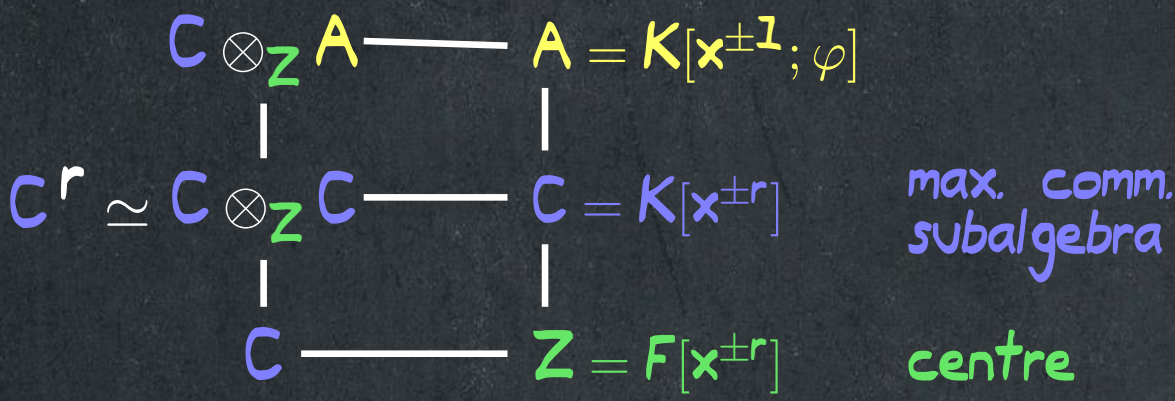


Proposition

$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A)$

More on Ore polynomials

Define $r = \dim_F K$

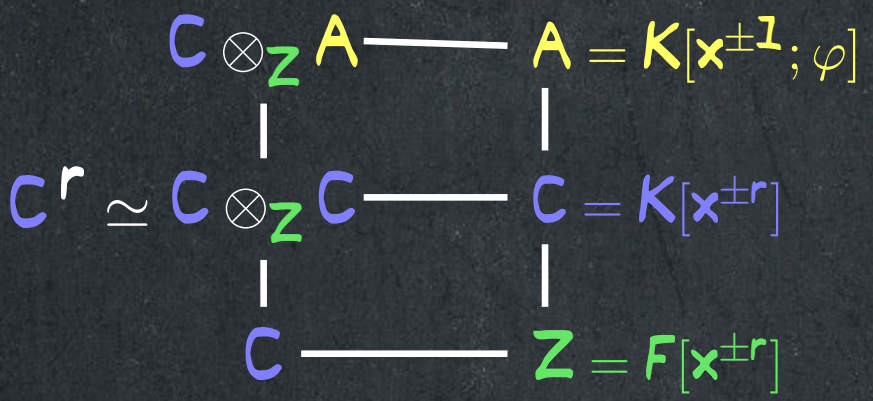


Proposition

$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

More on Ore polynomials

Define $r = \dim_F K$

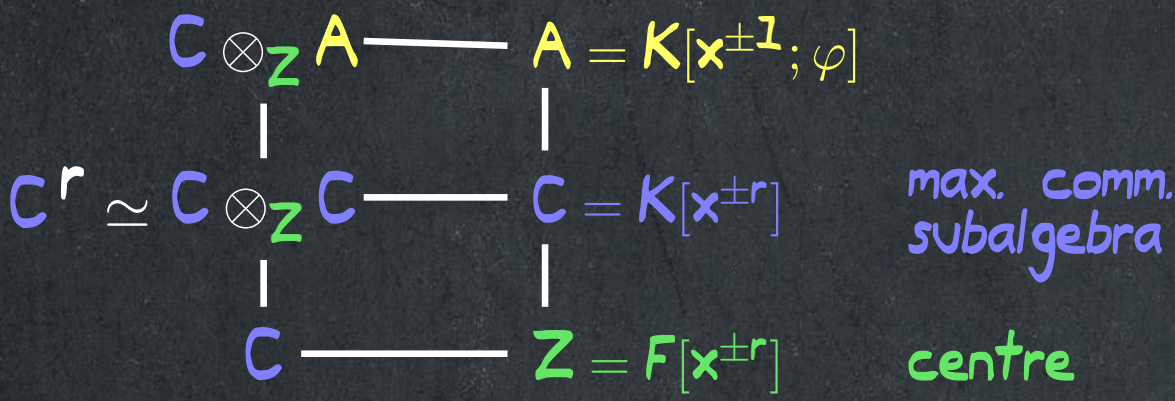


Proposition

$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

More on Ore polynomials

Define $r = \dim_F K$



Proposition

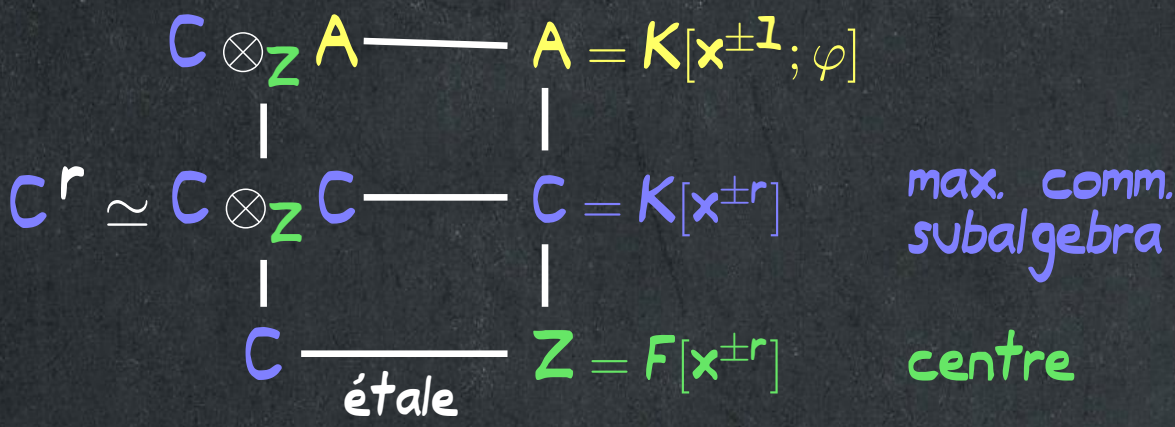
$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

Consequences

A is Azumaya

More on Ore polynomials

Define $r = \dim_F K$



Proposition

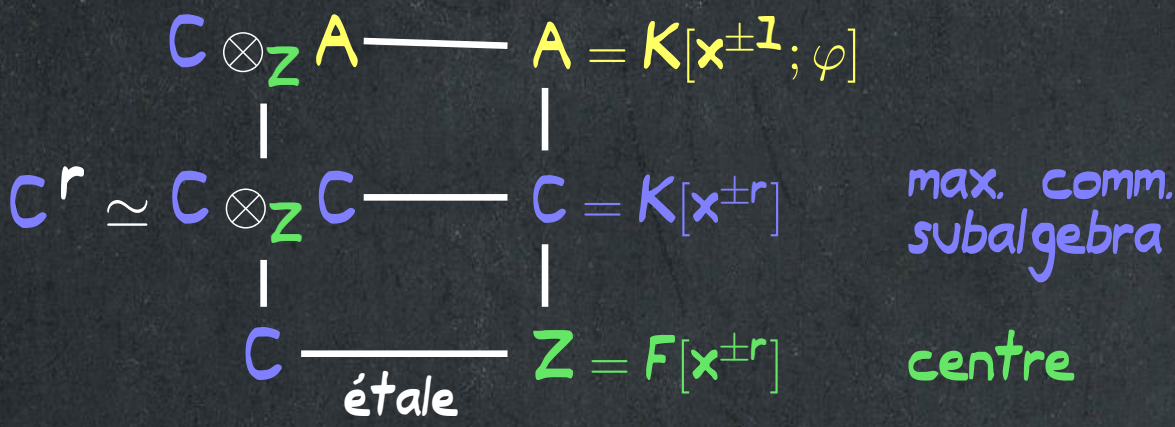
$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

Consequences

A is Azumaya

More on Ore polynomials

Define $r = \dim_F K$



Proposition

$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

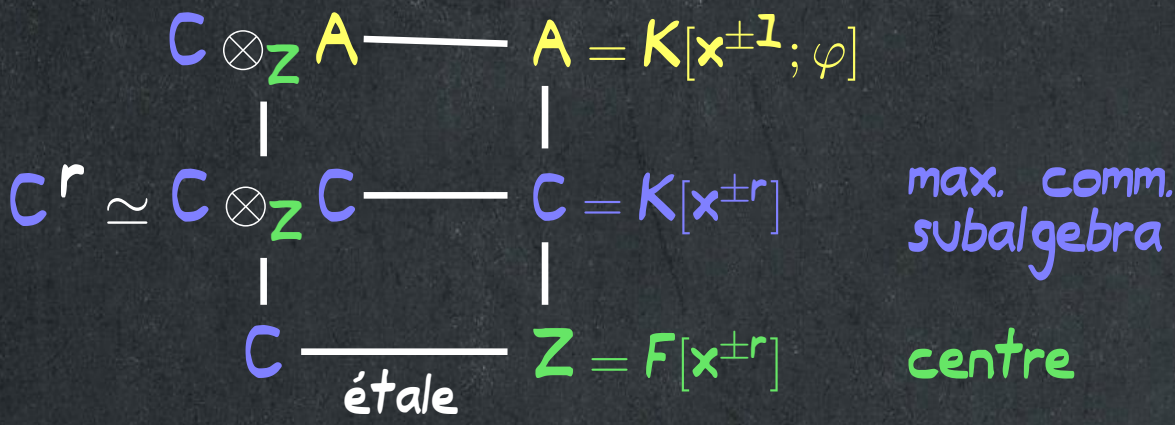
Consequences

A is Azumaya

Reduced trace $T_{rd} : A \to Z$

More on Ore polynomials

Define $r = \dim_F K$



Proposition

$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

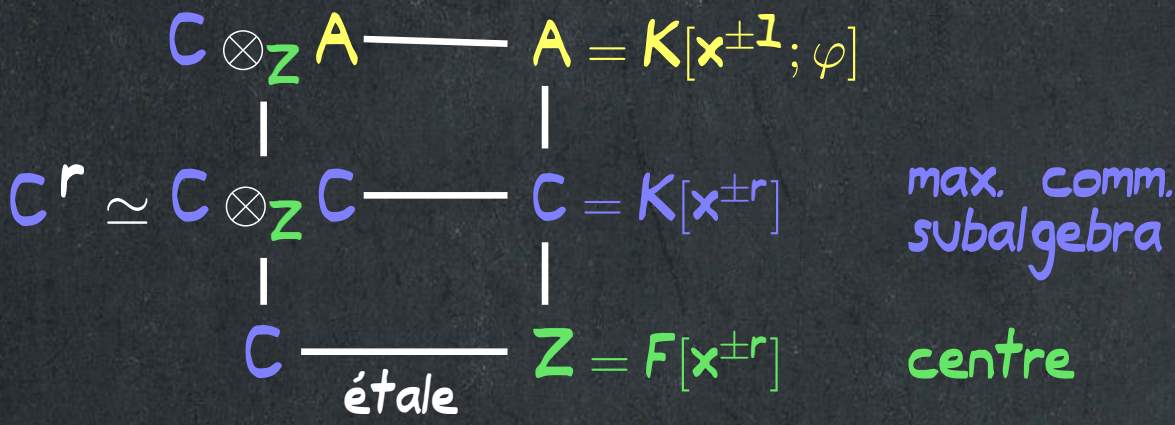
Consequences

A is Azumaya

Reduced trace $T_{rd} : A \to Z$ $\quad T_{rd}\left(\sum a_i x^i\right) = \sum Tr_{K/F}(a_{ri}) x^{ri}$

More on Ore polynomials

Define $r = \dim_F K$



Proposition

$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

Consequences

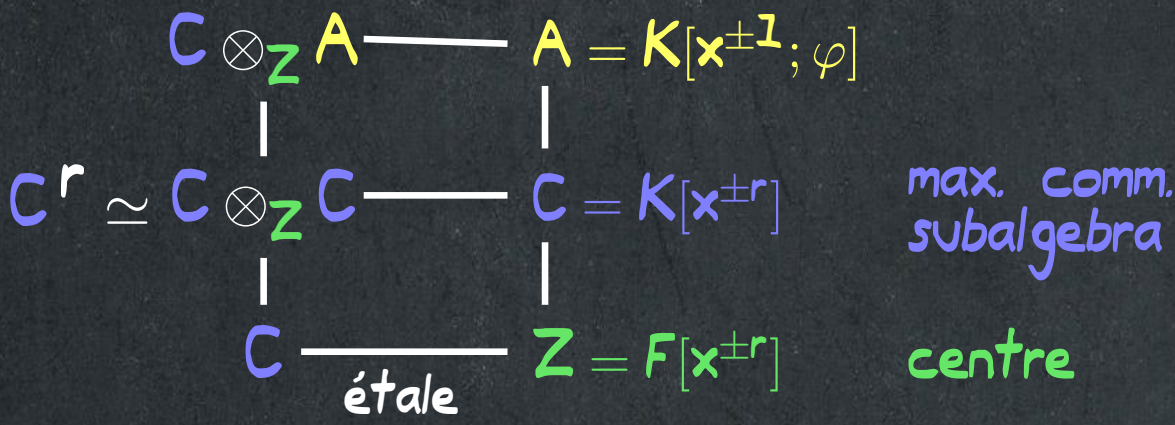
A is Azumaya

Reduced trace $T_{rd} : A \to Z$ $\quad T_{rd}\left(\sum a_i x^i\right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri}$

Reduced norm $N_{rd} : A \to Z$

More on Ore polynomials

Define $r = \dim_F K$



Proposition

$$C \otimes_Z A \xrightarrow{\sim} \mathrm{End}_C(A) \simeq M_{r\times r}(C)$$
$$c \otimes a \mapsto (x \mapsto c\,x\,a)$$

Consequences

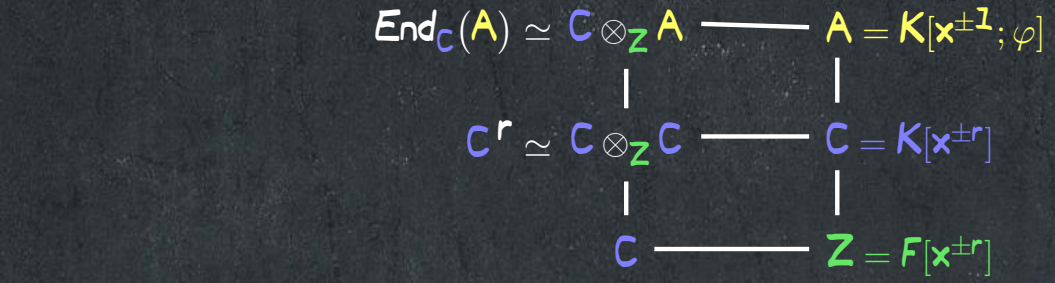
A is Azumaya

Reduced trace $T_{rd} : A \to Z$ $\quad T_{rd}\left(\sum a_i x^i\right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri}$

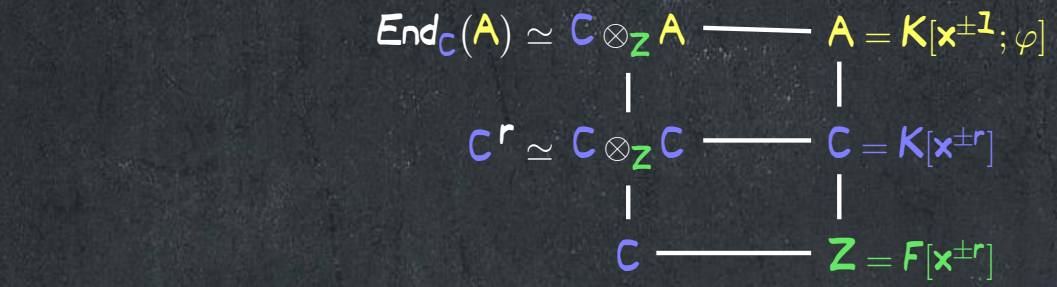
Reduced norm $N_{rd} : A \to Z$ $\quad N_{rd}(x - a) = x^r - N_{K/F}(a)$

A geometric perspective on LRS codes

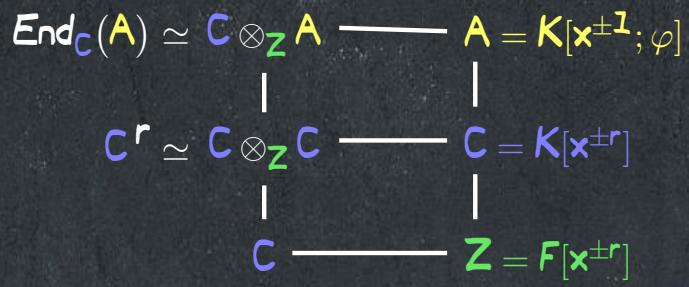
A geometric perspective on LRS codes

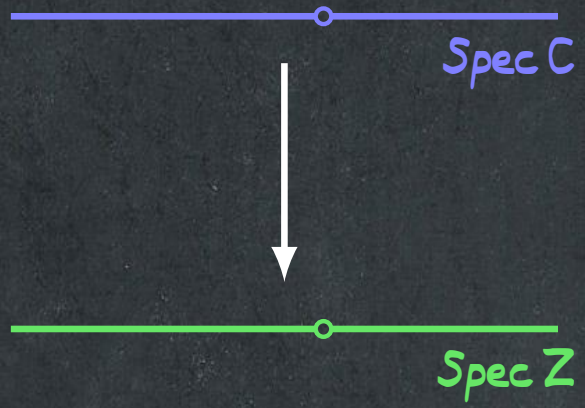


A geometric perspective on LRS codes

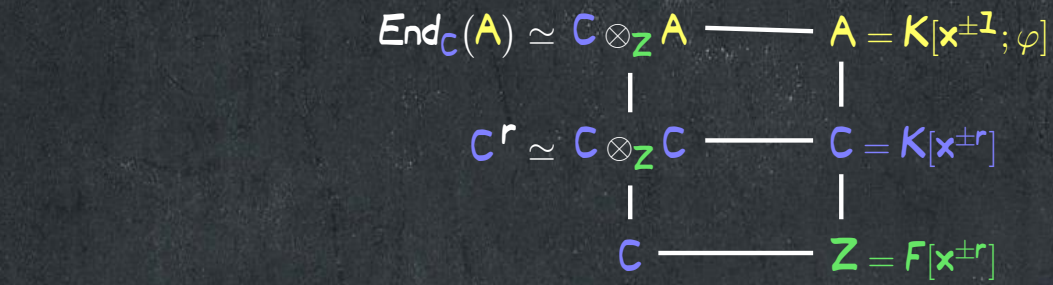


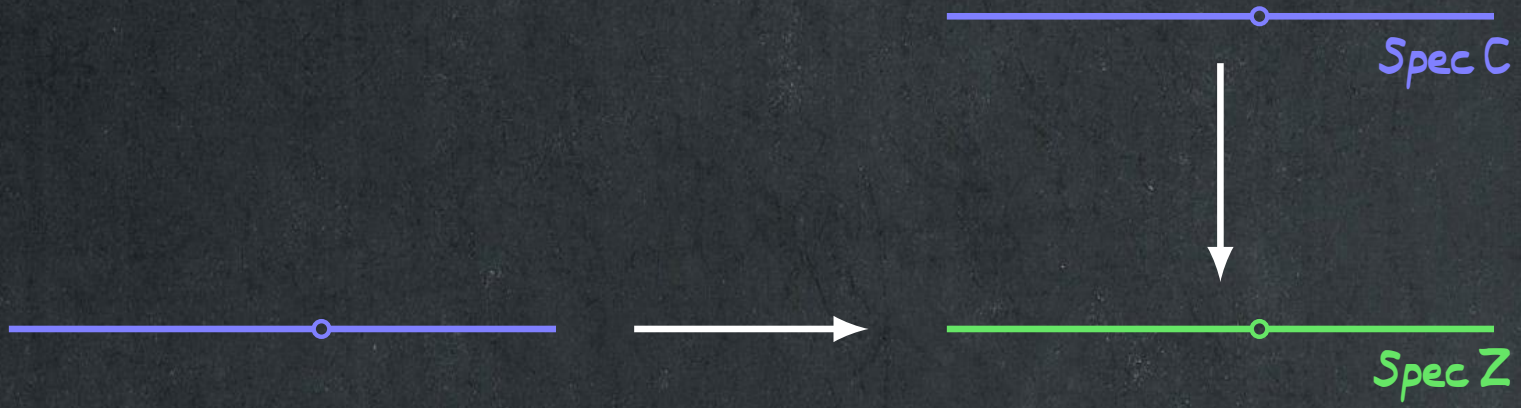
A geometric perspective on LRS codes





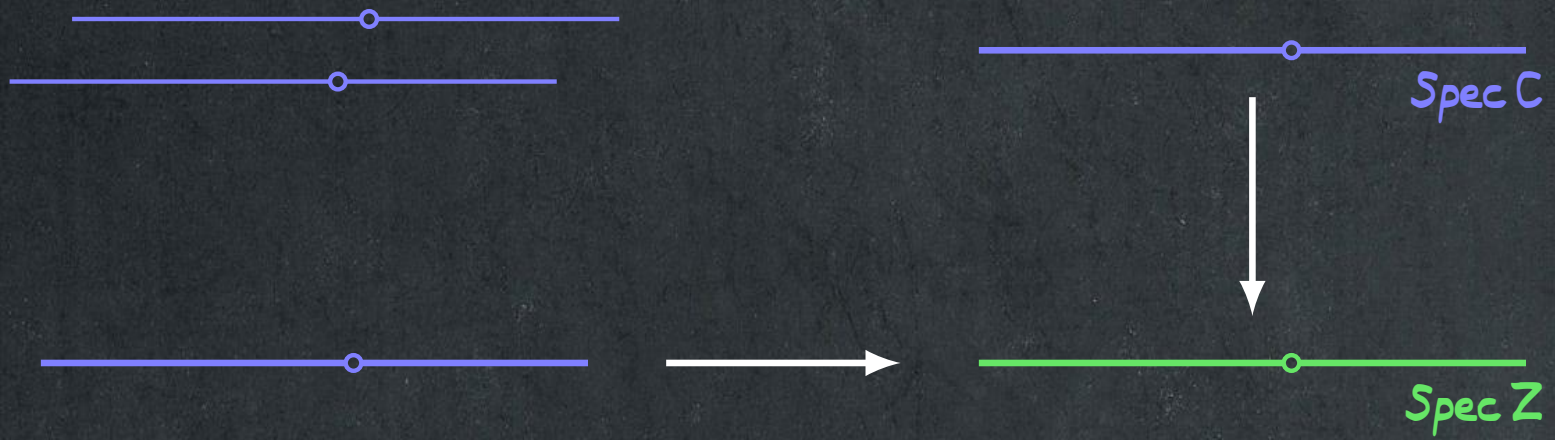
A geometric perspective on LRS codes





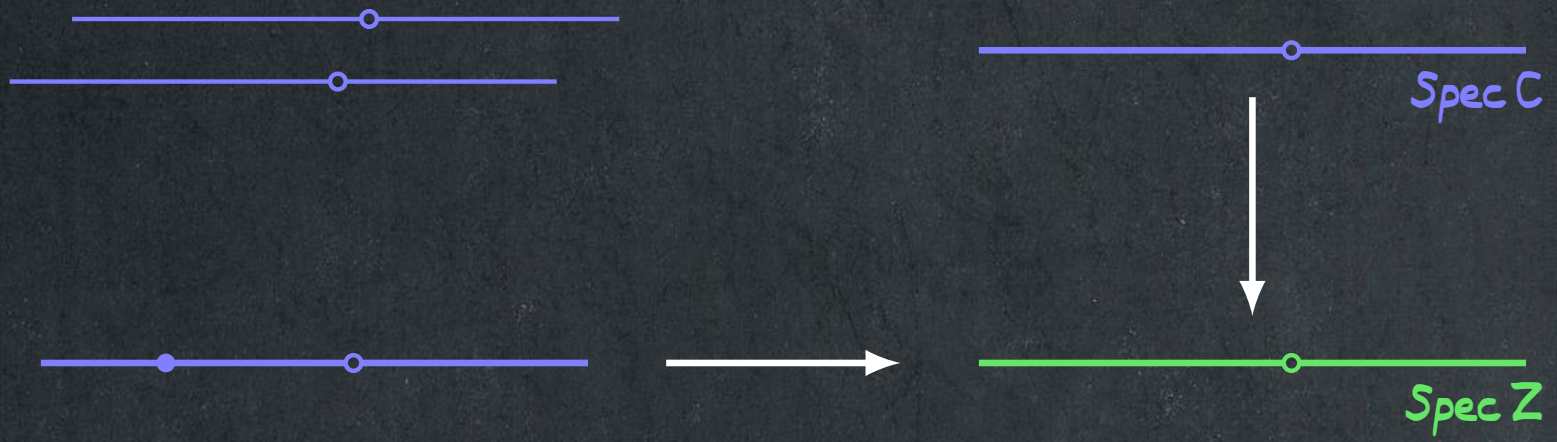
A geometric perspective on LRS codes

$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



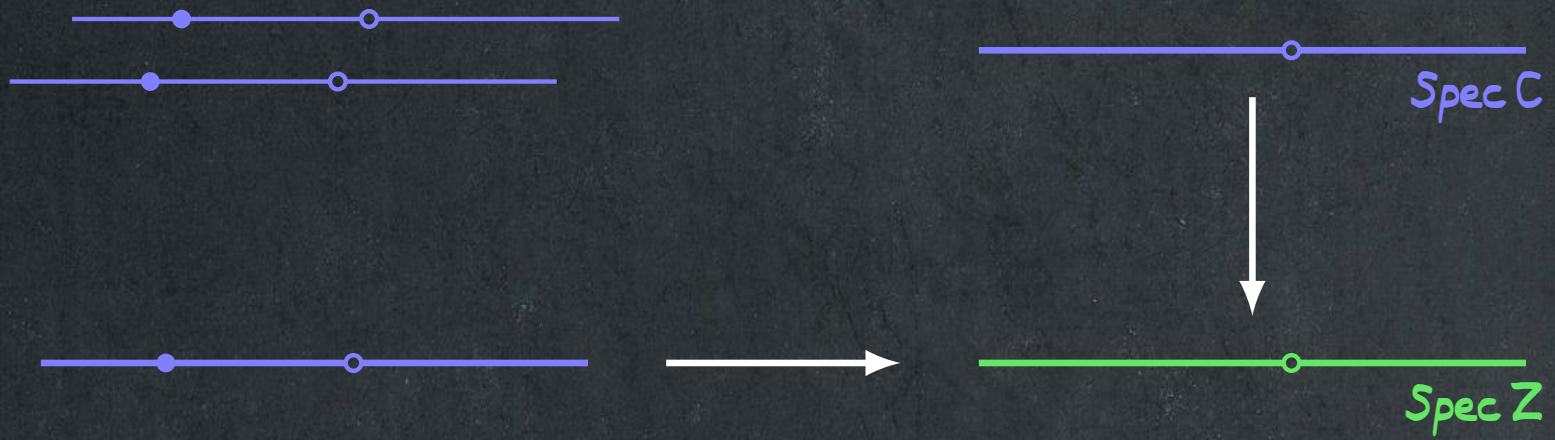
A geometric perspective on LRS codes

$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$

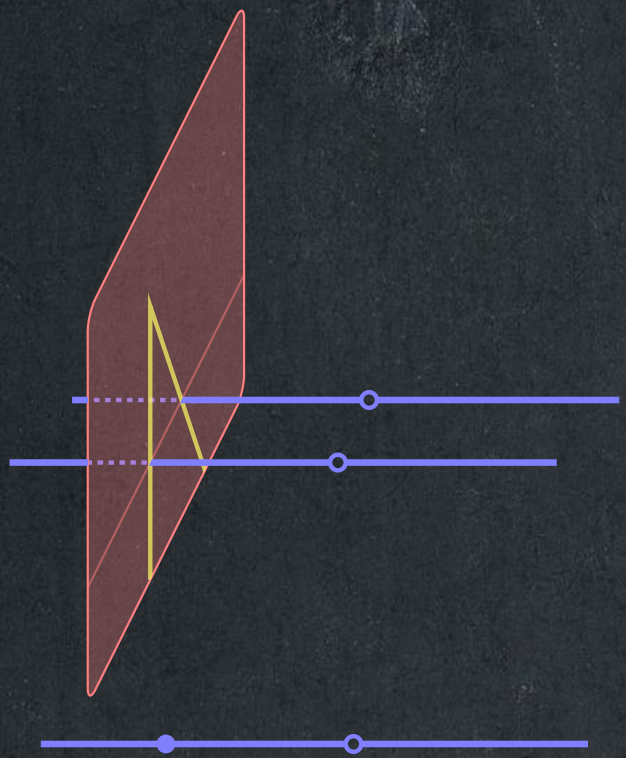


A geometric perspective on LRS codes

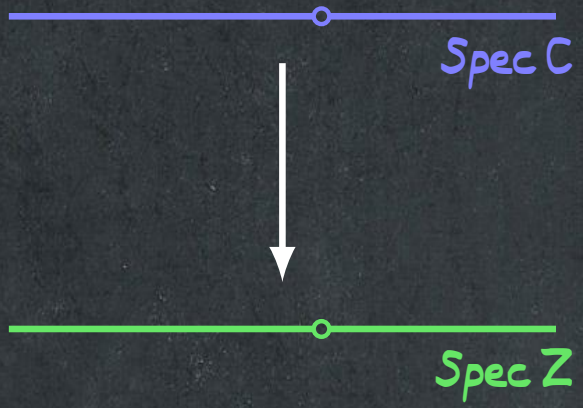
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



A geometric perspective on LRS codes

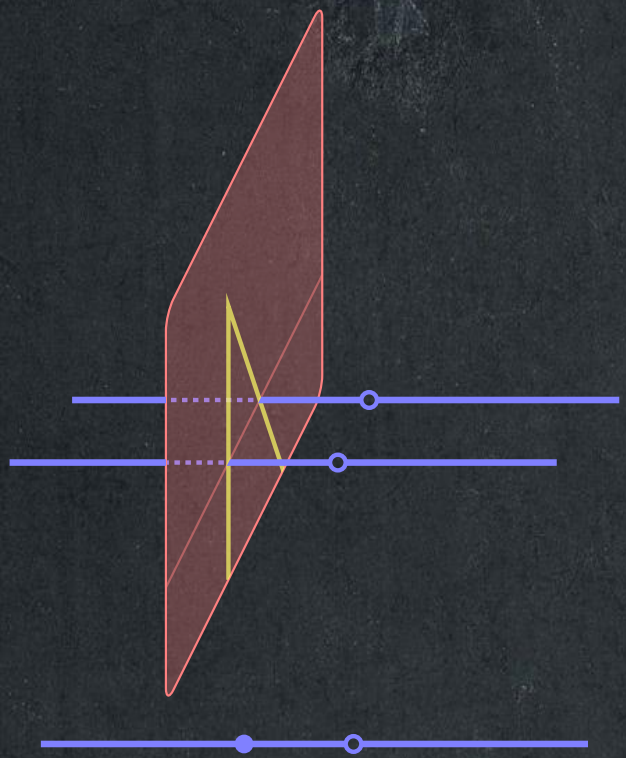


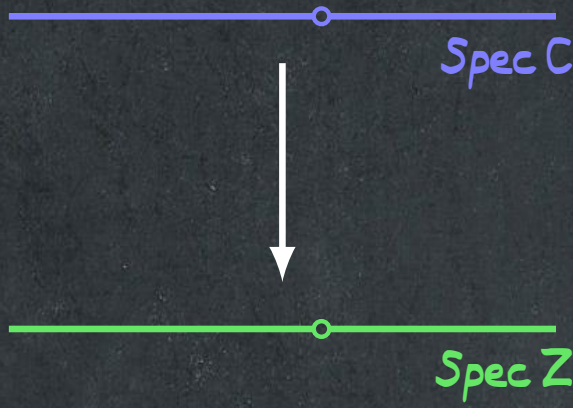
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



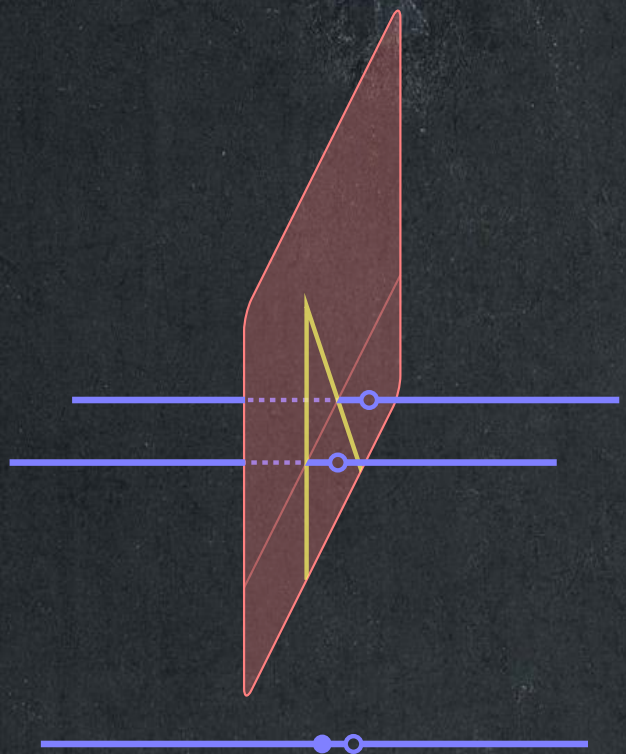
A geometric perspective on LRS codes

$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$

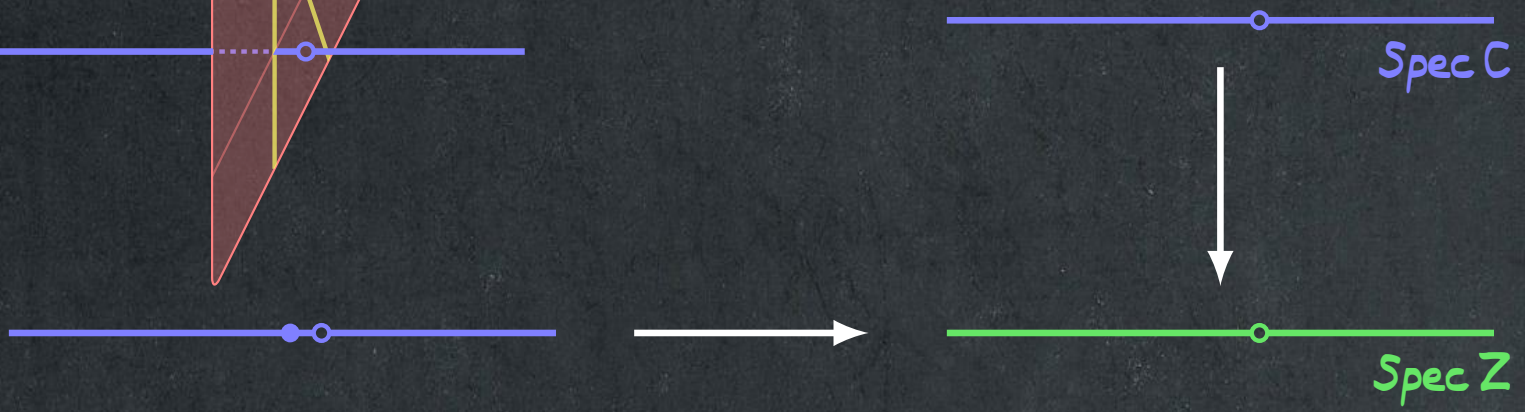




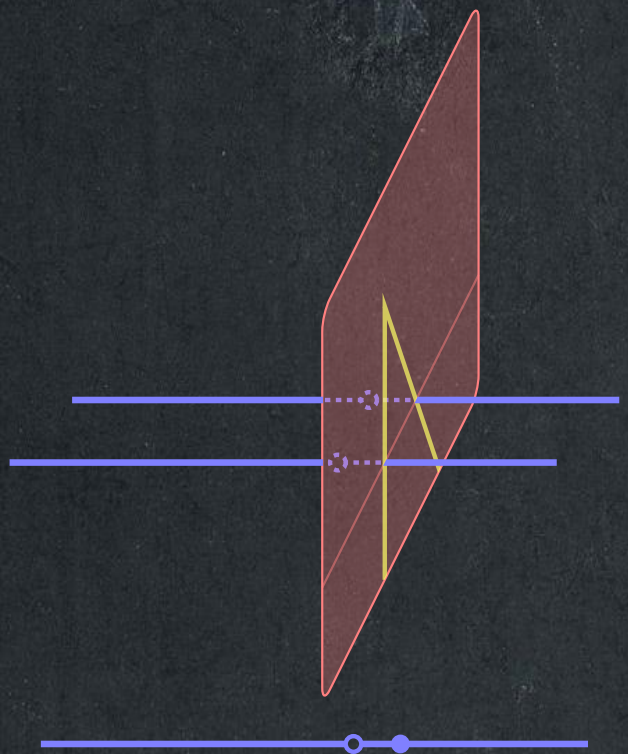
A geometric perspective on LRS codes



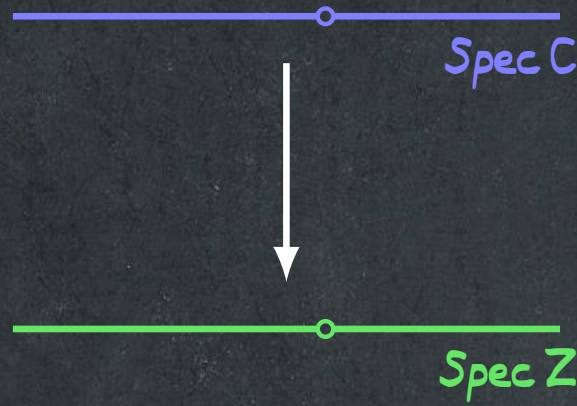
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



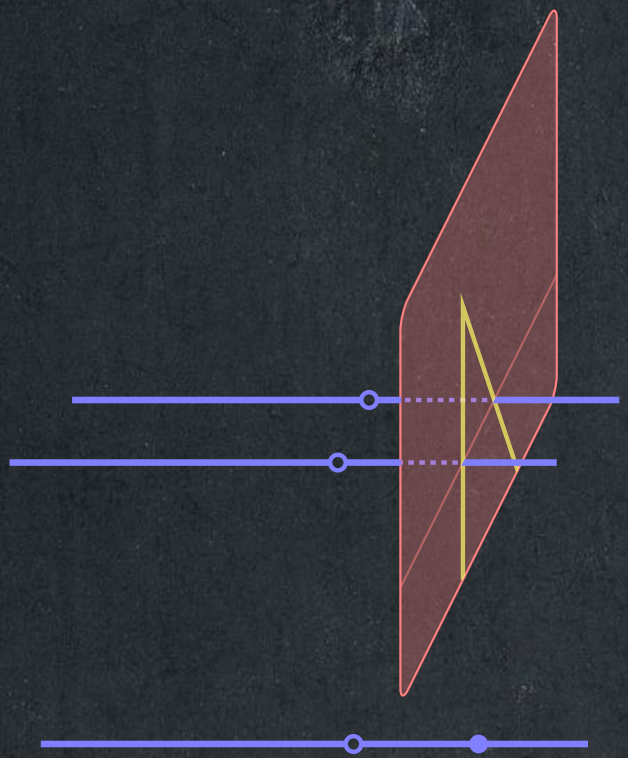
A geometric perspective on LRS codes



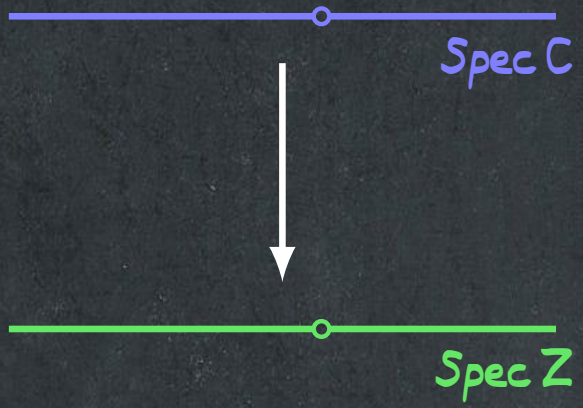
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ \vdots & & \vdots \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ \vdots & & \vdots \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



A geometric perspective on LRS codes

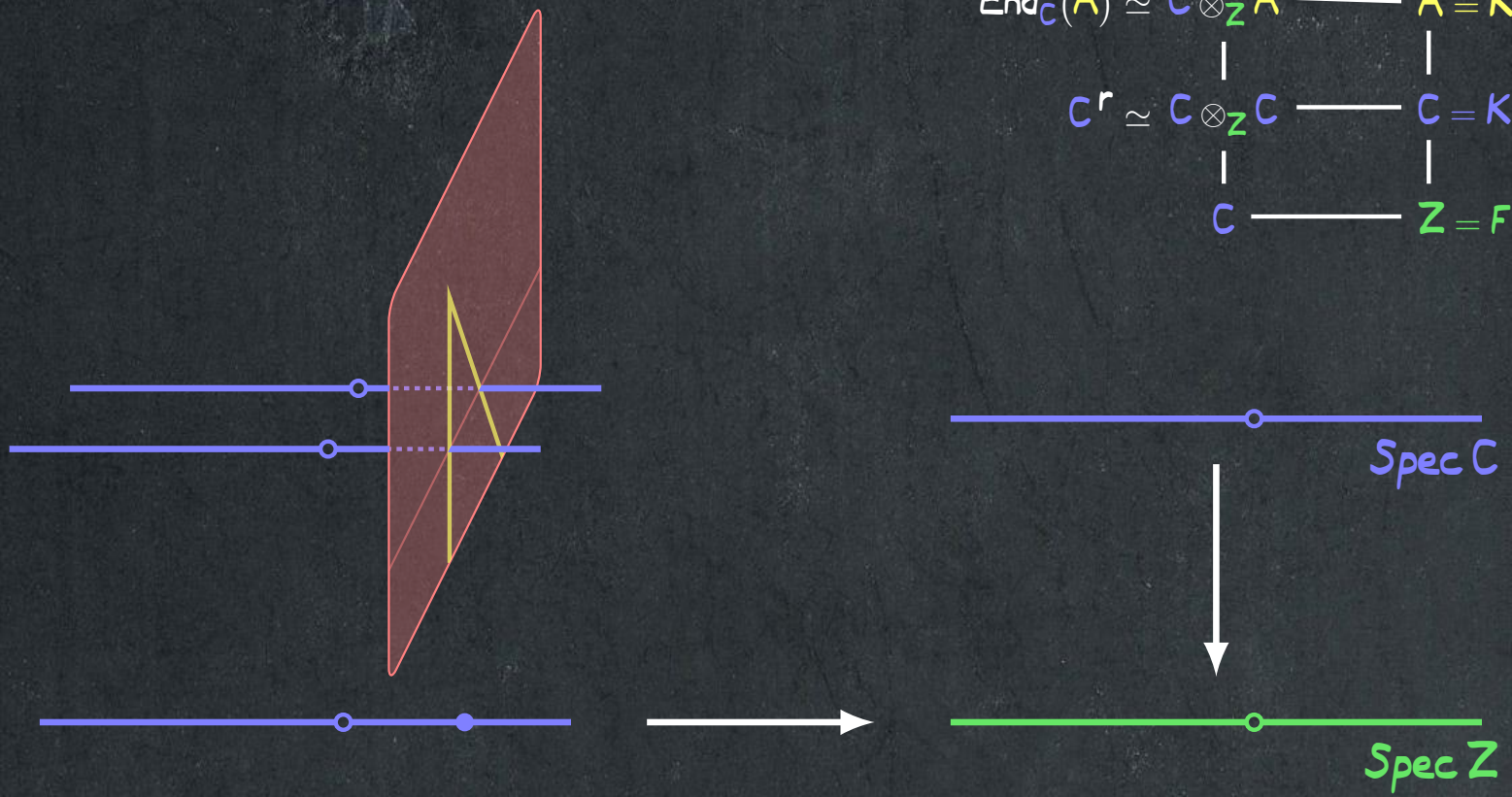


$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ \vdots & & \vdots \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ \vdots & & \vdots \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



A geometric perspective on LRS codes

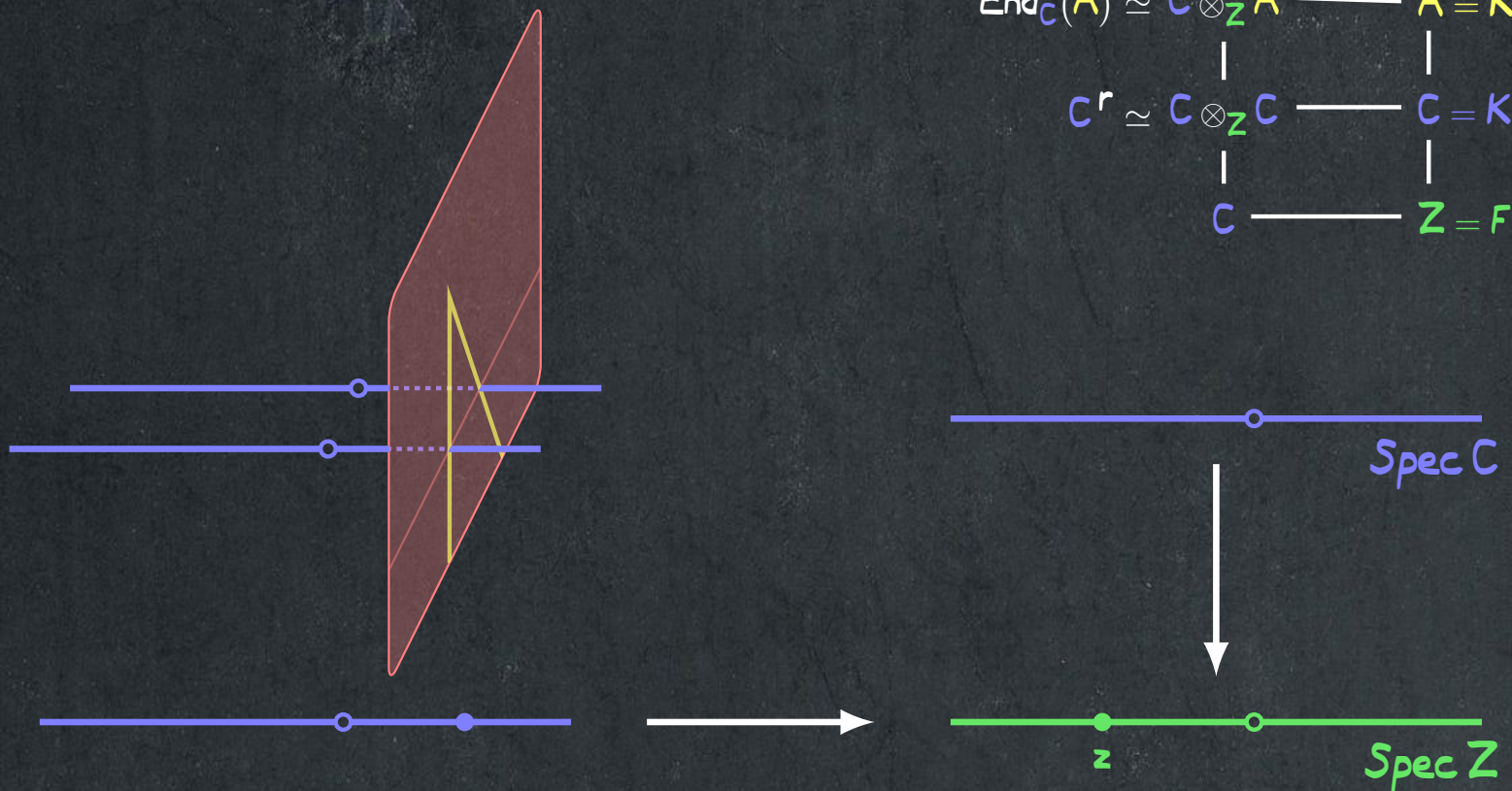
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



$$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$$

A geometric perspective on LRS codes

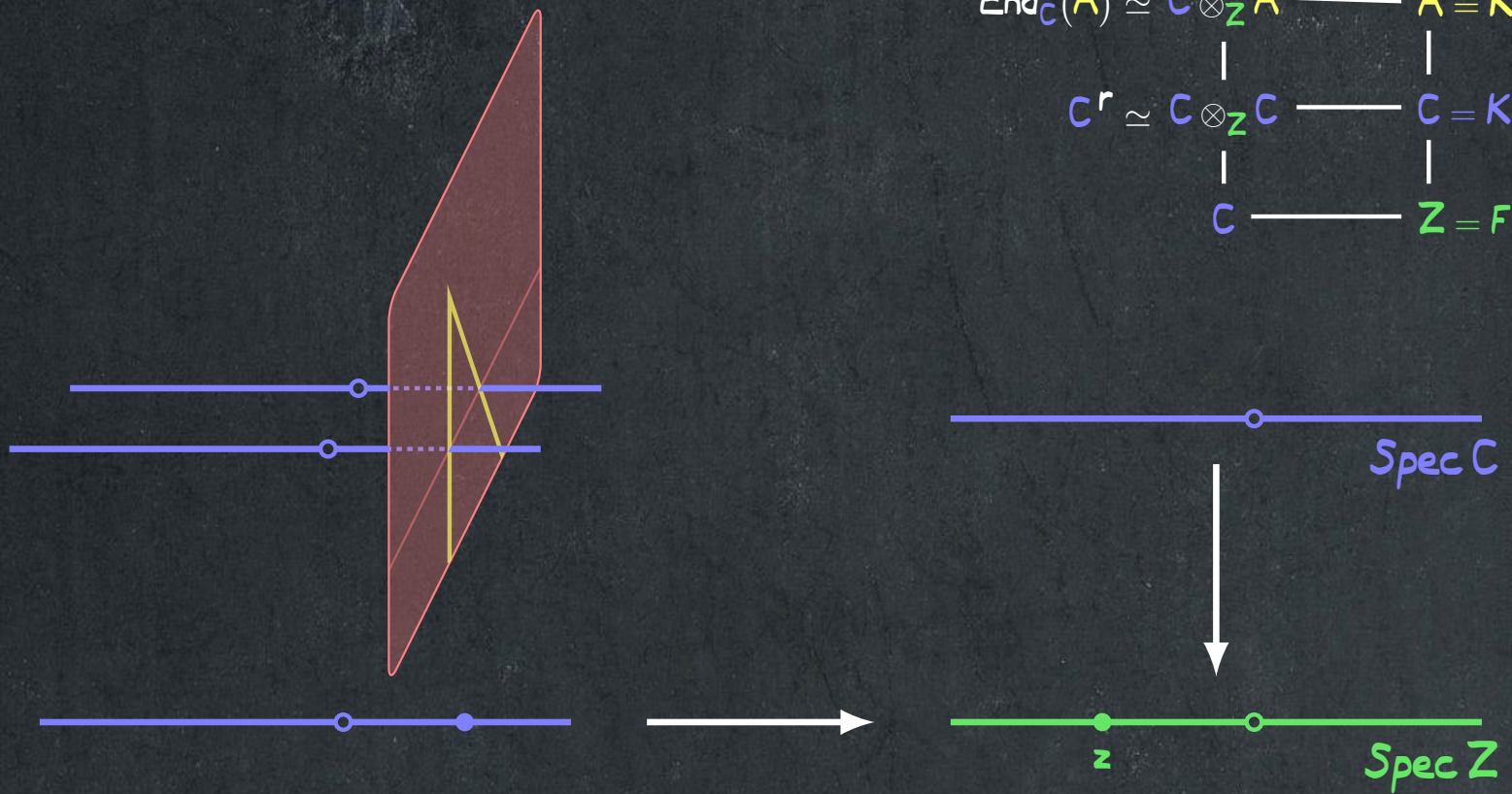
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



$$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$$

A geometric perspective on LRS codes

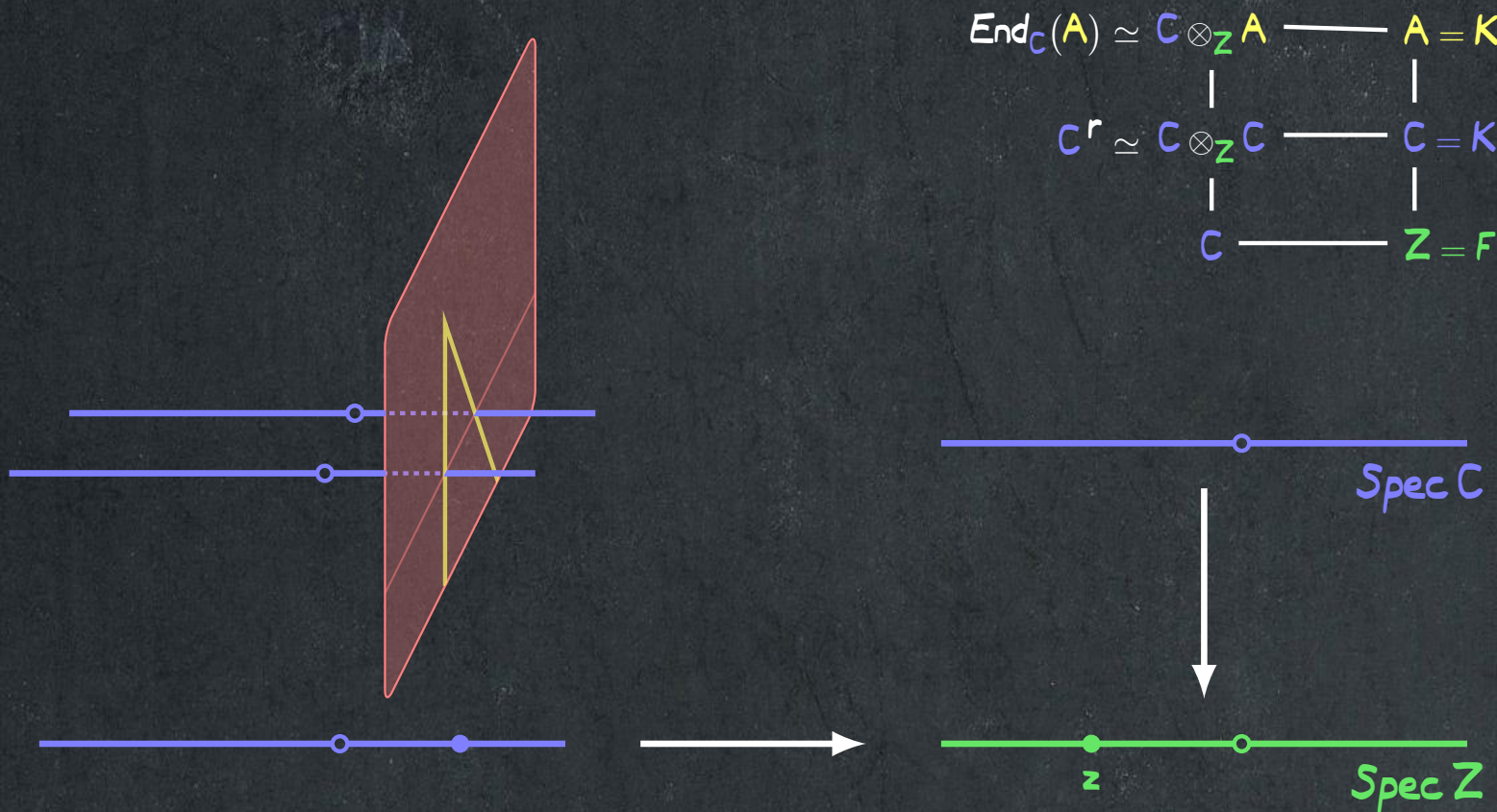
$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$



$$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$$

$$A_z = A/(x^r - z)$$

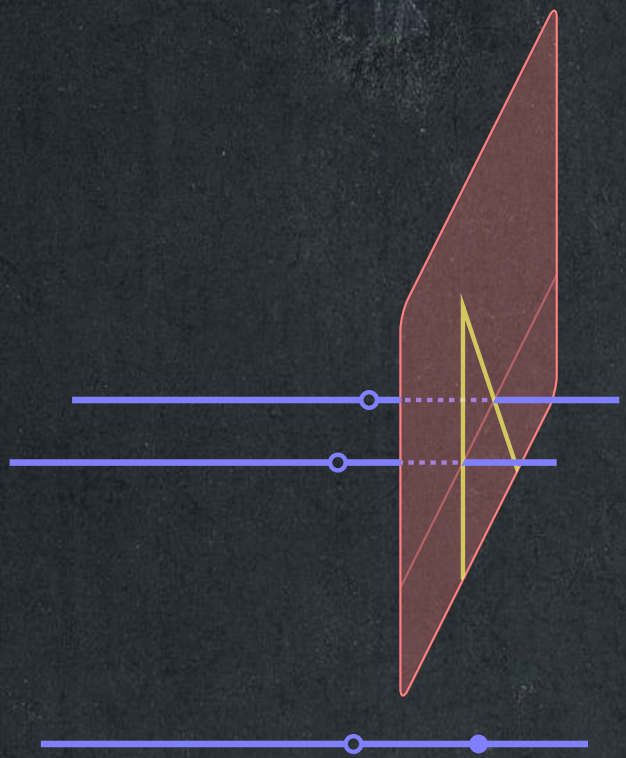
A geometric perspective on LRS codes



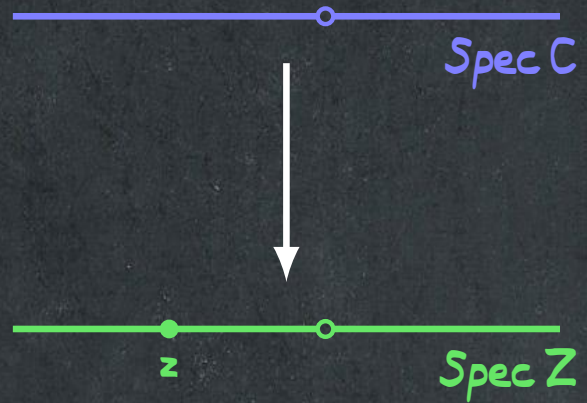
$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$

$A_z = A/(x^r - z)$ simple central algebra over F

A geometric perspective on LRS codes



$$\begin{array}{ccc} \mathrm{End}_C(A) \simeq C \otimes_Z A & \text{——} & A = K[x^{\pm 1}; \varphi] \\ | & & | \\ C^r \simeq C \otimes_Z C & \text{——} & C = K[x^{\pm r}] \\ | & & | \\ C & \text{——} & Z = F[x^{\pm r}] \end{array}$$

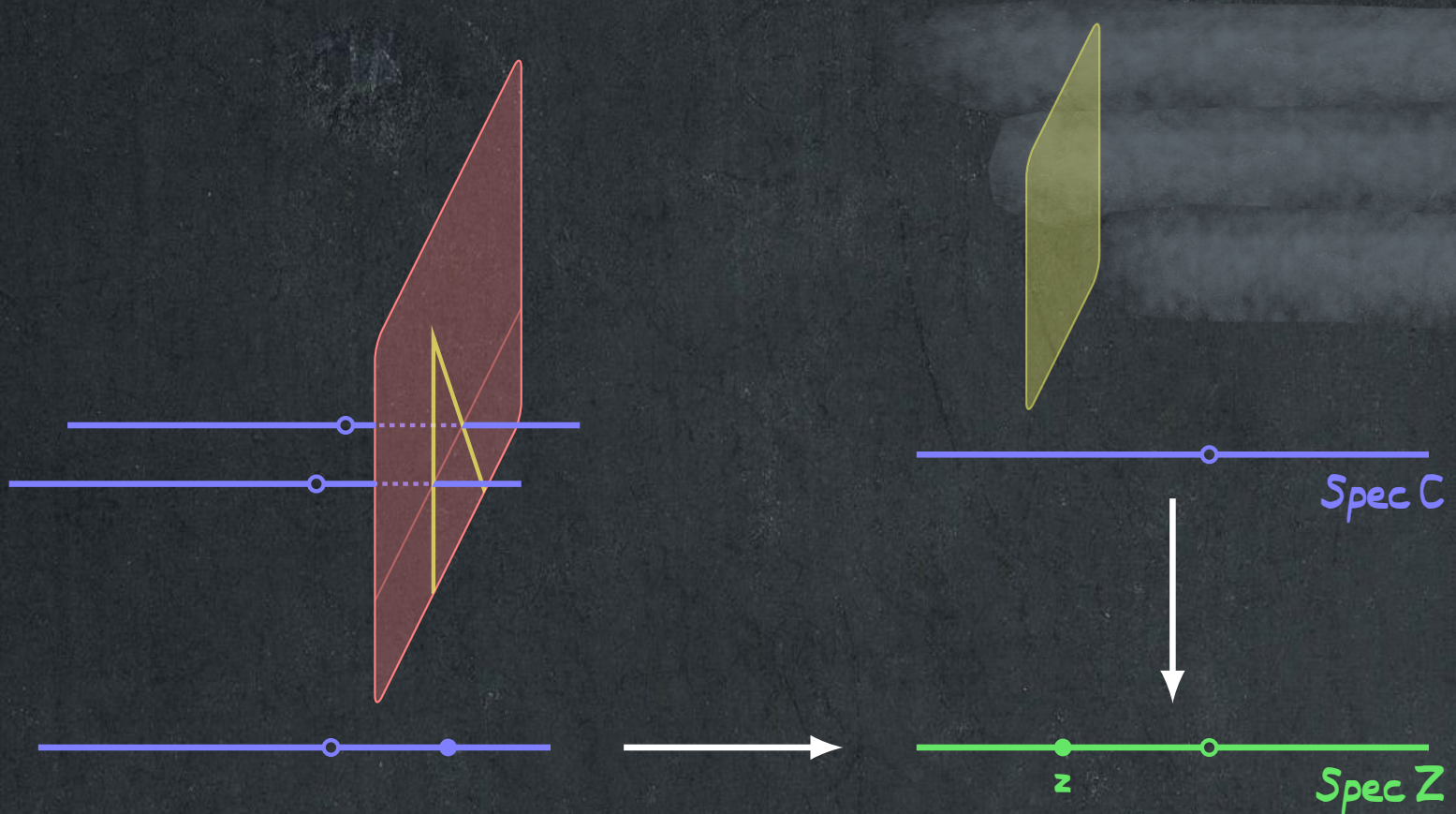


$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$

$A_z = A/(x^r - z)$ simple central algebra over F

It is split $\iff z = N_{K/F}(a)$

A geometric perspective on LRS codes

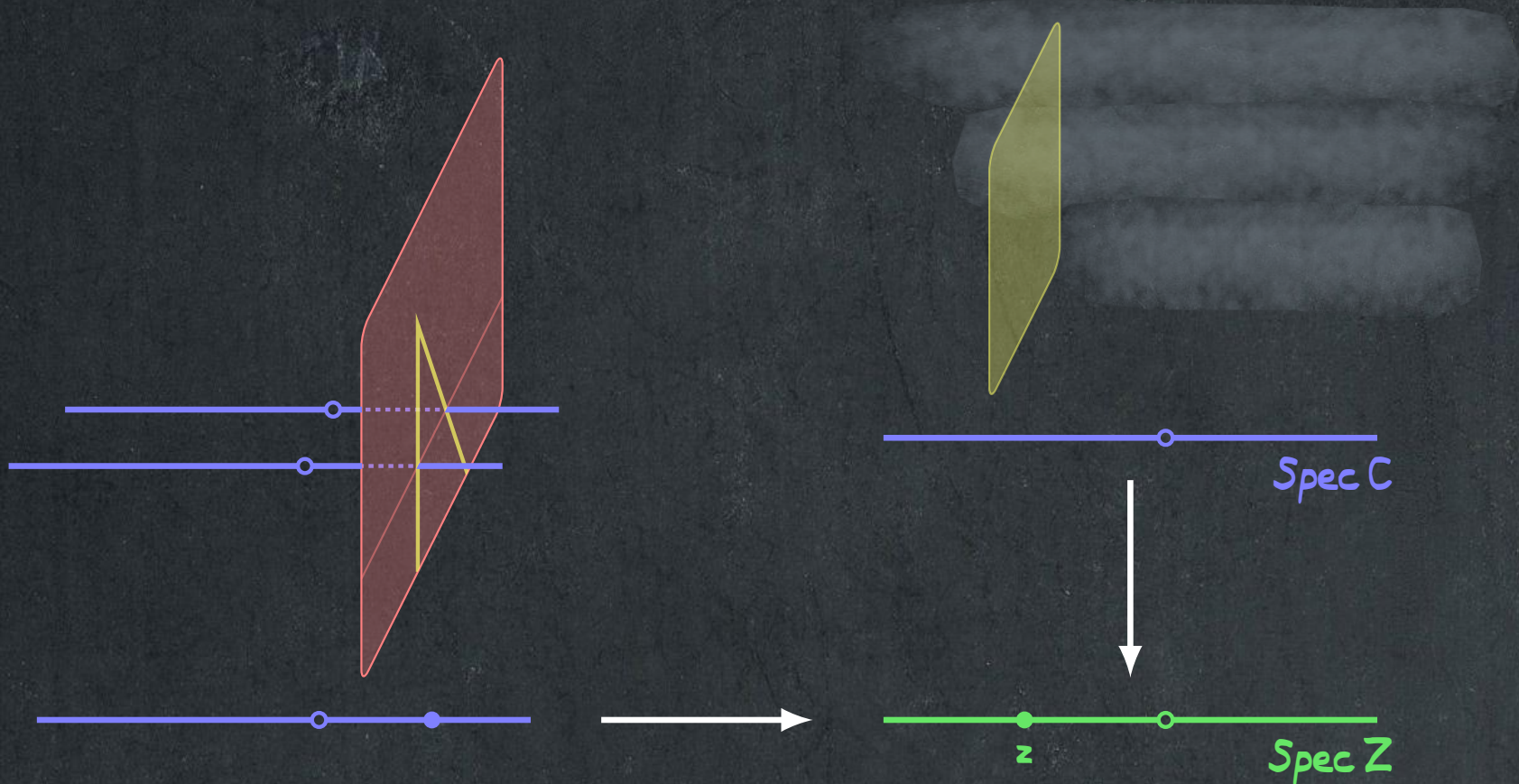


$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$

$A_z = A/(x^r - z)$ simple central algebra over F

It is split $\iff z = N_{K/F}(a)$

A geometric perspective on LRS codes



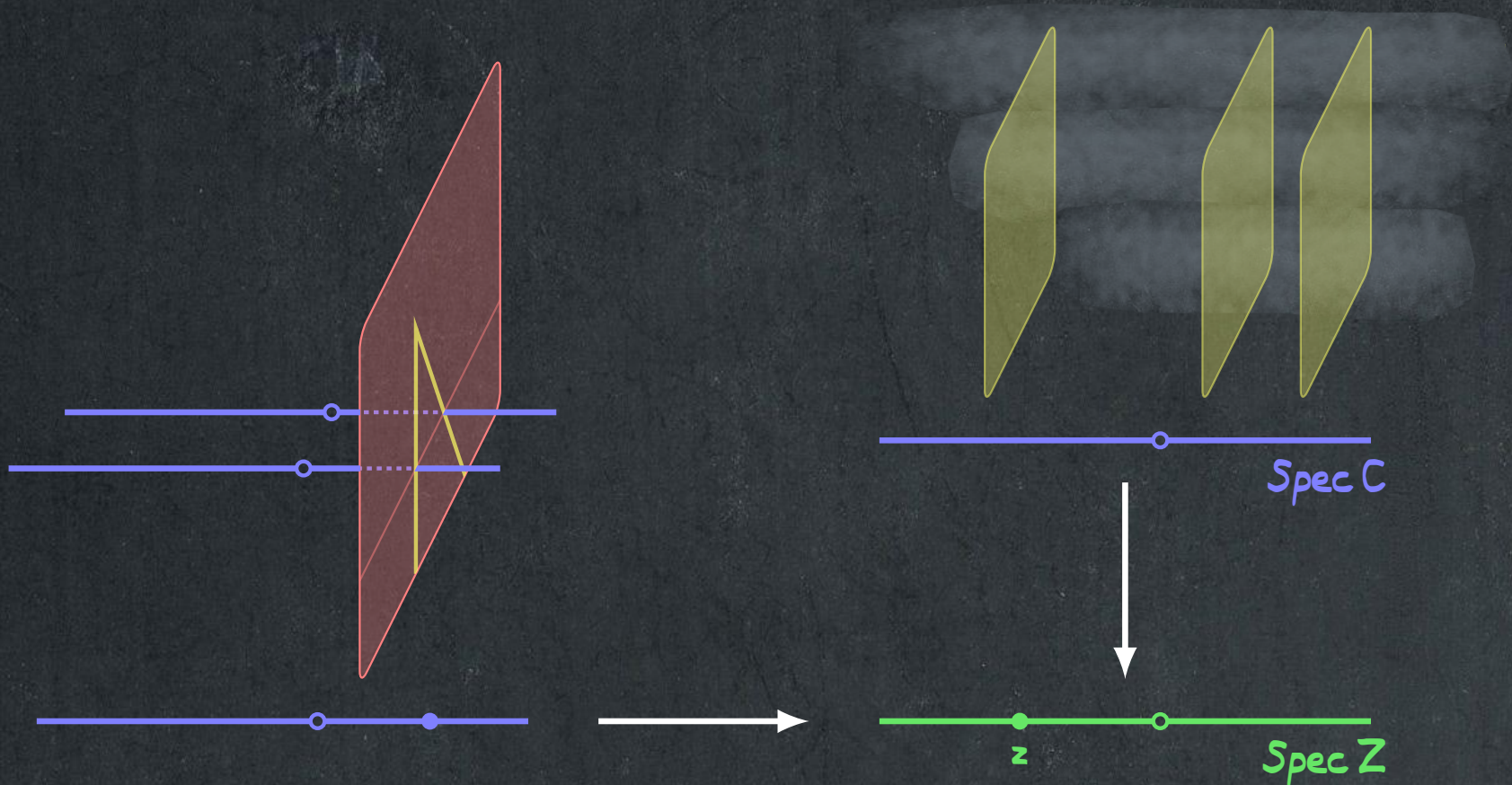
$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$

$A_z = A/(x^r - z)$ simple central algebra over F

It is split $\iff z = N_{K/F}(a)$

a splitting is $ev_{a\varphi} : A_z \xrightarrow{\sim} \mathrm{End}_F(K)$

A geometric perspective on LRS codes



$A = \mathrm{End}(\text{vector bundle})^{\varphi=1}$

$A_z = A/(x^r - z)$ simple central algebra over F

It is split $\iff z = N_{K/F}(a)$

a splitting is $ev_{a\varphi} : A_z \xrightarrow{\sim} \mathrm{End}_F(K)$

Towards Linearized Geometric codes

Towards Linearized Geometric codes

Towards Linearized Geometric codes

work in progress
with Amaury Durand

Duality

Duals of Reed Solomon codes

Duals of Reed Solomon codes

Theorem

The dual of $RS(k; a_1, \ldots, a_n)$

which was defined as the image of

$$\begin{aligned} K[x]_{<k} &\to K^n \\ f(x) &\mapsto (f(a_1), \ldots, f(a_n)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x]_{<n-k} &\longrightarrow K^n \\ g(x) &\mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h)) \\ &\quad \text{with } h(x) = (x-a_1)\cdots(x-a_n) \end{aligned}$$

Duals of Reed Solomon codes

Theorem (orthogonal for the natural pairing on K^n: $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$)

The dual of $RS(k; a_1, \ldots, a_n)$

which was defined as the image of

$$\begin{aligned} K[x]_{<k} &\to K^n \\ f(x) &\mapsto (f(a_1), \ldots, f(a_n)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x]_{<n-k} &\longrightarrow K^n \\ g(x) &\mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h)) \\ &\quad \text{with } h(x) = (x-a_1)\cdots(x-a_n) \end{aligned}$$

Duals of Reed Solomon codes

Theorem orthogonal for the natural pairing on K^n: $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$

The dual of $RS(k; a_1, \ldots, a_n)$

which was defined as the image of

$$\begin{aligned} K[x]_{<k} &\to K^n \\ f(x) &\mapsto (f(a_1), \ldots, f(a_n)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x]_{<n-k} &\longrightarrow K^n \\ g(x) &\mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h)) \\ &\quad \text{with } h(x) = (x-a_1)\cdots(x-a_n) \end{aligned}$$

Corollary

Duals of Reed Solomon codes meet the Singleton bound

Duals of Reed Solomon codes

Theorem (orthogonal for the natural pairing on K^n: $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$)

The dual of $LRS(k; a_1, \ldots, a_m)$

which was defined as the image of

$$\begin{aligned} K[x]_{<k} &\to K^n \\ f(x) &\mapsto (f(a_1), \ldots, f(a_n)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x]_{<n-k} &\longrightarrow K^n \\ g(x) &\mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h)) \\ &\quad \text{with } h(x) = (x-a_1)\cdots(x-a_n) \end{aligned}$$

Corollary

Duals of Reed Solomon codes meet the Singleton bound

Duals of Reed Solomon codes

Theorem (orthogonal for the natural pairing on K^n: $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$)

The dual of $LRS(k; a_1, \ldots, a_m)$

which was defined as the image of

$$\begin{aligned} K[x;\varphi]_{<k} &\to \mathrm{End}_F(K)^m \\ f(x) &\mapsto (f(a_1\varphi), \ldots, f(a_m\varphi)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x]_{<n-k} &\longrightarrow K^n \\ g(x) &\mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h)) \\ &\quad \text{with } h(x) = (x-a_1)\cdots(x-a_n) \end{aligned}$$

Corollary

Duals of Reed Solomon codes meet the Singleton bound

Duals of Reed Solomon codes

Theorem (orthogonal for the natural pairing on K^n: $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$)

The dual of $LRS(k; a_1, \ldots, a_m)$

which was defined as the image of

$$K[x;\varphi]_{<k} \to \mathrm{End}_F(K)^m$$
$$f(x) \mapsto (f(a_1\varphi), \ldots, f(a_m\varphi))$$

is the image of

$$K[x;\varphi]_{<mr-k} \longrightarrow \mathrm{End}_F(K)^m$$
$$g(x) \mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h))$$
$$\text{with } h(x) = (x-a_1)\cdots(x-a_n)$$

Corollary

Duals of Reed Solomon codes meet the Singleton bound

Duals of Reed Solomon codes

Theorem (orthogonal for the natural pairing on K^n: $\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n$)

The dual of $LRS(k; a_1, \ldots, a_m)$

which was defined as the image of

$$K[x;\varphi]_{<k} \to \mathrm{End}_F(K)^m$$
$$f(x) \mapsto (f(a_1\varphi), \ldots, f(a_m\varphi))$$

is the image of

$$K[x;\varphi]_{<mr-k} \longrightarrow \mathrm{End}_F(K)^m$$
$$g(x) \mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h))$$
$$\text{with } h(x) = (x-a_1)\cdots(x-a_n)$$

Corollary

Duals of Reed Solomon codes meet the Singleton bound

Duals of Reed Solomon codes

Theorem orthogonal for the natural pairing on K^n: $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$

The dual of $LRS(k; a_1, \ldots, a_m)$ $\qquad \mathrm{End}_F(K)^m$

which was defined as the image of

$$K[x;\varphi]_{<k} \to \mathrm{End}_F(K)^m$$
$$f(x) \mapsto (f(a_1\varphi), \ldots, f(a_m\varphi))$$

is the image of

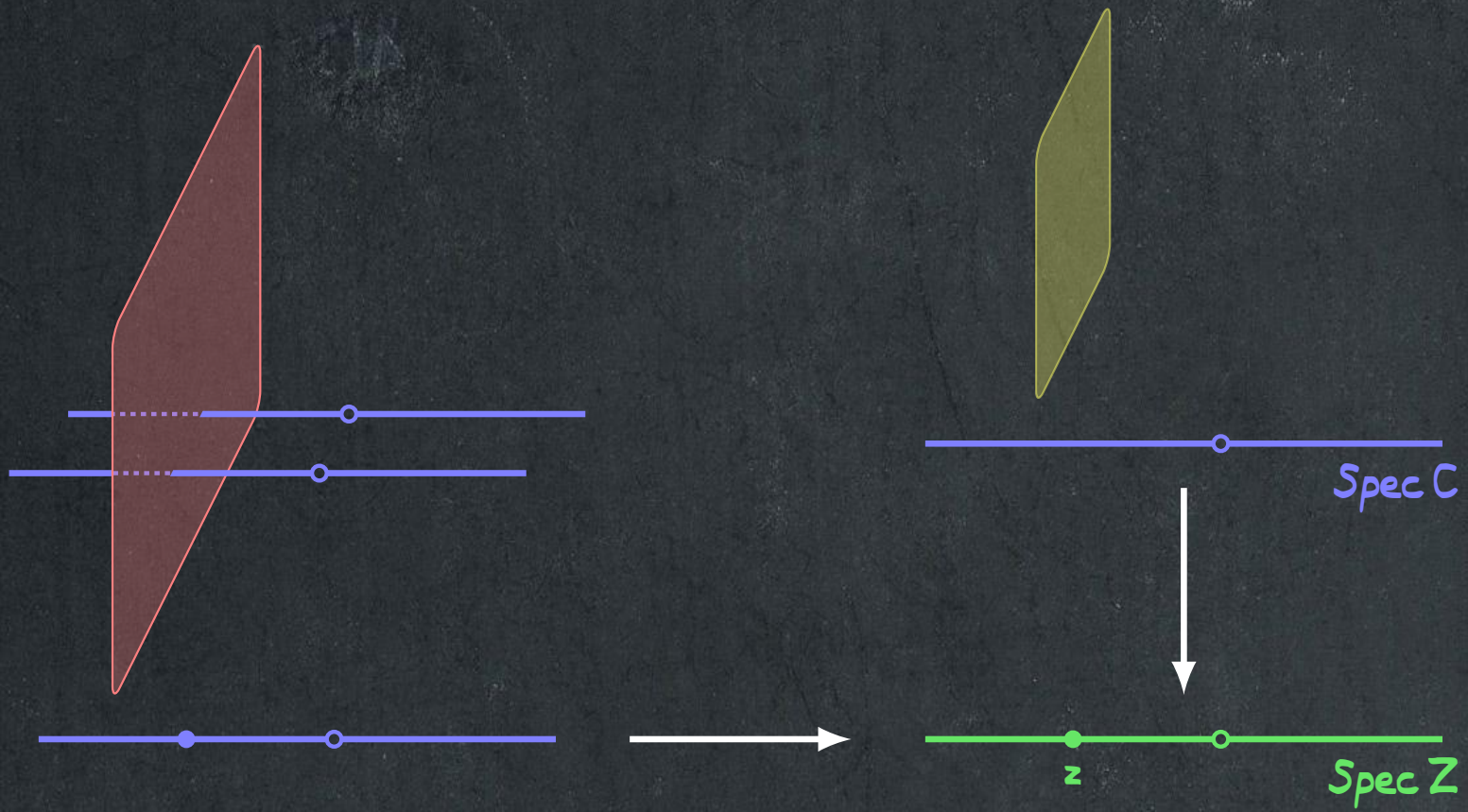
$$K[x;\varphi]_{<mr-k} \longrightarrow \mathrm{End}_F(K)^m$$
$$g(x) \mapsto (\mathrm{res}_{a_1}(g/h), \ldots, \mathrm{res}_{a_n}(g/h))$$
$$\text{with } h(x) = (x-a_1)\cdots(x-a_n)$$

Corollary

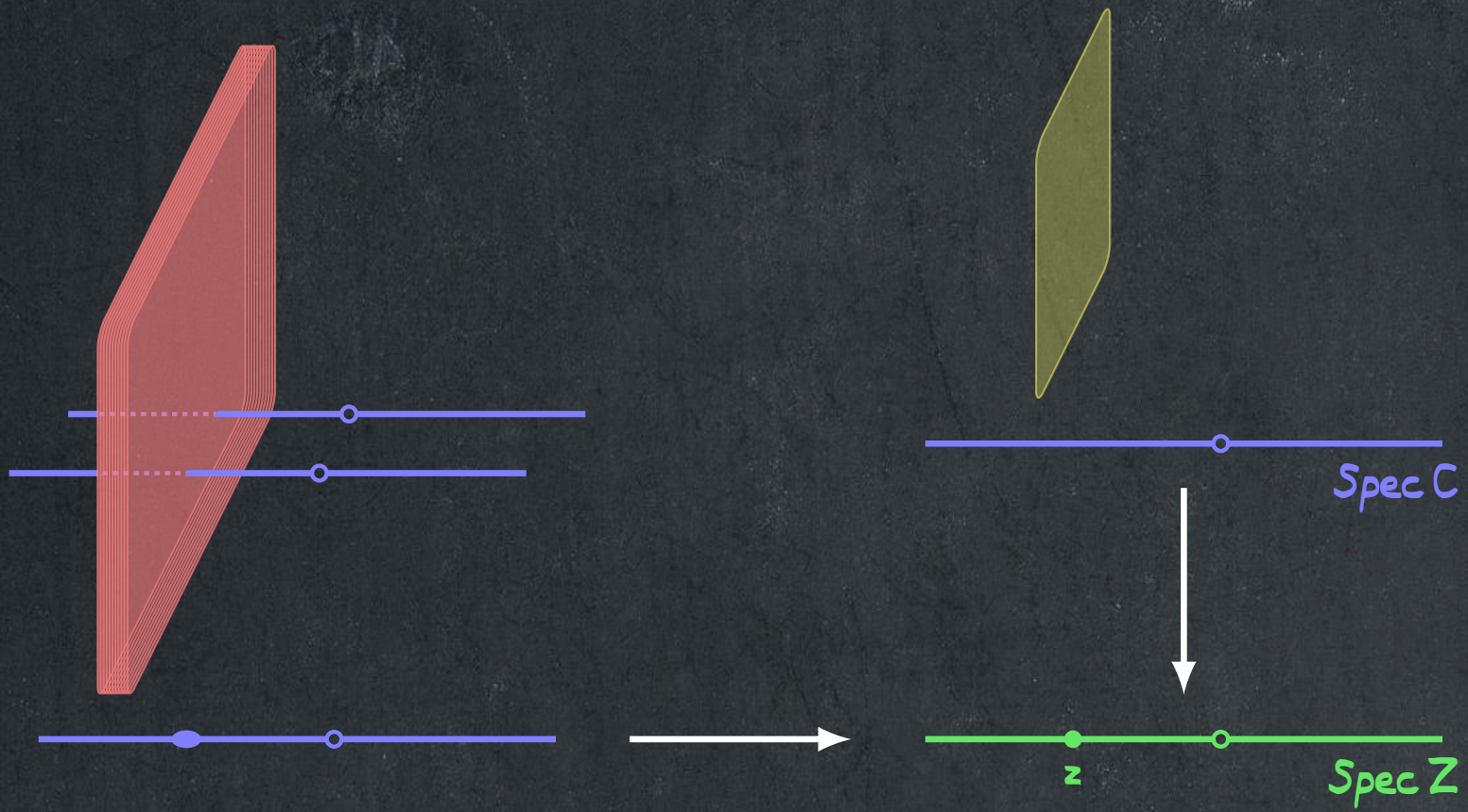
Duals of Reed Solomon codes meet the Singleton bound

Taylor expansion of Ore polynomials

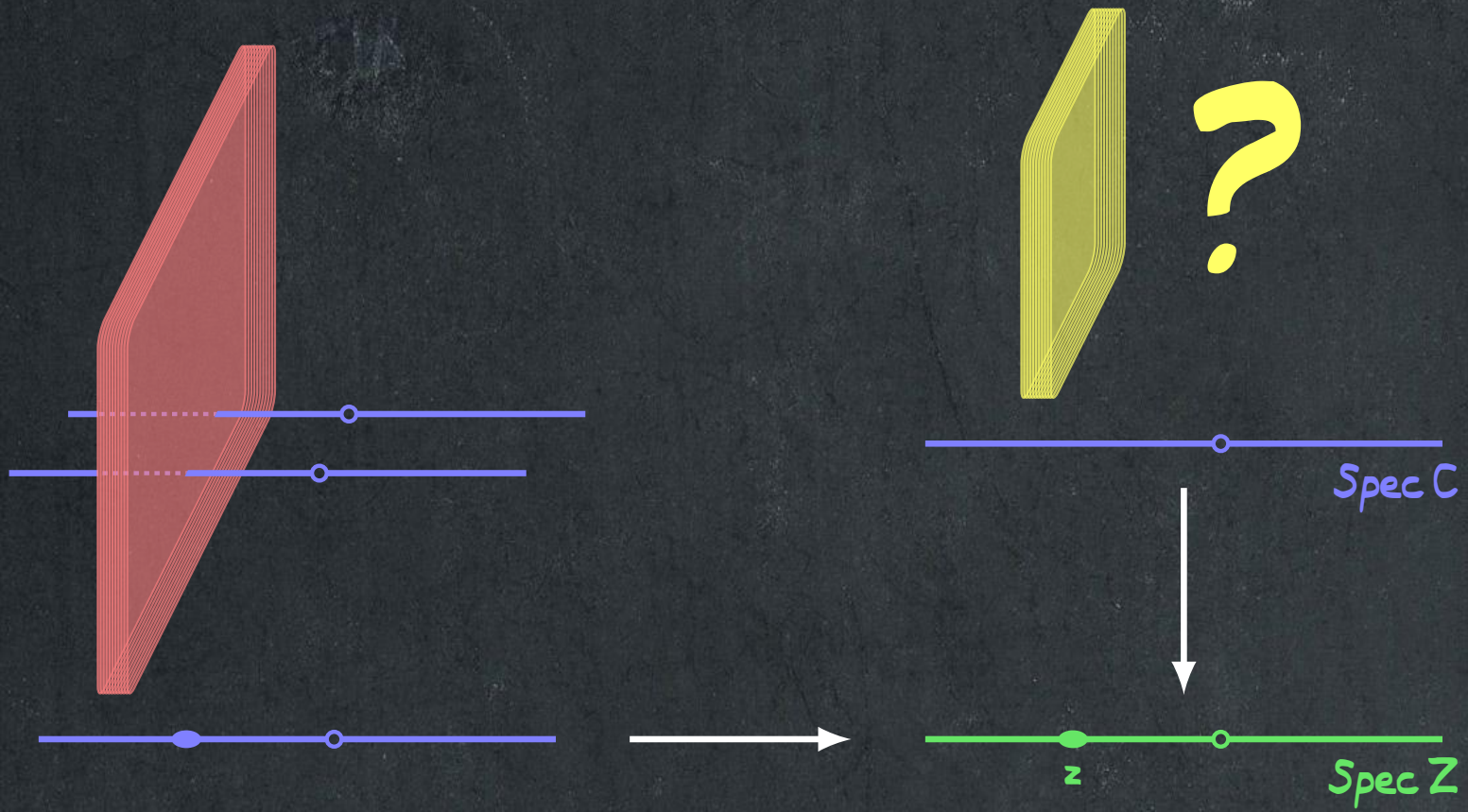
Taylor expansion of Ore polynomials



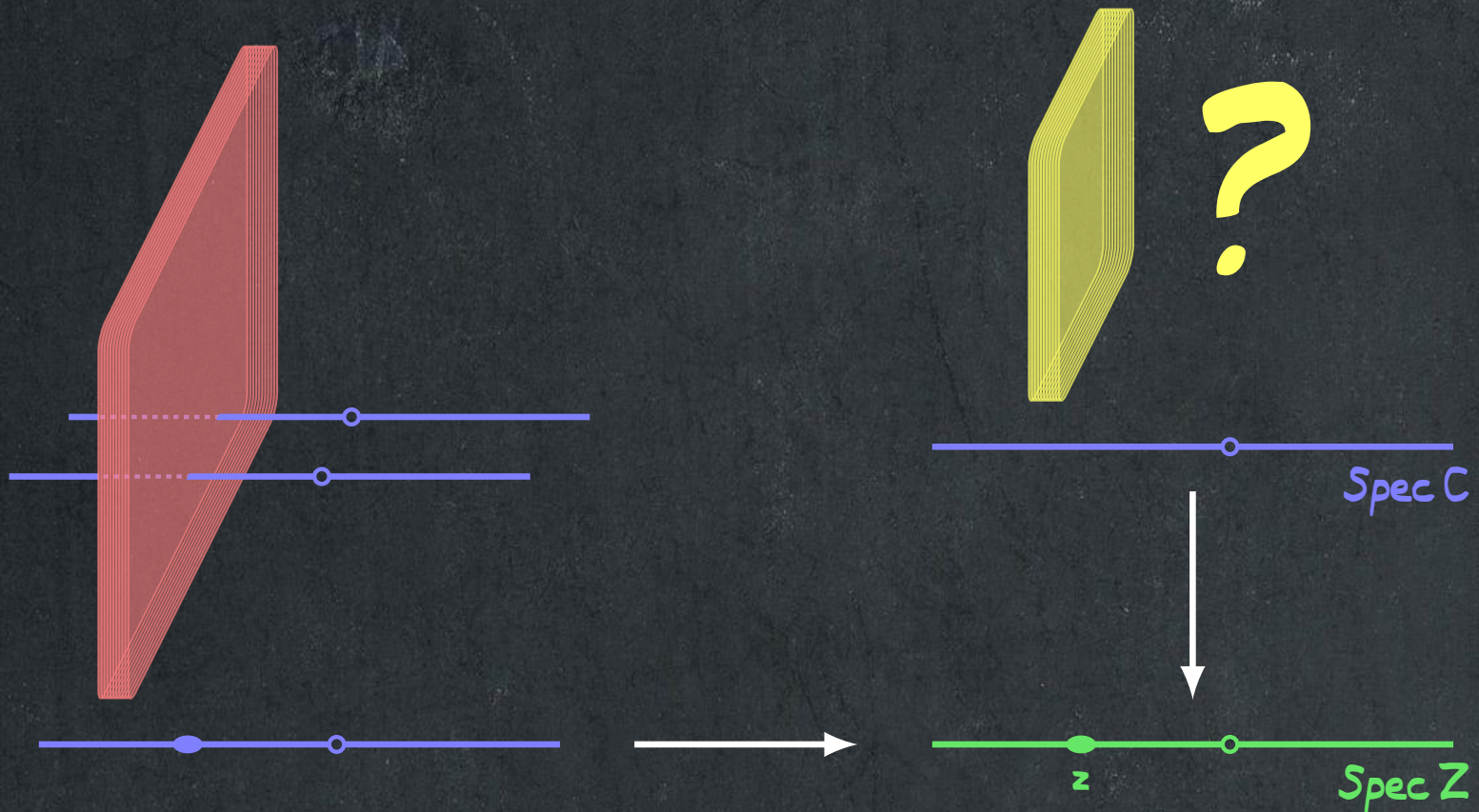
Taylor expansion of Ore polynomials



Taylor expansion of Ore polynomials



Taylor expansion of Ore polynomials

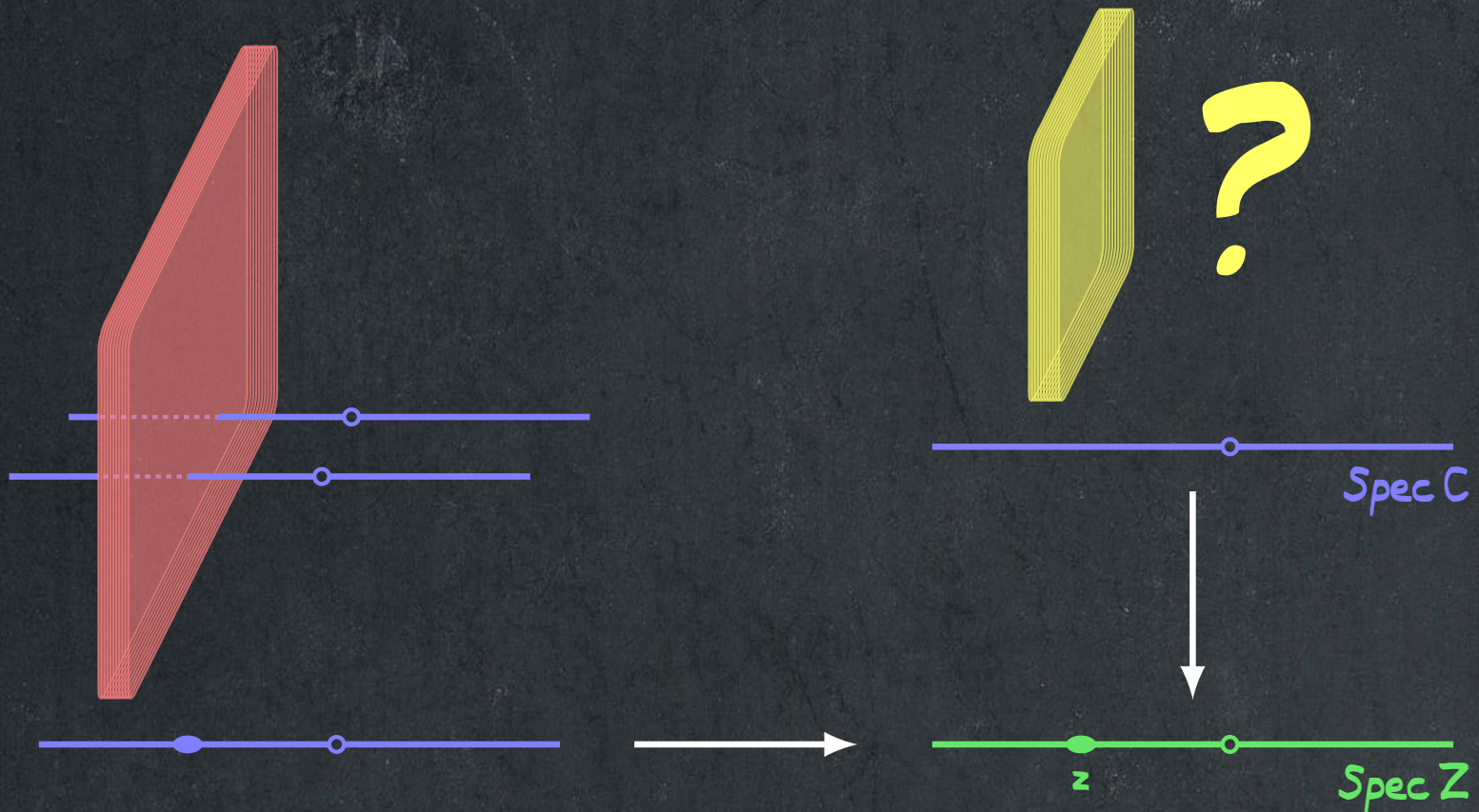


Theorem

Let N be an irreducible polynomial in Z

Then there is an isomorphism: $\varprojlim_m A/N^mA \simeq (A/NA)[[h]]$

Taylor expansion of Ore polynomials



Theorem

Let N be an irreducible polynomial in Z

Then there is an isomorphism: $\varprojlim_m A/N^mA \simeq (A/NA)[[h]]$

$N \mapsto h$

Residues of Ore polynomials

Residues of Ore polynomials

Ore rational functions

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

$$A \longrightarrow \varprojlim_m A/N^m A$$

Residues of Ore polynomials

Ore rational functions

Define $\mathrm{Frac}\, A = \mathrm{Frac}\, Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

$$A \longrightarrow \varprojlim_m A/N^m A \longrightarrow (A/NA)[[h]]$$

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

$$\operatorname{Frac} A \longrightarrow \varprojlim_m A/N^m A \longrightarrow (A/NA)[[h]]$$

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

$$\operatorname{Frac} A \longrightarrow \left(\varprojlim_m A/N^m A\right)[N^{-1}] \longrightarrow (A/NA)[[h]]$$

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

$$\operatorname{Frac} A \longrightarrow \left(\varprojlim_m A/N^m A\right)[N^{-1}] \longrightarrow (A/NA)((h))$$

Residues of Ore polynomials

Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z

$$\operatorname{Frac} A \longrightarrow \left(\varprojlim_m A/N^m A\right)[N^{-1}] \longrightarrow (A/NA)((h))$$

coeff in h^{-1} → A/NA

Residues of Ore polynomials

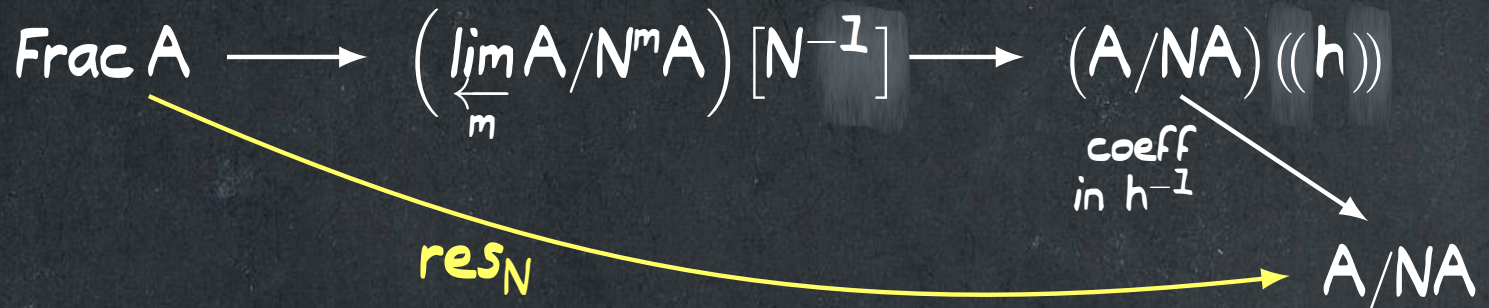
Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z



Residues of Ore polynomials

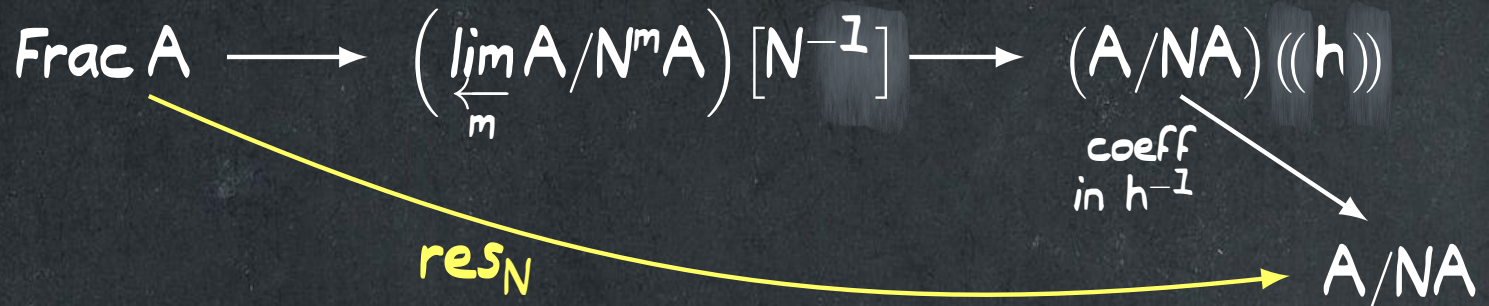
Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z



For $a \in K$, $f \in \operatorname{Frac} A$,
set $\mathrm{res}_a(f)$

Residues of Ore polynomials

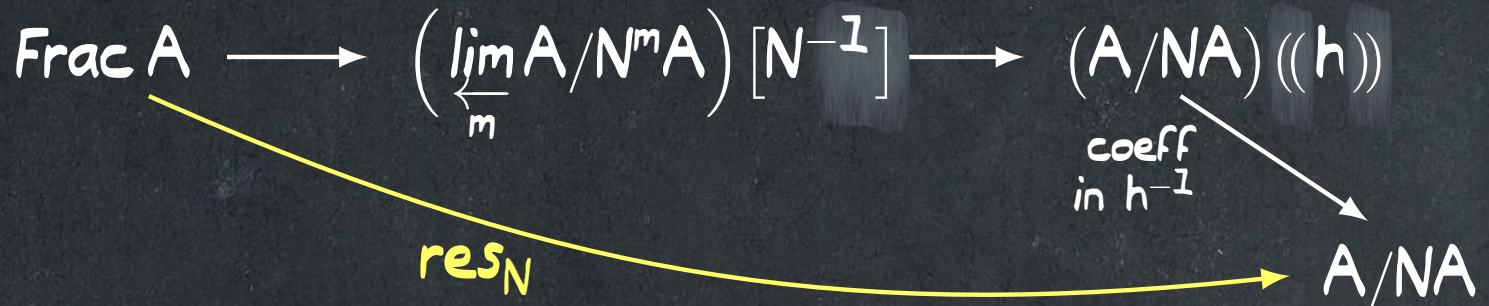
Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z



For $a \in K$, $f \in \operatorname{Frac} A$,
set $\mathrm{res}_a(f) = \mathrm{ev}_a \circ \mathrm{res}_{x^r - N_{K/F}(a)}(f)$

Residues of Ore polynomials

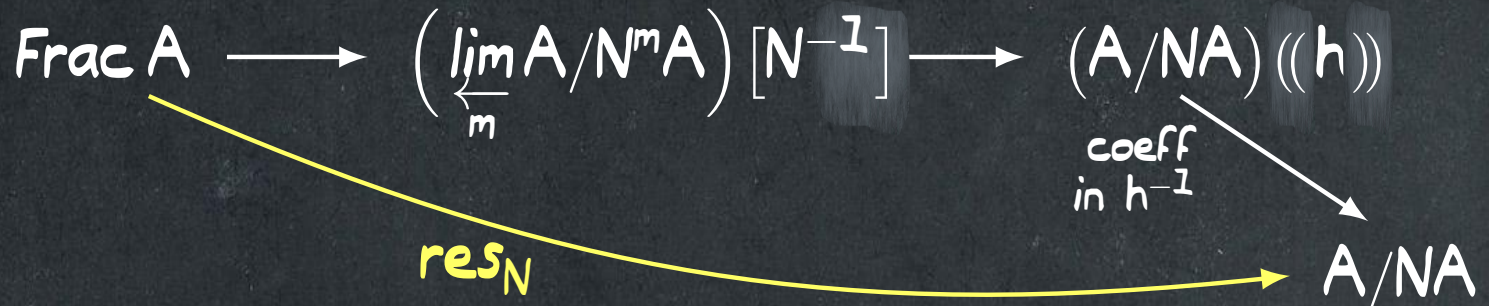
Ore rational functions

Define $\operatorname{Frac} A = \operatorname{Frac} Z \otimes_Z A$

This makes sense because
each Ore polynomial has a multiple in the centre:
$N_{rd}(f)$ divides f on both sides

The residue map

Let N be an irreducible polynomial in Z



For $a \in K$, $f \in \operatorname{Frac} A$,
set $\mathrm{res}_a(f) = \mathrm{ev}_a \circ \mathrm{res}_{x^r - N_{K/F}(a)}(f)$

$\mathrm{res}_a(f) \in \mathrm{End}_F(K)$

Pairing on $\mathrm{End}_F(K)^m$

Pairing on $\mathrm{End}_F(K)^m$

1. We equip K with the usual F-bilinear pairing

$$\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$$

Pairing on $\mathrm{End}_F(K)^m$

1. We equip K with the usual F-bilinear pairing

$$\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$$

2. We equip $\mathrm{End}_F(K)$ with the F-bilinear pairing

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

where u^* is the adjoint of u

Pairing on $\mathrm{End}_F(K)^m$

1. We equip K with the usual F-bilinear pairing

$$\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$$

2. We equip $\mathrm{End}_F(K)$ with the F-bilinear pairing

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

where u^* is the adjoint of u

3. We equip $\mathrm{End}_F(K)^m$ with the F-bilinear pairing

$$\langle (u_1, \ldots, u_m), (v_1, \ldots, v_m) \rangle = \sum_{i=1}^{m} \mathrm{Tr}(u_i^* \circ v_i)$$

Pairing on $\mathrm{End}_F(K)^m$

1. We equip K with the usual F-bilinear pairing

$$\langle x, y \rangle_K = \mathrm{Tr}_{K/F}(xy)$$

2. We equip $\mathrm{End}_F(K)$ with the F-bilinear pairing

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

where u^* is the adjoint of u

3. We equip $\mathrm{End}_F(K)^m$ with the F-bilinear pairing

$$\langle (u_1, \ldots, u_m), (v_1, \ldots, v_m) \rangle = \sum_{i=1}^{m} \mathrm{Tr}(u_i^* \circ v_i)$$

Fact

All these pairings are symmetric and non-degenerate

Pulling back the pairing on Ore polynomials

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{End_F(K)} = Tr(u^* \circ v)$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{End_F(K)} = Tr(u^* \circ v)$$

$T_{rd} : A \to Z$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

$$T_{rd}\left(\sum a_i x^i \right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri}$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

$$T_{rd}\left(\sum a_i x^i \right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri}$$

$$\begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle T_{rd}} & & \downarrow{\scriptstyle Tr} \\ Z & \xrightarrow{x^r \mapsto N_{K/F}(a)} & F \end{array}$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

$$T_{rd}\left(\sum a_i x^i \right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri} \qquad \left(\sum a_i x^i \right)^* = \sum x^{-i} a_i$$

$$\begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle T_{rd}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ Z & \xrightarrow{x^r \mapsto N_{K/F}(a)} & F \end{array}$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

$$T_{rd}\left(\sum a_i x^i\right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri} \qquad \left(\sum a_i x^i\right)^* = \sum x^{-i} a_i$$

$$\begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle T_{rd}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ Z & \xrightarrow{x^r \mapsto N_{K/F}(a)} & F \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle f \mapsto f^*} & & \downarrow{\scriptstyle u \mapsto u^*} \\ A & \xrightarrow[ev_{a^{-1}\varphi}]{} & \mathrm{End}_F(K) \end{array}$$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

$$T_{rd}\left(\sum a_i x^i\right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri} \qquad \left(\sum a_i x^i\right)^* = \sum x^{-i} a_i$$

$$\begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle T_{rd}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ Z & \xrightarrow{x^r \mapsto N_{K/F}(a)} & F \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle f \mapsto f^*} & & \downarrow{\scriptstyle u \mapsto u^*} \\ A & \xrightarrow[ev_{a^{-1}\varphi}]{} & \mathrm{End}_F(K) \end{array}$$

Consequence

$\langle ev_{a^{-1}\varphi}(g), ev_{a\varphi}(f) \rangle_{\mathrm{End}_K(F)} = T_{rd}(g^* f)$ eval. at $x^r = N_{K/F}(a)$

Pulling back the pairing on Ore polynomials

$$\langle u, v \rangle_{\mathrm{End}_F(K)} = \mathrm{Tr}(u^* \circ v)$$

$T_{rd} : A \to Z$ where $A = K[x^{\pm 1}; \varphi]$ and $Z = F[x^{\pm r}]$ (centre)

$$T_{rd}\left(\sum a_i x^i\right) = \sum \mathrm{Tr}_{K/F}(a_{ri}) x^{ri} \qquad \left(\sum a_i x^i\right)^* = \sum x^{-i} a_i$$

$$\begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle T_{rd}} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ Z & \xrightarrow{x^r \mapsto N_{K/F}(a)} & F \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{ev_{a\varphi}} & \mathrm{End}_F(K) \\ \downarrow{\scriptstyle f \mapsto f^*} & & \downarrow{\scriptstyle u \mapsto u^*} \\ A & \xrightarrow[ev_{a^{-1}\varphi}]{} & \mathrm{End}_F(K) \end{array}$$

Consequence

$$\langle ev_{a^{-1}\varphi}(g), ev_{a\varphi}(f) \rangle_{\mathrm{End}_K(F)} = T_{rd}(g^* f) \text{ eval. at } x^r = N_{K/F}(a)$$

$$\langle res_{a^{-1}}(gh^{-1}), ev_{a\varphi}(f) \rangle_{\mathrm{End}_K(F)} = res_{N_{K/F}(a)}(T_{rd}((gh^{-1})^* f))$$

Duals of Gabidulin codes

Duals of Gabidulin codes

Theorem

The dual of $\mathrm{LRS}(k; a_1, \ldots, a_m)$

which was defined as the image of

$$\begin{aligned} K[x;\varphi]_{<k} &\to \mathrm{End}_F(K)^m \\ f(x) &\mapsto (f(a_1\varphi), \ldots, f(a_m\varphi)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x;\varphi]_{<mr-k} &\longrightarrow \mathrm{End}_F(K)^m \\ g(x) &\mapsto (\mathrm{res}_{a_1^{-1}}(gh^{-1}), \ldots, \mathrm{res}_{a_n^{-1}}(gh^{-1})) \end{aligned}$$

$$\text{with } h(x) = x^{mr-r-k} \cdot (x^r - N_{K/F}(a_1)^{-1}) \cdots (x^r - N_{K/F}(a_n)^{-1})$$

Duals of Gabidulin codes

Theorem

The dual of $\mathrm{LRS}(k; a_1, \ldots, a_m)$

which was defined as the image of

$$\begin{aligned} K[x;\varphi]_{<k} &\to \mathrm{End}_F(K)^m \\ f(x) &\mapsto (f(a_1\varphi), \ldots, f(a_m\varphi)) \end{aligned}$$

is the image of

$$\begin{aligned} K[x;\varphi]_{<mr-k} &\longrightarrow \mathrm{End}_F(K)^m \\ g(x) &\mapsto (\mathrm{res}_{a_1^{-1}}(gh^{-1}), \ldots, \mathrm{res}_{a_n^{-1}}(gh^{-1})) \end{aligned}$$

with $h(x) = x^{mr-r-k} \cdot (x^r - N_{K/F}(a_1)^{-1}) \cdots (x^r - N_{K/F}(a_n)^{-1})$

Corollary

Duals of LRS codes meet the Singleton bound

Thanks

for your attention