# From curves to surfaces: a walk through Algebraic Geometry codes

**Elena Berardini**
**CNRS; Université de Bordeaux**

Academy Contact Forum "Coding Theory and Cryptography IX"
$8^{th}$ September 2023

Some slides were taken from or largely inspired by J. Nardi's talk at the conference COGNAC. The speaker is very grateful to her.

# Table of Contents

## Error–correcting codes

**GOAL:** retrieve the data which are lost/corrupted during transmission or storage.

Linear codes: $\mathbb{F}_q$–vector subspaces of $\mathbb{F}_q^n$ endowed with a metric. $d(\mathbf{x},\mathbf{0})=w(\mathbf{x})=\#\{x_i\neq 0\}$

$[n,k,d]_q$–code: code of length **n**, dimension **k** and minimum distance **d**. $d=\min_{\mathbf{x}\neq\mathbf{0}}\{w(\mathbf{x})\}$

$$\left.\begin{array}{r}\text{dimension} \leftrightarrow \text{information rate}\\ \text{minimum distance} \leftrightarrow \text{correction capacity}\end{array}\right\} \quad k+d\leqslant n+1$$

Singleton, 1964

## Error–correcting codes

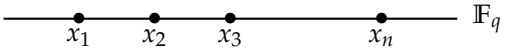
**GOAL:** retrieve the data which are lost/corrupted during transmission or storage.

Linear codes: $\mathbb{F}_q$–vector subspaces of $\mathbb{F}_q^n$ endowed with a metric. $d(\mathbf{x},\mathbf{0})=w(\mathbf{x})=\#\{x_i\neq 0\}$

$[n,k,d]_q$–code: code of length **n**, dimension **k** and minimum distance **d**. $d=\min_{\mathbf{x}\neq\mathbf{0}}\{w(\mathbf{x})\}$

$$\left.\begin{array}{r}\text{dimension} \leftrightarrow \text{information rate}\\ \text{minimum distance} \leftrightarrow \text{correction capacity}\end{array}\right\} \quad k+d\leqslant n+1$$ Singleton, 1964

**Reed–Solomon codes** Reed and Solomon, 1960




$$\mathrm{RS}_k(\mathbf{x}) \stackrel{\text{def}}{=} \{(f(x_1),f(x_2),f(x_3),\ldots,f(x_n)) \mid f\in \mathbb{F}_q[x]_{<k}\}$$

## Error–correcting codes

**GOAL:** retrieve the data which are lost/corrupted during transmission or storage.

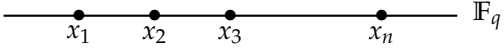
Linear codes: $\mathbb{F}_q$–vector subspaces of $\mathbb{F}_q^n$ endowed with a metric. $d(\mathbf{x},\mathbf{0})=w(\mathbf{x})=\#\{x_i\neq 0\}$

$[n,k,d]_q$–code: code of length **n**, dimension **k** and minimum distance **d**. $d=\min_{\mathbf{x}\neq\mathbf{0}}\{w(\mathbf{x})\}$

$$\left.\begin{array}{r}\text{dimension} \leftrightarrow \text{information rate}\\ \text{minimum distance} \leftrightarrow \text{correction capacity}\end{array}\right\} \quad k+d\leqslant n+1$$

Singleton, 1964

**Reed–Solomon codes** Reed and Solomon, 1960




$$\mathrm{RS}_k(\mathbf{x}) \stackrel{\text{def}}{=} \{(f(x_1),f(x_2),f(x_3),\ldots,f(x_n)) \mid f\in \mathbb{F}_q[x]_{<k}\}$$

$$\dim \mathbb{F}_q[x]_{<k}=k \Rightarrow \dim_{\mathbb{F}_q}\mathrm{RS}_k(\mathbf{x})=k$$
$$\text{zeros}(f)\leq k-1 \Rightarrow d\geq n-k+1$$

## Error–correcting codes

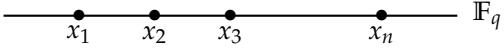
**GOAL:** retrieve the data which are lost/corrupted during transmission or storage.

Linear codes: $\mathbb{F}_q$–vector subspaces of $\mathbb{F}_q^n$ endowed with a metric. $d(\mathbf{x},\mathbf{0})=w(\mathbf{x})=\#\{x_i\neq 0\}$

$[n,k,d]_q$–code: code of length **n**, dimension **k** and minimum distance **d**. $d=\min_{\mathbf{x}\neq\mathbf{0}}\{w(\mathbf{x})\}$

$$\left.\begin{array}{r}\text{dimension} \leftrightarrow \text{information rate}\\ \text{minimum distance} \leftrightarrow \text{correction capacity}\end{array}\right\} \quad k+d \leqslant n+1$$ Singleton, 1964

**Reed–Solomon codes** Reed and Solomon, 1960




$$\mathrm{RS}_k(\mathbf{x}) \stackrel{\text{def}}{=} \{(f(x_1),f(x_2),f(x_3),\ldots,f(x_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$$

$\dim \mathbb{F}_q[x]_{<k} = k \Rightarrow \dim_{\mathbb{F}_q} \mathrm{RS}_k(\mathbf{x}) = k$

$\mathrm{zeros}(f) \leq k-1 \Rightarrow d \geq n-k+1$

✔ **Optimal parameters:**
$k+d=n+1$

## Error–correcting codes

**GOAL:** retrieve the data which are lost/corrupted during transmission or storage.

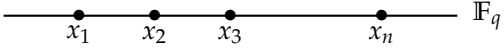
Linear codes: $\mathbb{F}_q$–vector subspaces of $\mathbb{F}_q^n$ endowed with a metric. $d(\mathbf{x},\mathbf{0})=w(\mathbf{x})=\#\{x_i\neq 0\}$

$[n,k,d]_q$–code: code of length **n**, dimension **k** and minimum distance **d**. $d=\min_{\mathbf{x}\neq\mathbf{0}}\{w(\mathbf{x})\}$

$$\left.\begin{array}{r}\text{dimension} \leftrightarrow \text{information rate}\\ \text{minimum distance} \leftrightarrow \text{correction capacity}\end{array}\right\} \quad k+d \leqslant n+1$$

Singleton, 1964

**Reed–Solomon codes** Reed and Solomon, 1960




$$\mathrm{RS}_k(\mathbf{x}) \stackrel{\text{def}}{=} \{(f(x_1),f(x_2),f(x_3),\ldots,f(x_n)) \mid f \in \mathbb{F}_q[x]_{<k}\}$$

$\dim \mathbb{F}_q[x]_{<k} = k \Rightarrow \dim_{\mathbb{F}_q} \mathrm{RS}_k(\mathbf{x}) = k$

$\mathrm{zeros}(f) \leq k-1 \Rightarrow d \geq n-k+1$

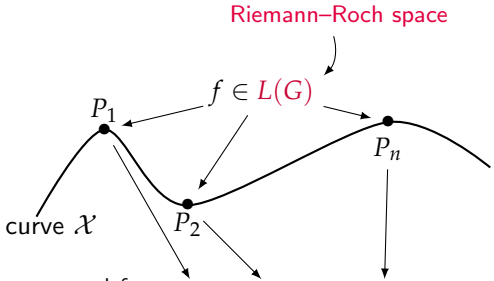
✔ **Optimal parameters:** $k+d=n+1$

⚠ **Drawback:** $n \leqslant q$.

The bigger the $q$, the less efficient the arithmetic.

# Table of Contents

# Algebraic Geometry (AG) codes from curves Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\ldots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\ldots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

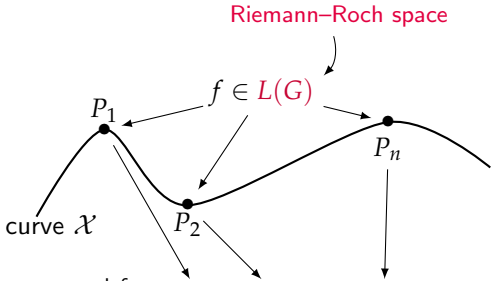
## Definition

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

An element of $L(G)$ is a function with

- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

## Algebraic Geometry (AG) codes from curves Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

### Definition

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

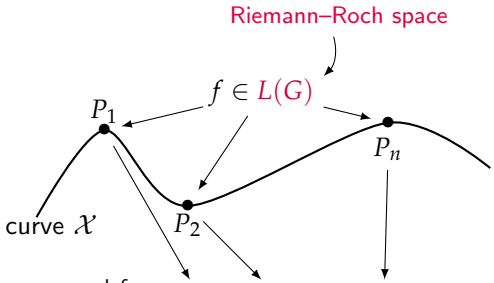
An element of $L(G)$ is a function with

- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

### Riemann–Roch theorem

$$\dim C(\mathcal{X},\mathcal{P},G) = \dim L(G) \geq \deg(G) + 1 - g$$

## Algebraic Geometry (AG) codes from curves Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

**Riemann–Roch theorem** $g$=genus of $\mathcal{X}$

$$\dim C(\mathcal{X},\mathcal{P},G) = \dim L(G) \geq \deg(G) + 1 - g$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

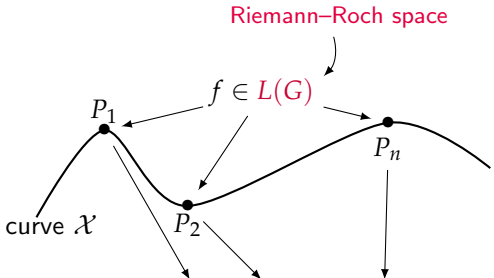
**Definition**

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

An element of $L(G)$ is a function with

- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

## Algebraic Geometry (AG) codes from curves Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

**Definition**

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

An element of $L(G)$ is a function with

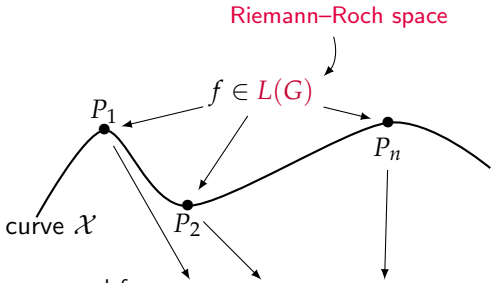
- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

**Riemann–Roch theorem** $g$=genus of $\mathcal{X}$

$$\dim C(\mathcal{X},\mathcal{P},G) = \dim L(G) \geq \deg(G) + 1 - g$$

$$\text{zeros}(f) \leq \deg(G) \Rightarrow d \geq n - \deg(G)$$

## Algebraic Geometry (AG) codes from curves Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

**Definition**

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

An element of $L(G)$ is a function with

- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

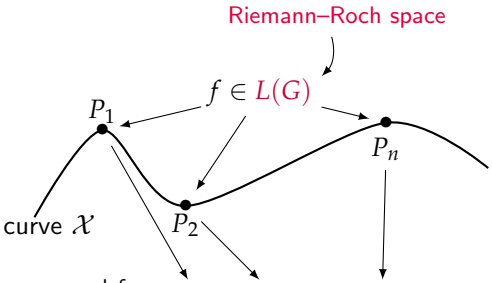
**Riemann–Roch theorem** $g$=genus of $\mathcal{X}$

$$\dim C(\mathcal{X},\mathcal{P},G) = \dim L(G) \geq \deg(G) + 1 - g$$

$$\text{zeros}(f) \leq \deg(G) \Rightarrow d \geq n - \deg(G)$$

✔ **Good parameters:** $k + d \geq n + 1 - g$

## Algebraic Geometry (AG) codes from curves 🕮 Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

### Definition

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

An element of $L(G)$ is a function with

- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

### Riemann–Roch theorem $g$=genus of $\mathcal{X}$

$$\dim C(\mathcal{X},\mathcal{P},G) = \dim L(G) \geq \deg(G) + 1 - g$$

$$\text{zeros}(f) \leq \deg(G) \Rightarrow d \geq n - \deg(G)$$

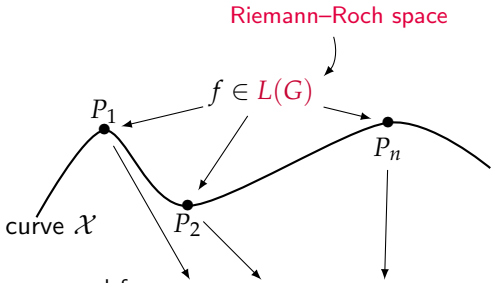
✔ **Good parameters:** $k + d \geq n + 1 - g$

### Hasse–Weil bound

For $\mathcal{X}$ a smooth curve of genus $g$ we have

$$n \leq \#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$$

## Algebraic Geometry (AG) codes from curves Goppa, 1980




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a curve, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

### Definition

*A divisor is a formal sum of points on $\mathcal{X}$*
$G = \sum_{P\in\mathcal{X}} n_P P$, $n_p \in \mathbb{Z}$. $\deg(G) = \sum n_P$

An element of $L(G)$ is a function with

- same number of zeros and poles
- poles controlled by the $P$ with $n_P > 0$
- zeros controlled by the $P$ with $n_P < 0$

### Riemann–Roch theorem $g$=genus of $\mathcal{X}$

$$\dim C(\mathcal{X},\mathcal{P},G) = \dim L(G) \geq \deg(G) + 1 - g$$

$$\text{zeros}(f) \leq \deg(G) \Rightarrow d \geq n - \deg(G)$$

✔ **Good parameters:** $k + d \geq n + 1 - g$

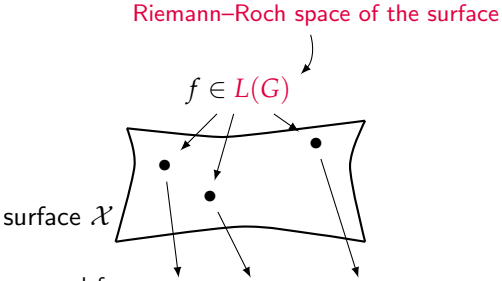
### Hasse–Weil bound

For $\mathcal{X}$ a smooth curve of genus $g$ we have

$$n \leq \#\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$$

✔ **Length:** we can have $n > q$

## AG codes from surfaces




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\ldots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a surface, $\mathcal{P} = \{P_1,\ldots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

**Definition**

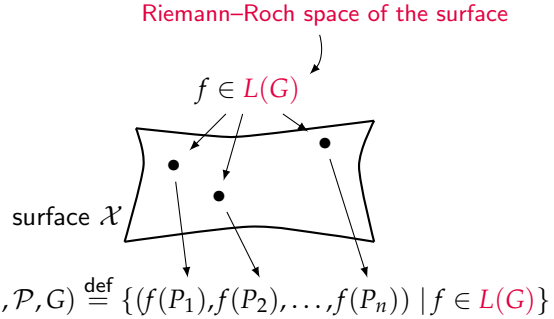
*A divisor is a formal sum of curves on $\mathcal{X}$*

$$G = \sum_{\mathcal{C}\subset\mathcal{X}} n_{\mathcal{C}}\mathcal{C},\ n_{\mathcal{C}} \in \mathbb{Z}.$$

Elements of $L(G)$ are functions with

- poles controlled by the $\mathcal{C}$ with $n_P > 0$
- zeros controlled by the $\mathcal{C}$ with $n_P < 0$

## AG codes from surfaces




$\mathcal{X}$ a surface, $\mathcal{P} = \{P_1, \ldots, P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

### Definition

*A divisor is a formal sum of curves on $\mathcal{X}$*

$$G = \sum_{\mathcal{C} \subset \mathcal{X}} n_{\mathcal{C}} \mathcal{C},\ n_{\mathcal{C}} \in \mathbb{Z}.$$

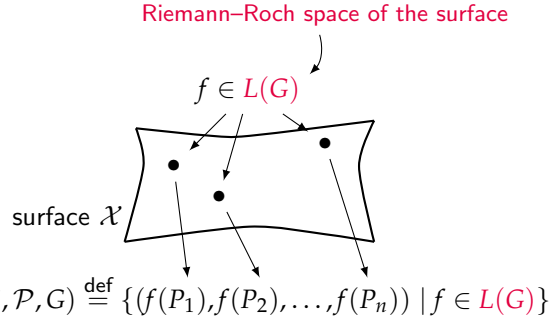
Elements of $L(G)$ are functions with

- poles controlled by the $\mathcal{C}$ with $n_P > 0$
- zeros controlled by the $\mathcal{C}$ with $n_P < 0$

### Riemann–Roch theorem for surfaces

Gives the dimension of AG codes from surfaces

## AG codes from surfaces




$\mathcal{X}$ a surface, $\mathcal{P} = \{P_1,\ldots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

### Definition

*A divisor is a formal sum of curves on $\mathcal{X}$*

$$G = \sum_{\mathcal{C}\subset\mathcal{X}} n_{\mathcal{C}}\mathcal{C},\ n_{\mathcal{C}} \in \mathbb{Z}.$$

Elements of $L(G)$ are functions with

- poles controlled by the $\mathcal{C}$ with $n_P > 0$
- zeros controlled by the $\mathcal{C}$ with $n_P < 0$

### Riemann–Roch theorem for surfaces

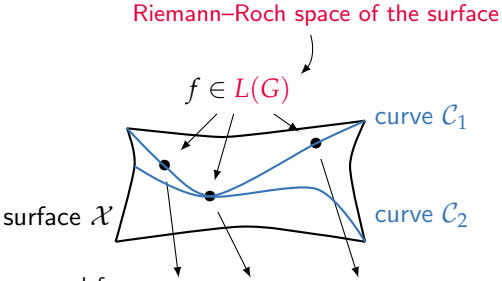
Gives the dimension of AG codes from surfaces

### Weil conjectures – Deligne theorem

For $\mathcal{X}$ a smooth surface over $\mathbb{F}_q$ we have

$$n \leq \#\mathcal{X}(\mathbb{F}_q) \sim q^2$$

## AG codes from surfaces




$$C(\mathcal{X},\mathcal{P},G) \stackrel{\text{def}}{=} \{(f(P_1),f(P_2),\dots,f(P_n)) \mid f \in L(G)\}$$

$\mathcal{X}$ a surface, $\mathcal{P} = \{P_1,\dots,P_n\} \subset \mathcal{X}(\mathbb{F}_q)$

### Definition

*A divisor is a formal sum of curves on $\mathcal{X}$*

$$G = \sum_{\mathcal{C}\subset\mathcal{X}} n_{\mathcal{C}}\mathcal{C},\ n_{\mathcal{C}} \in \mathbb{Z}.$$

Elements of $L(G)$ are functions with

- poles controlled by the $\mathcal{C}$ with $n_P > 0$
- zeros controlled by the $\mathcal{C}$ with $n_P < 0$

### Riemann–Roch theorem for surfaces

Gives the dimension of AG codes from surfaces

### Weil conjectures – Deligne theorem

For $\mathcal{X}$ a smooth surface over $\mathbb{F}_q$ we have

$$n \le \#\mathcal{X}(\mathbb{F}_q) \sim q^2$$

$$\text{zeros}(f) \le \sum_{i=1}^{s_f} \#\mathcal{C}_i(\mathbb{F}_q)$$

To bound the minimum distance we need to

- bound $s_f$ (see VZ19, ABHP21a, ABHP21b)
- bound $\#\mathcal{C}(\mathbb{F}_q)$ for $\mathcal{C} \subset \mathcal{X}$ (see BN22)

## Have you ever seen an AG codes from higher–dimensional varieties? Maybe yes!

### Definition (Reed–Muller code)

*Let $N \geq 1$ and $r \geq 0$. We define the Reed–Muller code of order $r$ by*

$$\mathrm{RM}(N,r) = \{(f(\boldsymbol{x}))_{\boldsymbol{x}\in\mathbb{F}_q^N} \mid f \in \mathbb{F}_q[X_1,\ldots,X_N]_{\leq r}\}.$$

For $r \leq q$, $\dim \mathrm{RM}(N,r) = \dim \mathbb{F}_q[X_1,\ldots,X_N]_{\leq r}$ and the minimum distance $d = q^N - rq^{N-1}$ is reached by product of linear factors.

## Have you ever seen an AG codes from higher–dimensional varieties? Maybe yes!

### Definition (Reed–Muller code)

*Let $N \geq 1$ and $r \geq 0$. We define the Reed–Muller code of order $r$ by*

$$\mathrm{RM}(N,r) = \{(f(\boldsymbol{x}))_{\boldsymbol{x}\in\mathbb{F}_q^N} \mid f \in \mathbb{F}_q[X_1,\ldots,X_N]_{\leq r}\}.$$

For $r \leq q$, $\dim \mathrm{RM}(N,r) = \dim \mathbb{F}_q[X_1,\ldots,X_N]_{\leq r}$ and the minimum distance $d = q^N - rq^{N-1}$ is reached by product of linear factors.

**Why is it an AG code?** ($N = 2 \rightsquigarrow$ AG code from a surface!)
Consider $\mathcal{X} = \mathbb{P}^N$ and $\mathcal{P} = \{(1,x_1,\ldots,x_N) \in \mathbb{P}^N(\mathbb{F}_q) \mid x_i \in \mathbb{F}_q\} = \mathbb{A}^N(\mathbb{F}_q) \simeq (\mathbb{F}_q)^N$.
Let $H$ be the hyperplane of $\mathbb{P}^N$ defined by $X_0 = 0$. Then, for any integer $r \geq 0$

$$L(rH) = \frac{1}{X_0^r} \cdot \mathbb{F}_q[X_0,\ldots,X_N]^{\mathsf{hom}}_{=r}.$$

Then $\mathrm{RM}(N,r) = C(\mathbb{P}^N,\mathcal{P},rH)$.

## (Non–exhaustive) Bibliography about AG codes from surfaces

- 1954: Reed–Muller codes
- 1986: Projective Reed–Muller (Lachaud) Parameters studied by Sorensen (1991)
- 1991: Restriction of RM Codes to projective algebraic varieties (Aubry)
- 1992: Quadric surfaces (Aubry)
- 2001: General study by Hansen
- 2001: Restrictions of RM codes (Duursma, Rentería, Tapia-Recillas)
  Parameters when $\mathcal{P}$ is in linearly general position by Ballico and Fontanari (2006)
- 2002: Toric varieties (Hansen)

## (Non–exhaustive) Bibliography about AG codes from surfaces

- 1954: Reed–Muller codes
- 1986: Projective Reed–Muller (Lachaud) Parameters studied by Sorensen (1991)
- 1991: Restriction of RM Codes to projective algebraic varieties (Aubry)
- 1992: Quadric surfaces (Aubry)
- 2001: General study by Hansen
- 2001: Restrictions of RM codes (Duursma, Rentería, Tapia-Recillas)
  Parameters when $\mathcal{P}$ is in linearly general position by Ballico and Fontanari (2006)
- 2002: Toric varieties (Hansen) Higher–dimensional varieties
- 2005: Hermitian surface (Edoukou) Surfaces
- 2007: Exploring surfaces with small Picard rank (Zarzar)
- 2018: $\mathrm{rk}\mathrm{Pic}\mathcal{X} = 1$ or sectional genus $= 0$ (Little, Schenck)
- 2019: Hirzebruch surfaces (Nardi)
- 2020: Del Pezzo surfaces with Picard rank one (Blache et al.)
- 2021: Abelian surfaces (Aubry, **B.**, Herbaut, Perret)
- 2021: Surfaces without small genus curves and fibrations (Aubry, **B.**, Herbaut, Perret)

## Why AG codes? Typical asymptotical behavior of linear codes

For an $[n,k,d]$–code $C$, we define its *rate* $R \stackrel{\text{def}}{=} \frac{k}{n}$ and its *relative distance* $\delta \stackrel{\text{def}}{=} \frac{d}{n}$.

**Good** code: $R$ and $\delta$ close to 1.

## Why AG codes? Typical asymptotical behavior of linear codes

For an $[n,k,d]$–code $C$, we define its *rate* $R \stackrel{\text{def}}{=} \frac{k}{n}$ and its *relative distance* $\delta \stackrel{\text{def}}{=} \frac{d}{n}$.

**Good** code: $R$ and $\delta$ close to 1.

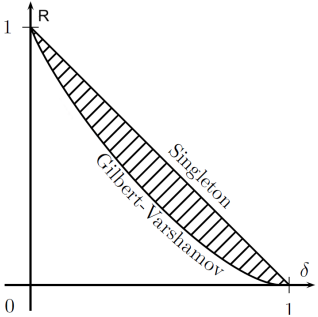
**Compromises:**

- **Singleton bound**: $R + \delta \leq 1 + \frac{1}{n}$.
- **Gilbert-Varshamov bound**: with fixed $q$ and $n \to +\infty$

$$\sup_{C\, q-\text{ary}} \{R(C) \mid \delta(C) = \delta\} \geq 1 - H_q(\delta)$$

where $H_q$ is the entropy function defined by

$$H_q(\delta) \stackrel{\text{def}}{=} \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta).$$



## Why AG codes? Typical asymptotical behavior of linear codes

For an $[n,k,d]$–code $C$, we define its *rate* $R \stackrel{\text{def}}{=} \frac{k}{n}$ and its *relative distance* $\delta \stackrel{\text{def}}{=} \frac{d}{n}$.

**Good** code: $R$ and $\delta$ close to 1.

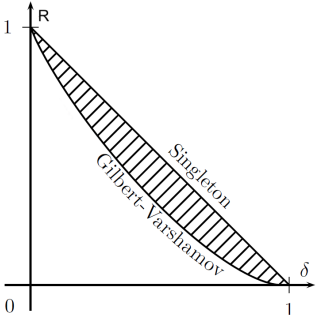
**Compromises:**

- **Singleton bound**: $R + \delta \leq 1 + \frac{1}{n}$.
- **Gilbert-Varshamov bound**: with fixed $q$ and $n \to +\infty$

$$\sup_{C\, q-\text{ary}} \{R(C) \mid \delta(C) = \delta\} \geq 1 - H_q(\delta)$$

where $H_q$ is the entropy function defined by

$$H_q(\delta) \stackrel{\text{def}}{=} \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta).$$




A random (linear) code of length $n$ and dimension $k$ satisfies $\frac{k}{n} \simeq 1 - H_q(\delta)$ with probability going to 1 when $n \to \infty$.

## Asymptotical behavior of AG codes: beating the GV bound

AG codes **from curves** satisfy

$$k + d \geq n + 1 - g$$

## Asymptotical behavior of AG codes: beating the GV bound

AG codes **from curves** satisfy

$$k + d \geq n + 1 - g$$

Denoting by $A(q)$ the Ihara function

$$A(q) = \lim_{g \to \infty} \frac{\max_{\mathrm{Genus}(\mathcal{X})=g}(\#\mathcal{X}(\mathbb{F}_q))}{g}$$

we have the existence of a sequence of codes such that

$$R + \delta \geq 1 - \frac{1}{A(q)} = 1 - \frac{1}{\sqrt{q} - 1}.$$

when $q$ is a square

## Asymptotical behavior of AG codes: beating the GV bound

AG codes **from curves** satisfy

$$k + d \geq n + 1 - g$$

Denoting by $A(q)$ the Ihara function

$$A(q) = \lim_{g \to \infty} \frac{\max_{\mathrm{Genus}(\mathcal{X})=g}(\#\mathcal{X}(\mathbb{F}_q))}{g}$$

we have the existence of a sequence of codes such that

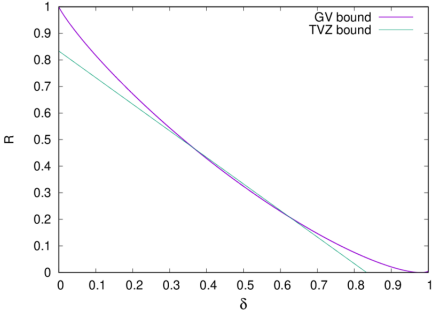
$$R + \delta \geq 1 - \frac{1}{A(q)} = 1 - \frac{1}{\sqrt{q} - 1}.$$

when $q$ is a square

Using a family of curves with many points e.g.

- modular curves TVZ82
- **towers of curves**

we get AG codes beating the GV bound!



## Asymptotical behavior of AG codes: beating the GV bound

AG codes **from curves** satisfy

$$k + d \geq n + 1 - g$$

Denoting by $A(q)$ the Ihara function

$$A(q) = \lim_{g \to \infty} \frac{\max_{\mathrm{Genus}(\mathcal{X})=g}(\#\mathcal{X}(\mathbb{F}_q))}{g}$$

we have the existence of a sequence of codes such that

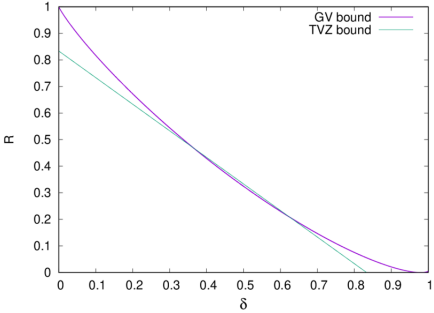
$$R + \delta \geq 1 - \frac{1}{A(q)} = 1 - \frac{1}{\sqrt{q} - 1}.$$

when $q$ is a square

Using a family of curves with many points e.g.

- modular curves TVZ82
- **towers of curves**

we get AG codes beating the GV bound!




**AG codes from surfaces?**

✔ Working with **towers of surfaces** we could get longer codes

?? **Several invariants** come into play, things get more difficult!

A fist attempt has been done by Couvreur-Lebacque-Perret CLP21. **The game is still open...**

# Table of Contents

## Encoding and decoding of AG codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ in practice we need to

1. **encode:**

2. **decode:**

## Encoding and decoding of AG codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ in practice we need to

1. **encode:** basis of $L(G)$ + (fast) evaluation at points of $\mathcal{P}$;

   On **curves**, several algorithms to compute Riemann–Roch spaces:

   - Arithmetic method
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–**B.**–Couvreur–Lecerf (2022),...

   Fast encoding on families of curves with structured $\mathcal{P}$ Beelen–Rosenkilde–Solomatov (2020)

2. **decode:**

## Encoding and decoding of AG codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ in practice we need to

1. **encode:** basis of $L(G)$ + (fast) evaluation at points of $\mathcal{P}$;

   On **curves**, several algorithms to compute Riemann–Roch spaces:

   - Arithmetic method
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–**B.**–Couvreur–Lecerf (2022),...

   Fast encoding on families of curves with structured $\mathcal{P}$ Beelen–Rosenkilde–Solomatov (2020)

   On **surfaces:** ✗ no general method for computing bases of Riemann–Roch spaces
   ✓ explicit bases for some families (e.g. projective space, Toric surfaces...)

2. **decode:**

## Encoding and decoding of AG codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ in practice we need to

1. **encode:** basis of $L(G)$ + (fast) evaluation at points of $\mathcal{P}$;

On **curves**, several algorithms to compute Riemann–Roch spaces:

- Arithmetic method
  Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
- Geometric method
  Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–**B.**–Couvreur–Lecerf (2022),...

Fast encoding on families of curves with structured $\mathcal{P}$ Beelen–Rosenkilde–Solomatov (2020)

On **surfaces:**
- ✗ no general method for computing bases of Riemann–Roch spaces
- ✓ explicit bases for some families (e.g. projective space, Toric surfaces...)

2. **decode:**

On **curves**:
- Unique decoding via Error Correcting Pairs Pelikaan (1992)
- List decoding Couvreur–Panaccione (2020), Beelen–Neiger (2023)

## Encoding and decoding of AG codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ in practice we need to

1. **encode:** basis of $L(G)$ + (fast) evaluation at points of $\mathcal{P}$;

   On **curves**, several algorithms to compute Riemann–Roch spaces:
   - Arithmetic method
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–**B.**–Couvreur–Lecerf (2022),...

   Fast encoding on families of curves with structured $\mathcal{P}$ Beelen–Rosenkilde–Solomatov (2020)

   On **surfaces:** ✗ no general method for computing bases of Riemann–Roch spaces
   ✓ explicit bases for some families (e.g. projective space, Toric surfaces...)

2. **decode:**

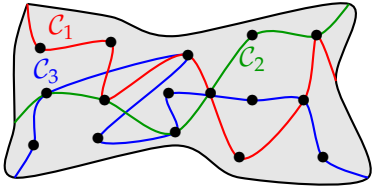
   On **curves**:
   - Unique decoding via Error Correcting Pairs Pelikaan (1992)
   - List decoding Couvreur–Panaccione (2020), Beelen–Neiger (2023)

   On **surfaces:** ✗ no global decoding algorithm
   ✓ natural local decoding using curves on the surface

## Globally decoding via local decoding

Consider an AG code $C = C(\mathcal{X}, \mathcal{P}, G)$ on a surface $\mathcal{X}$.
Assume we have a family of $\mathcal{P}$–covering curves $\mathcal{C}_i \subset \mathcal{X}$ s.t.

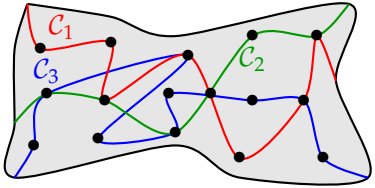
- $\mathcal{P} \subseteq \bigcup \mathcal{C}_i(\mathbb{F}_q)$ ($\mathcal{P}$–covering),
- $\boldsymbol{c} \in C \Leftrightarrow \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in C_{|\mathcal{C}_i} \stackrel{\text{def}}{=} C(\mathcal{C}_i, \mathcal{P} \cap \mathcal{C}_i, G \cap \mathcal{C}_i)$.
  The restrictions to the curves $\mathcal{C}_i$ completely characterizes $C$.



## Globally decoding via local decoding

Consider an AG code $C = C(\mathcal{X}, \mathcal{P}, G)$ on a surface $\mathcal{X}$.
Assume we have a family of $\mathcal{P}$–covering curves $\mathcal{C}_i \subset \mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup \mathcal{C}_i(\mathbb{F}_q)$ ($\mathcal{P}$–covering),
- $\boldsymbol{c} \in C \Leftrightarrow \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in C_{|\mathcal{C}_i} \stackrel{\text{def}}{=} C(\mathcal{C}_i, \mathcal{P} \cap \mathcal{C}_i, G \cap \mathcal{C}_i)$.
  The restrictions to the curves $\mathcal{C}_i$ completely characterizes $C$.




Then we have a procedure to decode a word $\boldsymbol{w}$ with respect to $C$.

1. Pick a curve $\mathcal{C}_i$ at random;
2. Use a decoding algorithm to decode $\boldsymbol{w}_{|\mathcal{C}_i}$ w.r.t. $C_{|\mathcal{C}_i}$ and replace the coordinates in $\boldsymbol{w}$;
3. Repeat 1 and 2 as many times as necessary so that for each $i$, $\boldsymbol{w}_{|\mathcal{C}_i} \in C_{|\mathcal{C}_i}$ ($\Rightarrow \boldsymbol{w} \in C$).

✔ Successfully applied to AG codes from cubic surfaces of $\mathbb{P}^3$ VZ10;
✖ May fail if too many errors gather on one curve;
✖ Characterizing codes from restrictions may be really hard.

# Table of Contents

## Locally recoverable codes

### Definition

*A code $C$ is said to be locally recoverable (LR) with locality $\ell$ if, for each $i \in \{1, \dots, n\}$, there is a subset $J_i \subseteq \{1, \dots, n\} \setminus \{i\}$, $\#J_i = \ell$ (called the recovery set), such that for any $c \in C$, we can recover the coordinate $c_i$ knowing the values $c_j$ for $j \in J_i$.*

## Locally recoverable codes

### Definition

*A code $C$ is said to be locally recoverable (LR) with locality $\ell$ if, for each $i \in \{1, \dots, n\}$, there is a subset $J_i \subseteq \{1, \dots, n\} \setminus \{i\}$, $\#J_i = \ell$ (called the recovery set), such that for any $c \in C$, we can recover the coordinate $c_i$ knowing the values $c_j$ for $j \in J_i$.*

### Singleton bound for LRCs

A LR code with parameters $[n, k, d]$ and locality $\ell$ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

## Locally recoverable codes

### Definition

*A code $C$ is said to be locally recoverable (LR) with locality $\ell$ if, for each $i \in \{1, \dots, n\}$, there is a subset $J_i \subseteq \{1, \dots, n\} \setminus \{i\}$, $\#J_i = \ell$ (called the recovery set), such that for any $c \in C$, we can recover the coordinate $c_i$ knowing the values $c_j$ for $j \in J_i$.*

### Singleton bound for LRCs

A LR code with parameters $[n, k, d]$ and locality $\ell$ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

✖ Reed–Solomon codes of dimension $k$ have locality $k$ (cannot be worse)

## Locally recoverable codes

### Definition

*A code $C$ is said to be locally recoverable (LR) with locality $\ell$ if, for each $i \in \{1, \dots, n\}$, there is a subset $J_i \subseteq \{1, \dots, n\} \setminus \{i\}$, $\#J_i = \ell$ (called the recovery set), such that for any $c \in C$, we can recover the coordinate $c_i$ knowing the values $c_j$ for $j \in J_i$.*

### Singleton bound for LRCs

A LR code with parameters $[n, k, d]$ and locality $\ell$ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

✖ Reed–Solomon codes of dimension $k$ have locality $k$ (cannot be worse)

**Many examples of good LRCs from algebraic geometry**

- Reed–Muller codes are locally recoverable of locality $\ell = q - 1$
- Barg, Tamo and Vladuts constructed LR codes on algebraic curves BTV17

## Locally recoverable codes

### Definition

*A code $C$ is said to be locally recoverable (LR) with locality $\ell$ if, for each $i \in \{1, \dots, n\}$, there is a subset $J_i \subseteq \{1, \dots, n\} \setminus \{i\}$, $\#J_i = \ell$ (called the recovery set), such that for any $c \in C$, we can recover the coordinate $c_i$ knowing the values $c_j$ for $j \in J_i$.*

### Singleton bound for LRCs

A LR code with parameters $[n, k, d]$ and locality $\ell$ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

✖ Reed–Solomon codes of dimension $k$ have locality $k$ (cannot be worse)

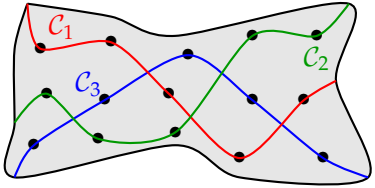
**Many examples of good LRCs from algebraic geometry**

- Reed–Muller codes are locally recoverable of locality $\ell = q - 1$
- Barg, Tamo and Vladuts constructed LR codes on algebraic curves BTV17
- **... and on surfaces?**

## How to achieve local recoverability for codes from surfaces?

From a family of $\mathcal{P}$–covering curves $\mathcal{C}_i \subset \mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup \mathcal{C}_i(\mathbb{F}_q)$ ($\mathcal{P}$–covering),
- $\#(\mathcal{P} \cap \mathcal{C}_i) = \ell + 1$;



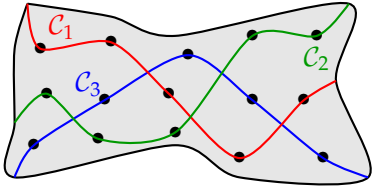

any AG code $C = C(\mathcal{X}, \mathcal{P}, G)$ is LR with locality $\ell$, **provided that** we know how to correct in the codes $C_{|\mathcal{C}_i}$.

In most constructions, $\mathcal{C}_i \simeq \mathcal{C}_j$ and the restricted codes are equivalent (e.g. $G \cap \mathcal{C}_i \simeq G \cap \mathcal{C}_j$).

## How to achieve local recoverability for codes from surfaces?

From a family of $\mathcal{P}$–covering curves $\mathcal{C}_i \subset \mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup \mathcal{C}_i(\mathbb{F}_q)$ ($\mathcal{P}$–covering),
- $\#(\mathcal{P} \cap \mathcal{C}_i) = \ell + 1$;




any AG code $C = C(\mathcal{X}, \mathcal{P}, G)$ is LR with locality $\ell$, **provided that** we know how to correct in the codes $C_{|\mathcal{C}_i}$.

In most constructions, $\mathcal{C}_i \simeq \mathcal{C}_j$ and the restricted codes are equivalent (e.g. $G \cap \mathcal{C}_i \simeq G \cap \mathcal{C}_j$).

*Alternative:* fix an AG code $C' = C(\mathcal{C}, \mathcal{P}', G')$ on the curves $\mathcal{C} \simeq \mathcal{C}_i$ and consider

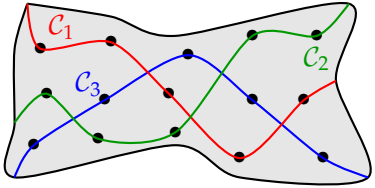
$$\{\boldsymbol{c} \in C(\mathcal{X}, \mathcal{P}, G) \mid \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in \phi_i(C')\}.$$

## How to achieve local recoverability for codes from surfaces?

From a family of $\mathcal{P}$–covering curves $\mathcal{C}_i \subset \mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup \mathcal{C}_i(\mathbb{F}_q)$ ($\mathcal{P}$–covering),
- $\#(\mathcal{P} \cap \mathcal{C}_i) = \ell + 1$;

any AG code $C = C(\mathcal{X}, \mathcal{P}, G)$ is LR with locality $\ell$, **provided that** we know how to correct in the codes $C_{|\mathcal{C}_i}$.

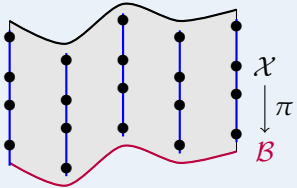



In most constructions, $\mathcal{C}_i \simeq \mathcal{C}_j$ and the restricted codes are equivalent (e.g. $G \cap \mathcal{C}_i \simeq G \cap \mathcal{C}_j$).

*Alternative:* fix an AG code $C' = C(\mathcal{C}, \mathcal{P}', G')$ on the curves $\mathcal{C} \simeq \mathcal{C}_i$ and consider

$$\{\boldsymbol{c} \in C(\mathcal{X}, \mathcal{P}, G) \mid \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in \phi_i(C')\}.$$

### LRCs on ruled surfaces — Salgado, Varilly-Alvarado, Voloch SVAV21




Fibers $\pi^{-1}(\{P\}) \simeq \mathbb{P}^1$ for every $P \in \mathcal{B}$.
Take $\mathcal{C}_i = \{$fibers of $\mathbb{F}_q$–points of $\mathcal{B}$ covering $\mathcal{P}\}$.

$\rightarrow$ Design codes from $\mathcal{X}$ whose restrictions to the $\mathcal{C}_i$ are Reed–Solomon codes of given degree.

## Quantum codes from classical linear codes: CSS codes

### Definition

*A quantum error-correcting code $Q$ is a subspace of $(\mathbb{C}^q)^{\otimes n}$. The length of $Q$ is $n$ and its dimension is the dimension as a subspace. We say that $Q$ has minimum distance $d$ if it can correct all quantum errors of weight less than or equal to $\lfloor (d-1)/2 \rfloor$.*

### Theorem (Calderbank and Shor '96, Steane '96)

Let $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$ be linear codes of dimension $k_1$ and $k_2$. Let $d_1$ and $d_2^\perp$ denote the minimum distance of $C_1$ and $C_2^\perp$, respectively. Then, there exists a quantum code $Q_{C_1,C_2}$, called CSS code, with dimension $k_1 - k_2$ and minimum distance $d \geq \min\{d_1, d_2^\perp\}$.

## Quantum codes from classical linear codes: CSS codes

### Definition

*A quantum error-correcting code $Q$ is a subspace of $(\mathbb{C}^q)^{\otimes n}$. The length of $Q$ is $n$ and its dimension is the dimension as a subspace. We say that $Q$ has minimum distance $d$ if it can correct all quantum errors of weight less than or equal to $\lfloor (d-1)/2 \rfloor$.*

### Theorem (Calderbank and Shor '96, Steane '96)

Let $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$ be linear codes of dimension $k_1$ and $k_2$. Let $d_1$ and $d_2^\perp$ denote the minimum distance of $C_1$ and $C_2^\perp$, respectively. Then, there exists a quantum code $Q_{C_1,C_2}$, called CSS code, with dimension $k_1 - k_2$ and minimum distance $d \geq \min\{d_1, d_2^\perp\}$.

### Remark

Let $C$ be a self-orthogonal $[n,k,d]_q$ linear code i.e. $C \subseteq C^\perp$. Then taking $C_1 = C^\perp$ and $C_2 = C$ gives a CSS code of dimension $n - 2k$ and minimum distance $d^\perp$.

## Quantum AG codes

**Quantum codes from curves:**

$$G \leq G' \Rightarrow C(\mathcal{X},\mathcal{P},G) \subseteq C(\mathcal{X},\mathcal{P},G')$$

$C(\mathcal{X},\mathcal{P},G)^{\perp} = C(\mathcal{X},\mathcal{P},H)$ for some $H$

the orthogonal of an AG code is an AG code

- ✔ Constructing self-orthogonal AG codes from curves is "easy"
- ✔ Many constructions of quantum AG codes from different families of curves

## Quantum AG codes

**Quantum codes from curves:**

$$G \leq G' \Rightarrow C(\mathcal{X},\mathcal{P},G) \subseteq C(\mathcal{X},\mathcal{P},G')$$

$C(\mathcal{X},\mathcal{P},G)^{\perp} = C(\mathcal{X},\mathcal{P},H)$ for some $H$

the orthogonal of an AG code is an AG code

✔ Constructing self-orthogonal AG codes from curves is "easy"

✔ Many constructions of quantum AG codes from different families of curves

**Asymptotic behavior of quantum AG codes:**

✔ Using **tower of curves** we get **asymptotically good** quantum codes LP17

## Quantum AG codes

**Quantum codes from curves:**

$$G \leq G' \Rightarrow C(\mathcal{X},\mathcal{P},G) \subseteq C(\mathcal{X},\mathcal{P},G')$$

$C(\mathcal{X},\mathcal{P},G)^{\perp} = C(\mathcal{X},\mathcal{P},H)$ for some $H$

the orthogonal of an AG code is an AG code

- ✔ Constructing self-orthogonal AG codes from curves is "easy"
- ✔ Many constructions of quantum AG codes from different families of curves

**Asymptotic behavior of quantum AG codes:**

- ✔ Using **tower of curves** we get **asymptotically good** quantum codes LP17

A quantum version of the Gilbert–Varshamov bound exists

- ✔ Quantum AG codes can **beat the quantum GV bound** HMMMF20

## Quantum AG codes

**Quantum codes from curves:**

$$G \leq G' \Rightarrow C(\mathcal{X},\mathcal{P},G) \subseteq C(\mathcal{X},\mathcal{P},G')$$

$C(\mathcal{X},\mathcal{P},G)^{\perp} = C(\mathcal{X},\mathcal{P},H)$ for some $H$

the orthogonal of an AG code is an AG code

✔ Constructing self-orthogonal AG codes from curves is "easy"

✔ Many constructions of quantum AG codes from different families of curves

**Asymptotic behavior of quantum AG codes:**

✔ Using **tower of curves** we get **asymptotically good** quantum codes LP17

A quantum version of the Gilbert–Varshamov bound exists

✔ Quantum AG codes can **beat the quantum GV bound** HMMMF20

**Quantum codes from surfaces:**

✔ Constructions have been done in particular cases (toric surfaces Han12)

✖ Dealing with the dual code is much more difficult in general

the orthogonal of an AG code from a surface is not an AG code from the surface

In a series of papers Couvreur studied the duality theory of AG codes from surfaces.

**The game is still open...**

# Table of Contents

## Something to take away?

### AG codes from curves

- ✔ provide long codes with nice properties
- ✔ can be effectively implemented
- ✔ have many applications (quantum codes, LRCs, McEliece cryptosystem, Proof of Knowledge...)
  (Leen Demuys's talk!) (Ruben De Smet's talk!)

### AG codes from surfaces

- ✔ allow to construct longer codes
- ✔ have a geometric structure richer than curves, which give interesting properties (e.g. locality),
- ✖ lack of generic algorithms to encode and decode

**We should study AG codes from surfaces and**

- rise to the challenge of implementing them;
- exploring families of surfaces giving good (classical and quantum) codes.

## Something to take away?

### AG codes from curves

- ✔ provide long codes with nice properties
- ✔ can be effectively implemented
- ✔ have many applications (quantum codes, LRCs, McEliece cryptosystem, Proof of Knowledge...)
  (Leen Demuys's talk!) (Ruben De Smet's talk!)

### AG codes from surfaces

- ✔ allow to construct longer codes
- ✔ have a geometric structure richer than curves, which give interesting properties (e.g. locality),
- ✖ lack of generic algorithms to encode and decode

**We should study AG codes from surfaces and**

- rise to the challenge of implementing them;
- exploring families of surfaces giving good (classical and quantum) codes.


# Thank you for your attention!

Questions? elena.berardini@math.u-bordeaux.fr

[ABCL22] S. Abelard, E. Berardini, A. Couvreur, and G. Lecerf. "Computing Riemann-Roch spaces via Puiseux expansions". In: *Journal of Complexity* (2022), p. 101666.

[ABHP21a] Y. Aubry, E. Berardini, F. Herbaut, and M. Perret. "Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus". In: *Finite Fields and Their Applications* 70 (2021), p. 101791.

[ABHP21b] Y. Aubry, E. Berardini, F. Herbaut, and M. Perret. "Bounds on the minimum distance of algebraic geometry codes defined over some families of surfaces". In: *Contemporary Mathematics* 770 (2021).

[Ber20] E. Berardini. "Algebraic geometry codes from surfaces over finite fields". PhD thesis. Aix-Marseille, 2020.

[BHHMVA17] A. Barg, K. Haymaker, E. W. Howe, G. L. Matthews, and A. Várilly-Alvarado. "Locally recoverable codes from algebraic curves and surfaces". In: *Algebraic geometry for coding theory and cryptography*. Vol. 9. Assoc. Women Math. Ser. Springer, Cham, 2017, pp. 95–127.

[BN22] E. Berardini and J. Nardi. "Curves on Frobenius classical surfaces in $\mathbb{P}^3$ over finite fields". In: *Acta Arithmetica* 205 (2022), pp. 303–320.

[BTV17] A. Barg, I. Tamo, and S. Vlăduţ. "Locally recoverable codes on algebraic curves". In: *IEEE Transactions on Information Theory* 63.8 (2017), pp. 4928–4939.

[CLP21] A. Couvreur, P. Lebacque, and M. Perret. "Toward good families of codes from towers of surfaces". In: *Contemporary Mathematics* 770 (2021).

[Cou11] A. Couvreur. "Construction of rational surfaces yielding good codes". In: *Finite Fields Appl.* 17.5 (2011), pp. 424–441.

[CS96] A. R. Calderbank and P. W. Shor. "Good quantum error-correcting codes exist". In: *Physical Review A* 54.2 (1996), p. 1098.

[Gop81] V. D. Goppa. "Codes on algebraic curves". In: *Dokl. Akad. Nauk SSSR* 259.6 (1981), pp. 1289–1290.

[Han01] S. H. Hansen. "Error-correcting codes from higher-dimensional varieties". In: *Finite Fields Appl.* 7.4 (2001), pp. 531–552.

[Han12] J. P. Hansen. "Quantum codes from toric surfaces". In: *IEEE transactions on information theory* 59.2 (2012), pp. 1188–1192.

[Hes02] F. Hess. "Computing Riemann–Roch spaces in algebraic function fields and related topics". In: *Journal of Symbolic Computation* 33.4 (2002), pp. 425–445.

[HMMMF20] F. Hernando, G. McGuire, F. Monserrat, and J. J. Moyano-Fernández. "Quantum codes from a new construction of self-orthogonal algebraic geometry codes". In: *Quantum Information Processing* 19 (2020), pp. 1–25.

[LGP17] G. G. La Guardia and F. R. F. Pereira. "Good and asymptotically good quantum codes derived from algebraic geometry". In: *Quantum Information Processing* 16 (2017), pp. 1–12.

[McE78] R. J. McEliece. "A public-key cryptosystem based on algebraic coding theory". In: *Coding Thv* 4244 (1978), pp. 114–116.

[SVAV21] C. Salgado, A. Várilly-Alvarado, and J. F. Voloch. "Locally recoverable codes on surfaces". In: *IEEE Transactions on Information Theory* (2021).

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink. "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound". In: *Math. Nachr.* 109 (1982), pp. 21–28.

[VZ10] J. F. Voloch and M. Zarzar. "Algebraic geometric codes on surfaces". In: *Arithmetics, geometry, and coding theory (AGCT 2005)*. Vol. 21. Sémin. Congr. Soc. Math. France, Paris, 2010, pp. 211–216.