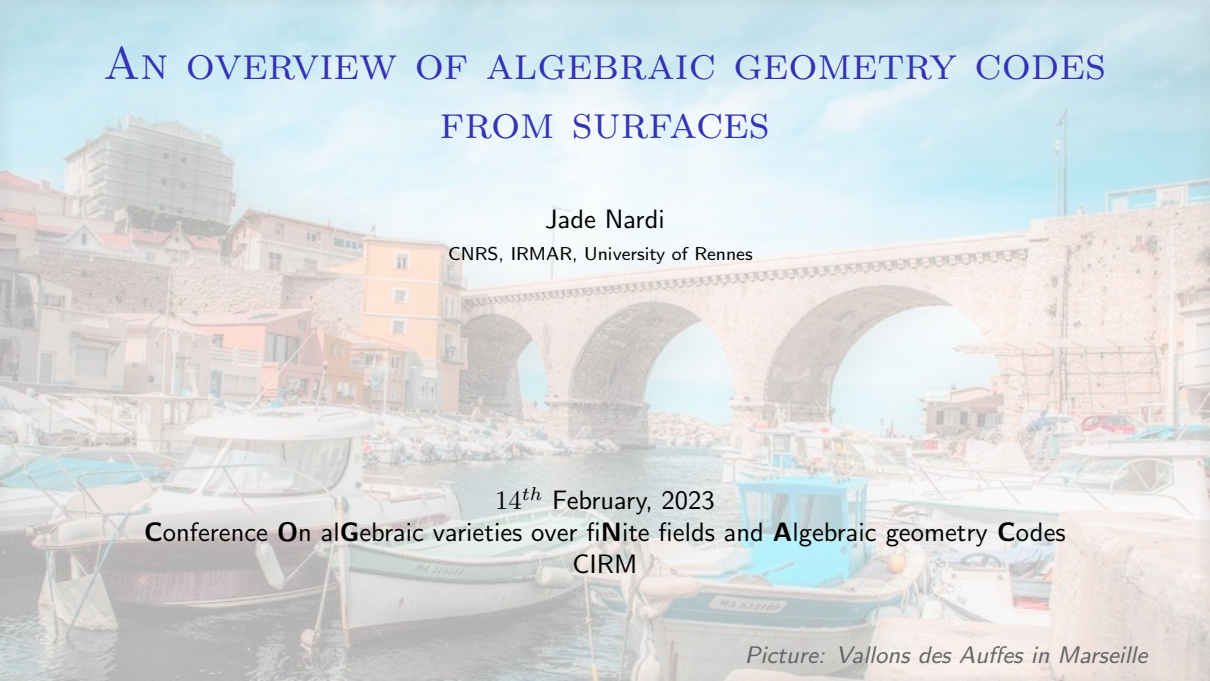
An overview of algebraic geometry codes from surfaces

Jade Nardi
CNRS, IRMAR, University of Rennes

14^{th} February, 2023
Conference **O**n al**G**ebraic varieties over fi**N**ite fields and **A**lgebraic geometry **C**odes
CIRM



Picture: Vallons des Auffes in Marseille

Outline of the presentation

Table of Contents

Algebraic geometry...

Let $\mathcal{X}$ be a smooth projective variety defined over the finite field $\mathbb{F}_q$.

Definition: Divisors and their properties.

A (Weil) divisor on $\mathcal{X}$ is a formal finite sum of irreducible subvarieties of $\mathcal{X}$ of codimension 1. The set of divisors of the variety $\mathcal{X}$ is denoted by $\operatorname{Div} \mathcal{X}$.

Algebraic geometry...

Let $\mathcal{X}$ be a smooth projective variety defined over the finite field $\mathbb{F}_q$.

Definition: Divisors and their properties.

A (Weil) divisor on $\mathcal{X}$ is a formal finite sum of irreducible subvarieties of $\mathcal{X}$ of codimension 1. The set of divisors of the variety $\mathcal{X}$ is denoted by $\operatorname{Div}\mathcal{X}$.

A divisor $G = \sum n_i \mathcal{Y}_i$ is said to be effective if $n_i \geq 0$ for every i. In this case, we write $G \geq 0$.

The support of a divisor $G = \sum n_i \mathcal{Y}_i$, is $\operatorname{Supp} G = \bigcup_{i \geq 1} \{\mathcal{Y}_i \mid n_i \neq 0\}$.

Its Riemann–Roch space is the $\mathbb{F}_q$–vector space

$$L(G) = \{f \in \mathbb{F}_q(X)^* \mid (f) + G \geq 0\} \cup \{0\}$$

where $(f) = \sum \operatorname{ord}_{\mathcal{Y}}(f)\mathcal{Y}$ is the principal divisor associated to a non–zero function f.

Algebraic geometry...

Let $\mathcal{X}$ be a smooth projective variety defined over the finite field $\mathbb{F}_q$.

Definition: Divisors and their properties.

A (Weil) divisor on $\mathcal{X}$ is a formal finite sum of irreducible subvarieties of $\mathcal{X}$ of codimension 1. The set of divisors of the variety $\mathcal{X}$ is denoted by $\operatorname{Div}\mathcal{X}$.

A divisor $G = \sum n_i \mathcal{Y}_i$ is said to be effective if $n_i \geq 0$ for every i. In this case, we write $G \geq 0$.

The support of a divisor $G = \sum n_i \mathcal{Y}_i$, is $\operatorname{Supp} G = \bigcup_{i \geq 1} \{\mathcal{Y}_i \mid n_i \neq 0\}$.

Its Riemann–Roch space is the $\mathbb{F}_q$–vector space

global section

$$L(G) = \{f \in \mathbb{F}_q(X)^* \mid (f) + G \geq 0\} \cup \{0\}$$

where $(f) = \sum \operatorname{ord}_{\mathcal{Y}}(f)\mathcal{Y}$ is the principal divisor associated to a non–zero function f.

Algebraic geometry...

Let $\mathcal{X}$ be a smooth projective variety defined over the finite field $\mathbb{F}_q$.

Definition: Divisors and their properties.

A (Weil) divisor on $\mathcal{X}$ is a formal finite sum of irreducible subvarieties of $\mathcal{X}$ of codimension 1.
The set of divisors of the variety $\mathcal{X}$ is denoted by $\operatorname{Div}\mathcal{X}$.

A divisor $G = \sum n_i \mathcal{Y}_i$ is said to be effective if $n_i \geq 0$ for every i. In this case, we write $G \geq 0$.
The support of a divisor $G = \sum n_i \mathcal{Y}_i$, is $\operatorname{Supp} G = \bigcup_{i \geq 1} \{\mathcal{Y}_i \mid n_i \neq 0\}$.
Its Riemann–Roch space is the $\mathbb{F}_q$–vector space

global section

$$L(G) = \{f \in \mathbb{F}_q(X)^* \mid (f) + G \geq 0\} \cup \{0\}$$

where $(f) = \sum \operatorname{ord}_{\mathcal{Y}}(f)\mathcal{Y}$ is the principal divisor associated to a non–zero function f.

Definition: Linear equivalence and Picard Group.

Two divisors are linearly equivalent if there is a function h such that $G' = G + (h)$, noted $G' \sim G$.
The Picard group $\operatorname{Pic}\mathcal{X}$ is the set of equivalent classes of $\operatorname{Div}\mathcal{X}$ modulo the linear equivalence $\sim$.

...Codes

Definition: $[n, k, d]$ linear code

A linear code C over $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$. We note k its dimension.
The weight of a word $\boldsymbol{x} \in \mathbb{F}_q^n$ is given by $\omega(\boldsymbol{x}) = \#\{i \in \{1, \ldots, n\},\ x_i \neq 0\}$.
The minimum distance of C is defined by $d = \min\{\omega(\boldsymbol{c}) \mid \boldsymbol{c} \in C,\ \boldsymbol{c} \neq \boldsymbol{0}\}$.

...Codes

Definition: $[n, k, d]$ linear code

A linear code C over $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$. We note k its dimension.
The weight of a word $\boldsymbol{x} \in \mathbb{F}_q^n$ is given by $\omega(\boldsymbol{x}) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$.
The minimum distance of C is defined by $d = \min\{\omega(\boldsymbol{c}) \mid \boldsymbol{c} \in C,\ \boldsymbol{c} \neq \boldsymbol{0}\}$.

Algebraic geometry codes **Tsfasman and Vladut's L-construction**

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$. Consider the map

$$\operatorname{ev}_{\mathcal{P}} : \begin{cases} L(G) & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \dots, f(P_n)) \end{cases}$$

well–defined

The AG code associated to G with evaluation support $\mathcal{P}$ is $C(\mathcal{X}, \mathcal{P}, G) = \operatorname{ev}_{\mathcal{P}}(L(G))$.

Remark: If $G' \sim G$, then $C(\mathcal{X}, \mathcal{P}, G)$ and $C(\mathcal{X}, \mathcal{P}, G')$ are equivalent.

...Codes

Definition: $[n, k, d]$ linear code

A linear code C over $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$. We note k its dimension.
The weight of a word $\boldsymbol{x} \in \mathbb{F}_q^n$ is given by $\omega(\boldsymbol{x}) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$.
The minimum distance of C is defined by $d = \min\{\omega(\boldsymbol{c}) \mid \boldsymbol{c} \in C,\ \boldsymbol{c} \neq \boldsymbol{0}\}$.

Algebraic geometry codes **Tsfasman and Vladut's L-construction**

Take $\mathcal{P} = \{P_1, \dots, P_n,\} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$. Consider the map

$$\operatorname{ev}_{\mathcal{P}} : \begin{cases} L(G) & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \dots, f(P_n)) \end{cases}$$

well–defined

The AG code associated to G with evaluation support $\mathcal{P}$ is $C(\mathcal{X}, \mathcal{P}, G) = \operatorname{ev}_{\mathcal{P}}(L(G))$.

Remark: If $G' \sim G$, then $C(\mathcal{X}, \mathcal{P}, G)$ and $C(\mathcal{X}, \mathcal{P}, G')$ are equivalent.

It has length $n = \#\mathcal{P}$ and dimension $k \leq \ell(G)$, $= \dim L(G)$
For $f \in L(G)$, $\omega(\operatorname{ev}_{\mathcal{P}}(f)) = n - \#(\mathcal{Z}(f) \cap \mathcal{P})$ where $\mathcal{Z}(f)$ is the zero locus of f.
Then the minimum distance satisfies $d = n - \max_{f \in L(G) \setminus \{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P})$.

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \ldots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G) \setminus \{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \ldots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G) \setminus \{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max\limits_{f \in L(G) \setminus \{0\}} \#\left(\mathcal{Z}(f) \cap \mathcal{P}\right) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max\limits_{f \in L(G) \setminus \{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G) \setminus \{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max\limits_{f \in L(G)\setminus\{0\}} \#\left(\mathcal{Z}(f) \cap \mathcal{P}\right) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

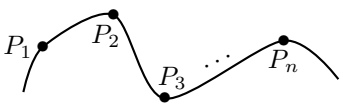
For every $f \in L(G)$, $\#\mathcal{Z}(f) \leq \deg G$.

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$



Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G)\setminus\{0\}} \#\left(\mathcal{Z}(f) \cap \mathcal{P}\right) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

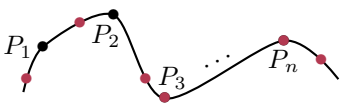
For every $f \in L(G)$, $\#\mathcal{Z}(f) \leq \deg G$.

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$



Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G)\setminus\{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

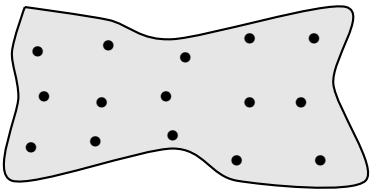
For every $f \in L(G)$, $\#\mathcal{Z}(f) \leq \deg G$.

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$



If $\mathcal{X}$ is a **surface**, $\mathcal{Z}(f)$ is a (possibly reducible) curve on $\mathcal{X}$.
Computing $\#\mathcal{Z}(f) \cap \mathcal{P}$ is harder...

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G)\setminus\{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

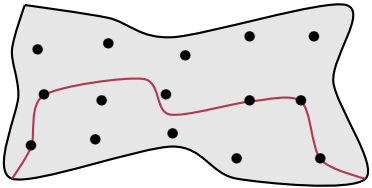
For every $f \in L(G)$, $\#\mathcal{Z}(f) \leq \deg G$.

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$



If $\mathcal{X}$ is a **surface**, $\mathcal{Z}(f)$ is a (possibly reducible) curve on $\mathcal{X}$.
Computing $\#\mathcal{Z}(f) \cap \mathcal{P}$ is harder...

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G)\setminus\{0\}} \#\left(\mathcal{Z}(f) \cap \mathcal{P}\right) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

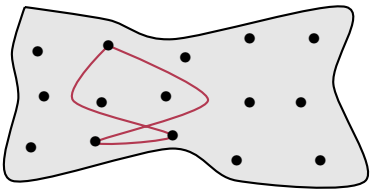
For every $f \in L(G)$, $\#\mathcal{Z}(f) \leq \deg G$.

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$



If $\mathcal{X}$ is a **surface**, $\mathcal{Z}(f)$ is a (possibly reducible) curve on $\mathcal{X}$.
Computing $\#\mathcal{Z}(f) \cap \mathcal{P}$ is harder...

Algebraic geometry codes: parameters

Take $\mathcal{P} = \{P_1, \dots, P_n, \} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ s.t. $\operatorname{Supp} G \cap \mathcal{P} = \varnothing$.

$$C(\mathcal{X}, \mathcal{P}, G) = \{(f(P_1), \dots, f(P_n)) \in \mathbb{F}_q^n \mid f \in L(G)\}.$$

If $\max_{f \in L(G)\setminus\{0\}} \#(\mathcal{Z}(f) \cap \mathcal{P}) \leq b < n$, then $C(\mathcal{X}, \mathcal{P}, G)$ has parameters $[n, \ell(G), \geq n - b]$.

If $\mathcal{X}$ is a (smooth projective) **curve** of genus g, then $G = \sum n_i P_i$ with $\deg G = \sum n_i \deg P_i$.

Hasse–Weil theorem

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

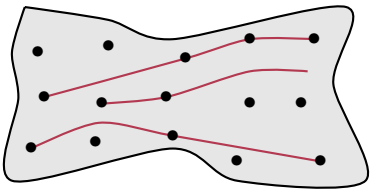
For every $f \in L(G)$, $\#\mathcal{Z}(f) \leq \deg G$.

Riemann–Roch theorem on curves

$$\ell(G) - \ell(K_{\mathcal{X}} - G) = \deg G - g + 1.$$

$= 0$ if $\deg G > 2g - 2$.

Canonical divisor of $\mathcal{X}$



If $\mathcal{X}$ is a **surface**, $\mathcal{Z}(f)$ is a (possibly reducible) curve on $\mathcal{X}$.
Computing $\#\mathcal{Z}(f) \cap \mathcal{P}$ is harder...

Very first example of AG codes from higher–dimensional varieties: Reed–Muller codes

Definition: Reed–Muller code

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

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

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

Very first example of AG codes from higher–dimensional varieties: Reed–Muller codes

Definition: Reed–Muller code

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

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

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

Why is it an AG code?
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 $\mathsf{RM}(N,r) = C(\mathbb{P}^N, \mathcal{P}, rH)$.

(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 when $\mathcal{P}$ is a complete intersection (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 when $\mathcal{P}$ is a complete intersection (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)
- 2020: Del Pezzo surfaces with Picard rank one (Blache, Couvreur, Hallouin, Madore, N., Rambaud, Randriam)
- 2021: Abelian surfaces (Aubry, Berardini, Herbaut, Perret)

Embedded case

Definition: Restriction of a code

Let $C \subseteq \mathbb{F}_q^n$. Take $I \subset \{1, \ldots, n\}$. The **restriction** of C to I is $p_I(C)$ where $p_I : \mathbb{F}_q^n \to \mathbb{F}_q^{\#I}$ is defined by $p_I(c_1, \ldots, c_n) = (c_i)_{i \in I}$. (*Puncturing* outside of I.)

- If $C = C(\mathcal{X}, \mathcal{P}, G)$ and $\mathcal{P}' \subset \mathcal{P}$, then $C' = C(\mathcal{X}, \mathcal{P}', G)$ is a restriction of C.
- If $\mathcal{Y} \subset \mathcal{X}$, we can restrict C to $\mathcal{Y}$: $C_{|\mathcal{Y}} = C(\mathcal{Y}, \mathcal{P} \cap \mathcal{Y}, G \cap \mathcal{Y})$. ← divisor on $\mathcal{Y}$

Embedded case

Definition: Restriction of a code

Let $C \subseteq \mathbb{F}_q^n$. Take $I \subset \{1, \dots, n\}$. The **restriction** of C to I is $p_I(C)$ where $p_I : \mathbb{F}_q^n \to \mathbb{F}_q^{\#I}$ is defined by $p_I(c_1, \dots, c_n) = (c_i)_{i \in I}$. (*Puncturing* outside of I.)

- If $C = C(\mathcal{X}, \mathcal{P}, G)$ and $\mathcal{P}' \subset \mathcal{P}$, then $C' = C(\mathcal{X}, \mathcal{P}', G)$ is a restriction of C.
- If $\mathcal{Y} \subset \mathcal{X}$, we can restrict C to $\mathcal{Y}$: $C_{|\mathcal{Y}} = C(\mathcal{Y}, \mathcal{P} \cap \mathcal{Y}, G \cap \mathcal{Y})$. ← divisor on $\mathcal{Y}$

Assume that $\mathcal{X} \subset \mathbb{P}^N$ for some $N \geq 2$. Let H be an hyperplane of $\mathbb{P}^N$ (say $X_0 = 0$ again). Take $\mathcal{P} \subseteq (\mathbb{A}^N \cap \mathcal{X})(\mathbb{F}_q)$. For $r \geq 0$, consider the restriction of $\mathrm{RM}(N, r)$ to $\mathcal{P}$

hyperplane section $H \cap \mathcal{X}$

$$C(\mathbb{P}^N, \mathcal{P}, rH) = \{(f(P))_{P \in \mathcal{P}} \mid f \in L(rH)\} \simeq C(\mathcal{X}, \mathcal{P}, rh).$$

Embedded case

Definition: Restriction of a code

Let $C \subseteq \mathbb{F}_q^n$. Take $I \subset \{1, \dots, n\}$. The **restriction** of C to I is $p_I(C)$ where $p_I : \mathbb{F}_q^n \to \mathbb{F}_q^{\#I}$ is defined by $p_I(c_1, \dots, c_n) = (c_i)_{i \in I}$. (*Puncturing* outside of I.)

- If $C = C(\mathcal{X}, \mathcal{P}, G)$ and $\mathcal{P}' \subset \mathcal{P}$, then $C' = C(\mathcal{X}, \mathcal{P}', G)$ is a restriction of C.
- If $\mathcal{Y} \subset \mathcal{X}$, we can restrict C to $\mathcal{Y}$: $C_{|\mathcal{Y}} = C(\mathcal{Y}, \mathcal{P} \cap \mathcal{Y}, G \cap \mathcal{Y})$. ← divisor on $\mathcal{Y}$

Assume that $\mathcal{X} \subset \mathbb{P}^N$ for some $N \geq 2$. Let H be an hyperplane of $\mathbb{P}^N$ (say $X_0 = 0$ again). Take $\mathcal{P} \subseteq (\mathbb{A}^N \cap \mathcal{X})(\mathbb{F}_q)$. For $r \geq 0$, consider the restriction of $\mathrm{RM}(N, r)$ to $\mathcal{P}$

hyperplane section $H \cap \mathcal{X}$

$$C(\mathbb{P}^N, \mathcal{P}, rH) = \{(f(P))_{P \in \mathcal{P}} \mid f \in L(rH)\} \simeq C(\mathcal{X}, \mathcal{P}, rh).$$

To handle the parameters, we can use properties of the 0-dimensional algebraic set $\mathcal{P}$.

$$0 \to \mathcal{I}_{\mathcal{P}} \to \mathcal{O}_{\mathbb{P}^N} \to \mathcal{O}_{\mathcal{P}} \to 0$$

measures how the points in $\mathcal{P}$ fail to give independent relations in degree r

$$0 \to \underbrace{H^0(\mathcal{I}_{\mathcal{P}}(r))}_{\ker \mathrm{ev}_{\mathcal{P}}} \to H^0(\mathcal{O}_{\mathbb{P}^N}(r)) \to H^0(\mathcal{O}_{\mathcal{P}}(r)) \to H^1(\mathcal{I}_{\mathcal{P}}(r)) \to 0$$

Embedded case

Definition: Restriction of a code

Let $C \subseteq \mathbb{F}_q^n$. Take $I \subset \{1, \dots, n\}$. The **restriction** of C to I is $p_I(C)$ where $p_I : \mathbb{F}_q^n \to \mathbb{F}_q^{\#I}$ is defined by $p_I(c_1, \dots, c_n) = (c_i)_{i \in I}$. (*Puncturing* outside of I.)

- If $C = C(\mathcal{X}, \mathcal{P}, G)$ and $\mathcal{P}' \subset \mathcal{P}$, then $C' = C(\mathcal{X}, \mathcal{P}', G)$ is a restriction of C.
- If $\mathcal{Y} \subset \mathcal{X}$, we can restrict C to $\mathcal{Y}$: $C_{|\mathcal{Y}} = C(\mathcal{Y}, \mathcal{P} \cap \mathcal{Y}, G \cap \mathcal{Y})$. ← divisor on $\mathcal{Y}$

Assume that $\mathcal{X} \subset \mathbb{P}^N$ for some $N \geq 2$. Let H be an hyperplane of $\mathbb{P}^N$ (say $X_0 = 0$ again). Take $\mathcal{P} \subseteq (\mathbb{A}^N \cap \mathcal{X})(\mathbb{F}_q)$. For $r \geq 0$, consider the restriction of $\mathrm{RM}(N, r)$ to $\mathcal{P}$

$$C(\mathbb{P}^N, \mathcal{P}, rH) = \{(f(P))_{P \in \mathcal{P}} \mid f \in L(rH)\} \simeq C(\mathcal{X}, \mathcal{P}, rh).$$

hyperplane section $H \cap \mathcal{X}$

To handle the parameters, we can use properties of the 0-dimensional algebraic set $\mathcal{P}$.

$$0 \to \mathcal{I}_{\mathcal{P}} \to \mathcal{O}_{\mathbb{P}^N} \to \mathcal{O}_{\mathcal{P}} \to 0$$

measures how the points in $\mathcal{P}$ fail to give independent relations in degree r

$$0 \to \underbrace{H^0(\mathcal{I}_{\mathcal{P}}(r))}_{\ker \mathrm{ev}_{\mathcal{P}}} \to H^0(\mathcal{O}_{\mathbb{P}^N}(r)) \to H^0(\mathcal{O}_{\mathcal{P}}(r)) \to H^1(\mathcal{I}_{\mathcal{P}}(r)) \to 0$$

👍 Explicit generating family. 👎 Cannot explore all the AG codes on $\mathcal{X}$.

Table of Contents

An important tool on surfaces

Theorem: Intersection product on a surface

There is a unique pairing $\operatorname{Div}\mathcal{X} \times \operatorname{Div}\mathcal{X} \to \mathbb{Z}$, denoted by $C \cdot D$ for any two divisors C, D, s.t.

1. if C and D are nonsingular curves meeting transversally, then $C \cdot D = \#(C \cap D)$;
2. it is symmetric: $C \cdot D = D \cdot C$;
3. it is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$;
4. it depends only on the linear equivalence classes: if $C_1 \sim C_2$, then $C_1 \cdot D = C_2 \cdot D$.

We denote by $C^2 = C \cdot C$ the *self–intersection* of $C \in \operatorname{Div}\mathcal{X}$.

An important tool on surfaces

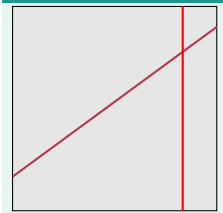
Theorem: Intersection product on a surface

There is a unique pairing $\operatorname{Div}\mathcal{X} \times \operatorname{Div}\mathcal{X} \to \mathbb{Z}$, denoted by $C \cdot D$ for any two divisors C, D, s.t.

1. if C and D are nonsingular curves meeting transversally, then $C \cdot D = \#(C \cap D)$;
2. it is symmetric: $C \cdot D = D \cdot C$;
3. it is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$;
4. it depends only on the linear equivalence classes: if $C_1 \sim C_2$, then $C_1 \cdot D = C_2 \cdot D$.

We denote by $C^2 = C \cdot C$ the *self–intersection* of $C \in \operatorname{Div}\mathcal{X}$.

Intersection product on $\mathcal{X} = \mathbb{P}^2$



Let L, L' be 2 lines. Then $L \sim L''$ and $L^2 = L'^2 = L \cdot L' = 1$.

An important tool on surfaces

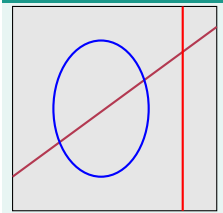
Theorem: Intersection product on a surface

There is a unique pairing $\operatorname{Div}\mathcal{X} \times \operatorname{Div}\mathcal{X} \to \mathbb{Z}$, denoted by $C \cdot D$ for any two divisors C, D, s.t.

1. if C and D are nonsingular curves meeting transversally, then $C \cdot D = \#(C \cap D)$;
2. it is symmetric: $C \cdot D = D \cdot C$;
3. it is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$;
4. it depends only on the linear equivalence classes: if $C_1 \sim C_2$, then $C_1 \cdot D = C_2 \cdot D$.

We denote by $C^2 = C \cdot C$ the *self–intersection* of $C \in \operatorname{Div}\mathcal{X}$.

Intersection product on $\mathcal{X} = \mathbb{P}^2$



Let L, L' be 2 lines. Then $L \sim L''$ and $L^2 = L'^2 = L \cdot L' = 1$.
Let C be a conic. Then $L \cdot C = L' \cdot C = 2$. Moreover, $C \sim 2L$.

An important tool on surfaces

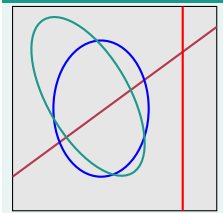
Theorem: Intersection product on a surface

There is a unique pairing $\operatorname{Div}\mathcal{X} \times \operatorname{Div}\mathcal{X} \to \mathbb{Z}$, denoted by $C \cdot D$ for any two divisors C, D, s.t.

1. if C and D are nonsingular curves meeting transversally, then $C \cdot D = \#(C \cap D)$;
2. it is symmetric: $C \cdot D = D \cdot C$;
3. it is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$;
4. it depends only on the linear equivalence classes: if $C_1 \sim C_2$, then $C_1 \cdot D = C_2 \cdot D$.

We denote by $C^2 = C \cdot C$ the *self–intersection* of $C \in \operatorname{Div}\mathcal{X}$.

Intersection product on $\mathcal{X} = \mathbb{P}^2$



Let L, L' be 2 lines. Then $L \sim L''$ and $L^2 = L'^2 = L \cdot L' = 1$.
Let C be a conic. Then $L \cdot C = L' \cdot C = 2$. Moreover, $C \sim 2L$.
Let C' another conic. Then $C' \sim C$. And $C^2 = C \cdot C' = 4$.

An important tool on surfaces

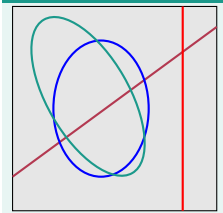
Theorem: Intersection product on a surface

There is a unique pairing $\operatorname{Div}\mathcal{X} \times \operatorname{Div}\mathcal{X} \to \mathbb{Z}$, denoted by $C \cdot D$ for any two divisors C, D, s.t.

1. if C and D are nonsingular curves meeting transversally, then $C \cdot D = \#(C \cap D)$;
2. it is symmetric: $C \cdot D = D \cdot C$;
3. it is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$;
4. it depends only on the linear equivalence classes: if $C_1 \sim C_2$, then $C_1 \cdot D = C_2 \cdot D$.

We denote by $C^2 = C \cdot C$ the *self–intersection* of $C \in \operatorname{Div}\mathcal{X}$.

Intersection product on $\mathcal{X} = \mathbb{P}^2$



Let L, L' be 2 lines. Then $L \sim L''$ and $L^2 = L'^2 = L \cdot L' = 1$.
Let C be a conic. Then $L \cdot C = L' \cdot C = 2$. Moreover, $C \sim 2L$.
Let C' another conic. Then $C' \sim C$. And $C^2 = C \cdot C' = 4$.
For any curve D of degree d, $D \sim dL$.
Two curves are linearly equivalent iff they have the same degree.
Then $D \cdot D' = dL \cdot d'L = dd'$. (Bézout's theorem)

Dimension of AG codes from surfaces

Denote by $K_{\mathcal{X}}$ a canonical divisor of $\mathcal{X}$.

Riemann–Roch theorem on surfaces

If $G \in \operatorname{Div} \mathcal{X}$, then

superabundance $h^1(\mathcal{X}, \mathcal{L}(G))$

Arithmetic genus of $\mathcal{X}$: $p_a(\mathcal{X}) = \chi(\mathcal{O}_{\mathcal{X}}) + 1$.

$$\chi(\mathcal{L}(G)) = \ell(G) - s(G) + \ell(K_{\mathcal{X}} - G) = \frac{1}{2} G \cdot (G - K_{\mathcal{X}}) + 1 + p_a(\mathcal{X}).$$

$h^0(\mathcal{X}, \mathcal{L}(G))$

$h^2(\mathcal{X}, \mathcal{L}(G))$ + Serre's duality

Dimension of AG codes from surfaces

Denote by $K_{\mathcal{X}}$ a canonical divisor of $\mathcal{X}$.

Riemann–Roch theorem on surfaces

If $G \in \operatorname{Div} \mathcal{X}$, then

superabundance $h^1(\mathcal{X}, \mathcal{L}(G))$

Arithmetic genus of $\mathcal{X}$: $p_a(\mathcal{X}) = \chi(\mathcal{O}_{\mathcal{X}}) + 1$.

$$\chi(\mathcal{L}(G)) = \ell(G) - s(G) + \ell(K_{\mathcal{X}} - G) = \frac{1}{2} G \cdot (G - K_{\mathcal{X}}) + 1 + p_a(\mathcal{X}).$$

$h^0(\mathcal{X}, \mathcal{L}(G))$

$h^2(\mathcal{X}, \mathcal{L}(G))$ + Serre's duality

Definition: ample divisor (Nakai–Moishezon criterion)

A divisor $A \in \operatorname{Div} \mathcal{X}$ is said to be *ample* if $A^2 > 0$ and for every irreducible curve, $C \cdot A > 0$.

Dimension of AG codes from surfaces

Denote by $K_{\mathcal{X}}$ a canonical divisor of $\mathcal{X}$.

Riemann–Roch theorem on surfaces

If $G \in \operatorname{Div} \mathcal{X}$, then

superabundance $h^1(\mathcal{X}, \mathcal{L}(G))$

Arithmetic genus of $\mathcal{X}$: $p_a(\mathcal{X}) = \chi(\mathcal{O}_{\mathcal{X}}) + 1$.

$$\chi(\mathcal{L}(G)) = \ell(G) - s(G) + \ell(K_{\mathcal{X}} - G) = \frac{1}{2} G \cdot (G - K_{\mathcal{X}}) + 1 + p_a(\mathcal{X}).$$

$h^0(\mathcal{X}, \mathcal{L}(G))$

$h^2(\mathcal{X}, \mathcal{L}(G))$ + Serre's duality

Definition: ample divisor (Nakai–Moishezon criterion)

A divisor $A \in \operatorname{Div} \mathcal{X}$ is said to be *ample* if $A^2 > 0$ and for every irreducible curve, $C \cdot A > 0$.

Proposition

If there exists an ample divisor A such that $K_{\mathcal{X}} \cdot A < G \cdot A$, then $\ell(K_{\mathcal{X}} - G) = 0$.

$$\Rightarrow \ell(G) \geq \frac{1}{2} G \cdot (G - K_{\mathcal{X}}) + 1 + p_a(\mathcal{X}).$$

How to get a lower bound for the minimum distance?

Assume that $\mathcal{P} = \mathcal{X}(\mathbb{F}_q)$.

For any $f \in L(G)$, we decompose its zero locus $\mathcal{Z}(f) = \sum_{i=1}^{s_f} n_i \mathcal{Y}_i$ with $n_i > 0$.

Then the minimum distance satisfies

$$d \geq n - \max_{f \in L(G) \setminus \{0\}} \sum \#\mathcal{Y}_i(\mathbb{F}_q).$$

To bound the minimum distance from below, you need an upper bound for

- the number of irreducible components s_f,
- the number of $\mathbb{F}_q$–rational points of the curves $\mathcal{Y}_i$.

e.g. Berardini, N. (2022) for $\mathcal{X} \subset \mathbb{P}^3$
See Elena Berardini's talk this afternoon

Adjunction formula

If $\mathcal{C}$ is a curve of arithmetic genus π on the surface $\mathcal{X}$, then

$$2\pi - 2 = \mathcal{C} \cdot (\mathcal{C} + K_{\mathcal{X}}).$$

A generic lower bound for the minimum distance: Seshadri constant

Let $\mathcal{P} = \{P_1 \dots, P_n\} \subset \mathcal{X}(\mathbb{F}_q)$ and $G \in \operatorname{Div} \mathcal{X}$ an ample divisor.

Definition: Seshadri constant

The *Seshadri constant* of G at $\mathcal{P}$ is $\varepsilon(G, \mathcal{P}) = \inf \left\{ \dfrac{G \cdot C}{\sum_i m_{P_i} C} \mid C \subset \mathcal{X} \text{ curves s.t. } C \cap \mathcal{P} \neq \varnothing \right\}$.

multiplicity of the curve C at P_i

Proposition — **Hansen (2001)**

1. If $\varepsilon(G, \mathcal{P}) \geq \varepsilon \in \mathbb{N}$, then the minimum distance of $C(\mathcal{X}, \mathcal{P}, G)$ satisfies $d \geq n - \dfrac{G^2}{\varepsilon}$.
2. If there exists $\zeta \in \mathbb{N}$ s.t. $\mathcal{L}(G)^{\otimes \zeta} \otimes \mathcal{I}_{\mathcal{P}}$ is generated by global sections, then $d \geq n - \zeta G^2$.

👎 Hard to compute in practice!

Lower bound for the minimum distance: $\mathcal{P}$–covering curves

Proposition **Hansen (2001)**

Fix some curves $C_1, \ldots, C_r$ on $\mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup_i \mathcal{C}_i(\mathbb{F}_q)$,
- $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$,
- $G \cdot \mathcal{C}_i \geq 0$.

Set $\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq \mathcal{Z}(f)\}$.

Then the minimum distance of $C(\mathcal{X}, \mathcal{P}, G)$ satisfies $d \geq n - \ell N - \sum_{i=1}^{r} G \cdot \mathcal{C}_i$.

Lower bound for the minimum distance: $\mathcal{P}$–covering curves

Proposition **Hansen (2001)**

Fix some curves $C_1, \ldots, C_r$ on $\mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup_i \mathcal{C}_i(\mathbb{F}_q)$,
- $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$,
- $G \cdot \mathcal{C}_i \geq 0$.

Set $\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq \mathcal{Z}(f)\}$.

Then the minimum distance of $C(\mathcal{X}, \mathcal{P}, G)$ satisfies $d \geq n - \ell N - \sum_{i=1}^{r} G \cdot \mathcal{C}_i$.

If $G \cdot \mathcal{C}_i \leq \eta \leq N$, then $d \geq n - \ell N - (r - \ell)\eta$.

Lower bound for the minimum distance: $\mathcal{P}$–covering curves

Proposition — **Hansen (2001)**

Fix some curves $C_1, \dots, C_r$ on $\mathcal{X}$ s.t.

- $\mathcal{P} \subseteq \bigcup_i \mathcal{C}_i(\mathbb{F}_q)$,
- $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$,
- $G \cdot \mathcal{C}_i \geq 0$.

Set $\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq \mathcal{Z}(f)\}$.

Then the minimum distance of $C(\mathcal{X}, \mathcal{P}, G)$ satisfies $d \geq n - \ell N - \sum_{i=1}^{r} G \cdot \mathcal{C}_i$.

If $G \cdot \mathcal{C}_i \leq \eta \leq N$, then $d \geq n - \ell N - (r - \ell)\eta$.

Moreover, if there exists a nef divisor H s.t. $H \cdot \mathcal{C}_i > 0$ for every i, then $\ell \leq \dfrac{G \cdot H}{\min_i\{\mathcal{C}_i \cdot H\}}$.

nef: $H \cdot \mathcal{C} \geq 0$ for every curve $\mathcal{C}$.

Application of the $\mathcal{P}$–covering curves method to $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

Proposition **Hansen (2001)**

$\mathcal{P} \subseteq \bigcup_{i=1}^{r} \mathcal{C}_i(\mathbb{F}_q)$, $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$ and $0 \leq G \cdot \mathcal{C}_i \leq \eta \leq N$.

$\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq (f = 0)\} \leq \dfrac{G \cdot H}{\min_i\{\mathcal{C}_i \cdot H\}}$ if there exists a nef divisor H s.t. $H \cdot \mathcal{C}_i > 0$.

$$d \geq n - \ell N - (r - \ell)\eta.$$

Application of the $\mathcal{P}$–covering curves method to $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

Proposition — **Hansen (2001)**

$\mathcal{P} \subseteq \bigcup_{i=1}^{r} \mathcal{C}_i(\mathbb{F}_q)$, $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$ and $0 \leq G \cdot \mathcal{C}_i \leq \eta \leq N$.

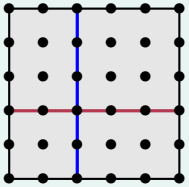
$\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq (f = 0)\} \leq \dfrac{G \cdot H}{\min_i\{\mathcal{C}_i \cdot H\}}$ if there exists a nef divisor H s.t. $H \cdot \mathcal{C}_i > 0$.

$$d \geq n - \ell N - (r - \ell)\eta.$$

On $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

$\operatorname{Pic} \mathcal{X} = \mathbb{Z}[H] \oplus \mathbb{Z}[V]$ with $H^2 = V^2 = 0$ and $H \cdot V = 1$. Take $G = d_1 H + d_2 V$. We have

$$L(G) \simeq \{\text{bihomogeneous } f \in \mathbb{F}_q[X_0, X_1, Y_0, Y_1] \mid \deg_X(f) = d_1 \text{ and } \deg_Y(f) = d_2\}.$$



Application of the $\mathcal{P}$–covering curves method to $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

Proposition — **Hansen (2001)**

$\mathcal{P} \subseteq \bigcup_{i=1}^{r} \mathcal{C}_i(\mathbb{F}_q)$, $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$ and $0 \leq G \cdot \mathcal{C}_i \leq \eta \leq N$.

$\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq (f = 0)\} \leq \dfrac{G \cdot H}{\min_i\{\mathcal{C}_i \cdot H\}}$ if there exists a nef divisor H s.t. $H \cdot \mathcal{C}_i > 0$.

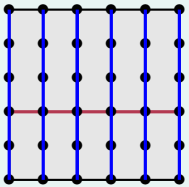
$$d \geq n - \ell N - (r - \ell)\eta.$$

On $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

$\operatorname{Pic} \mathcal{X} = \mathbb{Z}[H] \oplus \mathbb{Z}[V]$ with $H^2 = V^2 = 0$ and $H \cdot V = 1$. Take $G = d_1 H + d_2 V$. We have

$$L(G) \simeq \{\text{bihomogeneous } f \in \mathbb{F}_q[X_0, X_1, Y_0, Y_1] \mid \deg_X(f) = d_1 \text{ and } \deg_Y(f) = d_2\}.$$

Choose $\mathcal{P} = \mathcal{X}(\mathbb{F}_q)$ and $r = q + 1$ vertical lines $\mathcal{C}_i \sim V \Rightarrow N = q + 1$.



Application of the $\mathcal{P}$–covering curves method to $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

Proposition — **Hansen (2001)**

$\mathcal{P} \subseteq \bigcup_{i=1}^{r} \mathcal{C}_i(\mathbb{F}_q)$, $\#(\mathcal{C}_i(\mathbb{F}_q) \cap \mathcal{P}) \leq N$ and $0 \leq G \cdot \mathcal{C}_i \leq \eta \leq N$.

$\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq (f = 0)\} \leq \dfrac{G \cdot H}{\min_i\{\mathcal{C}_i \cdot H\}}$ if there exists a nef divisor H s.t. $H \cdot \mathcal{C}_i > 0$.

$$d \geq n - \ell N - (r - \ell)\eta.$$

On $\mathcal{X} = \mathbb{P}^1 \times \mathbb{P}^1$

$\operatorname{Pic} \mathcal{X} = \mathbb{Z}[H] \oplus \mathbb{Z}[V]$ with $H^2 = V^2 = 0$ and $H \cdot V = 1$. Take $G = d_1 H + d_2 V$. We have

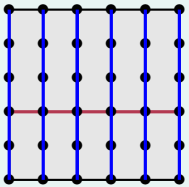
$$L(G) \simeq \{\text{bihomogeneous } f \in \mathbb{F}_q[X_0, X_1, Y_0, Y_1] \mid \deg_X(f) = d_1 \text{ and } \deg_Y(f) = d_2\}.$$

Choose $\mathcal{P} = \mathcal{X}(\mathbb{F}_q)$ and $r = q + 1$ vertical lines $\mathcal{C}_i \sim V \Rightarrow N = q + 1$.

Since $H \cdot \mathcal{C}_i = H \cdot V = 1$, we have $\ell \leq G \cdot H = d_2$.

$$n = (q+1)^2, \qquad k = (d_1 + 1)(d_2 + 1)$$

$$d \geq n - d_2(q+1) - (q + 1 - d_2)d_1 = (q + 1 - d_1)(q + 1 - d_2)$$



Attained!

Lower bound for the minimum distance: $\mathcal{P}$–interpolating linear system

Definition: Linear system

- A *linear system* is a family of linearly equivalent effective divisors.
- The *base locus* of a linear system Γ is defined as $\bigcap_{D\in\Gamma} \operatorname{Supp} D$.
- For any linear system $\Gamma \subset \operatorname{Div} \mathcal{X}$ and $\mathcal{Y} \subset \mathcal{X}$ a subvariety, we denote by $\Gamma - \mathcal{Y}$ the maximal linear subsystem of Γ of elements whose base locus contains $\mathcal{Y}$.

Lower bound for the minimum distance: $\mathcal{P}$–interpolating linear system

Definition: Linear system

- A *linear system* is a family of linearly equivalent effective divisors.
- The *base locus* of a linear system Γ is defined as $\bigcap_{D\in\Gamma} \operatorname{Supp} D$.
- For any linear system $\Gamma \subset \operatorname{Div} \mathcal{X}$ and $\mathcal{Y} \subset \mathcal{X}$ a subvariety, we denote by $\Gamma - \mathcal{Y}$ the maximal linear subsystem of Γ of elements whose base locus contains $\mathcal{Y}$.

Definition: $\mathcal{P}$–interpolating linear system — Couvreur, Perret, Lebacque (2020)

Given $\mathcal{P} \subseteq \mathcal{X}(\mathbb{F}_q)$, a linear system Γ of divisors on $\mathcal{X}$ is said to be $\mathcal{P}$–interpolating if

1. $\Gamma - \mathcal{P}$ is non empty;
2. the base locus of $\Gamma - \mathcal{P}$ has dimension 0.

Lower bound for the minimum distance: $\mathcal{P}$–interpolating linear system

Definition: Linear system

- A *linear system* is a family of linearly equivalent effective divisors.
- The *base locus* of a linear system Γ is defined as $\bigcap_{D\in\Gamma} \operatorname{Supp} D$.
- For any linear system $\Gamma \subset \operatorname{Div}\mathcal{X}$ and $\mathcal{Y} \subset \mathcal{X}$ a subvariety, we denote by $\Gamma - \mathcal{Y}$ the maximal linear subsystem of Γ of elements whose base locus contains $\mathcal{Y}$.

Definition: $\mathcal{P}$–interpolating linear system — Couvreur, Perret, Lebacque (2020)

Given $\mathcal{P} \subseteq \mathcal{X}(\mathbb{F}_q)$, a linear system Γ of divisors on $\mathcal{X}$ is said to be $\mathcal{P}$–interpolating if

❶ $\Gamma - \mathcal{P}$ is non empty; ❷ the base locus of $\Gamma - \mathcal{P}$ has dimension 0.

Proposition — Couvreur, Perret, Lebacque (2020)

- The minimum distance d of $C(\mathcal{X}, \mathcal{P}, G)$ satisfies $d \geq n - \Gamma \cdot G$.
- If H is very ample, then the complete linear system $|(q+1)H|$ is $\mathcal{P}$–interpolating.

└ The map $\phi_H : \mathcal{X} \dashrightarrow \mathbb{P}^{\ell(H)-1}$ is an embedding.

Comparison between $\mathcal{P}$–covering curves and $\mathcal{P}$–interpolating linear system

	Curves $C_1, \dots, C_r$ on $\mathcal{X}$ s.t. ❶ $\mathcal{P} \subseteq \bigcup_i \mathcal{C}_i(\mathbb{F}_q)$; ❷ $G \cdot \mathcal{C}_i \geq 0$. Set $\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq \mathcal{Z}(f)\}$.	Linear system Γ s.t. ❶ $\Gamma - \mathcal{P}$ is non empty; ❷ the base locus of $\Gamma - \mathcal{P}$ has dim. 0.
Lower bound for d	$d \geq n - \sum_{i=1}^{r} G \cdot \mathcal{C}_i - \ell \max \#\mathcal{C}_i(\mathbb{F}_q)$	$d \geq n - G \cdot \Gamma$

Comparison between $\mathcal{P}$–covering curves and $\mathcal{P}$–interpolating linear system

	Curves $C_1, \dots, C_r$ on $\mathcal{X}$ s.t.	Linear system Γ s.t.
Definition	❶ $\mathcal{P} \subseteq \bigcup_i \mathcal{C}_i(\mathbb{F}_q)$; ❷ $G \cdot \mathcal{C}_i \geq 0$. Set $\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq \mathcal{Z}(f)\}$.	❶ $\Gamma - \mathcal{P}$ is non empty; ❷ the base locus of $\Gamma - \mathcal{P}$ has dim. 0.
Lower bound for d	$d \geq n - \sum_{i=1}^{r} G \cdot \mathcal{C}_i - \ell \max \#\mathcal{C}_i(\mathbb{F}_q)$ 👍 Better bound	$d \geq n - G \cdot \Gamma$
Relation	$\Gamma = \Gamma - \mathcal{P} = \left\{ \sum_{i=1}^{r} \mathcal{C}_i \right\}$	$A = \sum n_i \mathcal{C}_i \in \Gamma$ with $n_i \geq 0$.
Similarities	❶ $\Rightarrow$ ❶	$A \in \Gamma - \mathcal{P}$ (exists by ❶) satisfies ❶.
Differences	❷ $\Rightarrow$ $\#(\Gamma - \mathcal{P}) \geq 2$.	

Comparison between $\mathcal{P}$–covering curves and $\mathcal{P}$–interpolating linear system

	Curves $C_1, \dots, C_r$ on $\mathcal{X}$ s.t.	Linear system Γ s.t.
Definition	❶ $\mathcal{P} \subseteq \bigcup_i \mathcal{C}_i(\mathbb{F}_q)$; ❷ $G \cdot \mathcal{C}_i \geq 0$. Set $\ell = \max_{f \in L(G)} \#\{i \mid \mathcal{C}_i \subseteq \mathcal{Z}(f)\}$.	❶ $\Gamma - \mathcal{P}$ is non empty; ❷ the base locus of $\Gamma - \mathcal{P}$ has dim. 0.
Lower bound for d	$d \geq n - \sum_{i=1}^{r} G \cdot \mathcal{C}_i - \ell \max \#\mathcal{C}_i(\mathbb{F}_q)$ 👍 Better bound	$d \geq n - G \cdot \Gamma$
Relation	$\Gamma = \Gamma - \mathcal{P} = \left\{ \sum_{i=1}^{r} \mathcal{C}_i \right\}$	$A = \sum n_i \mathcal{C}_i \in \Gamma$ with $n_i \geq 0$.
Similarities	❶ $\Rightarrow$ ❶	$A \in \Gamma - \mathcal{P}$ (exists by ❶) satisfies ❶.
Differences	❷ $\Rightarrow$ $\#(\Gamma - \mathcal{P}) \geq 2$.	
Behaviour under morphisms	If $\pi : \mathcal{X}' \to \mathcal{X}$ and $\mathcal{P}' \subseteq \pi^{-1}(\mathcal{P})$ 👍 $\pi^*(\mathcal{C}_i)$ are $\mathcal{P}'$–covering, 👎 Few control over the analogue of ℓ.	👍 $\pi^*(\Gamma)$ is $\mathcal{P}'$–interpolating.

Paving the ground towards codes from towers of surfaces — Couvreur, Lebacque, Perret (2020)

AG codes from curves are well–known for having better parameters than random codes asymptotically for q square and $q \geq 49$. Ihara (1981), Tsfasman, Vlăduț, Zink (1982)

Paving the ground towards codes from towers of surfaces — Couvreur, Lebacque, Perret (2020)

AG codes from curves are well–known for having better parameters than random codes asymptotically for q square and $q \geq 49$. Ihara (1981), Tsfasman, Vlăduț, Zink (1982)

Constructions of *asymptotically good codes* are based on **tower of curves**:

1. modular curves Ihara (1981), Tsfasman, Vlăduț, Zink (1982),
2. recursive towers Garcia, Stichtenoth (1995)...,
3. class field theory.

Paving the ground towards codes from towers of surfaces — Couvreur, Lebacque, Perret (2020)

AG codes from curves are well–known for having better parameters than random codes asymptotically for q square and $q \geq 49$. Ihara (1981), Tsfasman, Vlăduț, Zink (1982)

Constructions of *asymptotically good codes* are based on **tower of curves**:

1. modular curves Ihara (1981), Tsfasman, Vlăduț, Zink (1982),
2. recursive towers Garcia, Stichtenoth (1995)...,
3. class field theory.

In the context of curves, the key is to control $\#\mathcal{X}(\mathbb{F}_q)/g(\mathcal{X})$.

Working with **towers of surfaces**, we may get longer codes.
But several invariants come into play (e.g. $K_{\mathcal{X}}^2$ and $\deg c_2(\mathcal{X})$ or $\chi(\mathcal{O}_{\mathcal{X}})$).

$\rightarrow$ Criterion for a surface to admit an infinite tower of étale covers where a finite set of points of the surface splits completely.

Table of Contents

Actually using algebraic geometry codes

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

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

Actually using algebraic geometry codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ for practical applications, 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 (ideals in function fields)
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method (Brill–Noether's theory)
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–Couvreur–Lecerf (2020),...

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

2. **decode**

Actually using algebraic geometry codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ for practical applications, 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 (ideals in function fields)
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method (Brill–Noether's theory)
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–Couvreur–Lecerf (2020),...

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

   On **surfaces**: 👎 no generic method to compute Riemann–Roch spaces,
   👍 families of varieties with explicit bases of Riemann–Roch spaces.

2. **decode**

Actually using algebraic geometry codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ for practical applications, 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 (ideals in function fields)
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method (Brill–Noether's theory)
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–Couvreur–Lecerf (2020),...

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

   On **surfaces**: 👎 no generic method to compute Riemann–Roch spaces,
   👍 families of varieties with explicit bases of Riemann–Roch spaces.

2. **decode**

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

Actually using algebraic geometry codes

To use an AG code $C(\mathcal{X}, \mathcal{P}, G)$ for practical applications, 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 (ideals in function fields)
     Hensel–Landberg (1902), Coated (1970), Davenport (1981), Hess (2001)...
   - Geometric method (Brill–Noether's theory)
     Goppa, Le Brigand–Risler (80's), Huang–Ierardi (90's), Khuri–Makdisi (2007), Le Gluher–Spaenlehauer (2018), Abelard–Couvreur–Lecerf (2020),...

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

   On **surfaces**: 👎 no generic method to compute Riemann–Roch spaces,
   👍 families of varieties with explicit bases of Riemann–Roch spaces.

2. **decode**

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

   On **surfaces**: 👎 no generic global decoding algorithm,
   👍 natural local decoding.

Some varieties with explicit bases of Riemann–Roch spaces: toric varieties

Toric varieties come with a handy combinatorial description.

An integral polytope $P \subset \mathbb{R}^N$ (vertices in $\mathbb{Z}^N$) defines a N-dimensional polarized toric variety $\mathcal{X}_P$, *i.e.* with a divisor G and a monomial basis of $L(G)$ (set of polynomials of a certain *degree*).

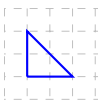
Some varieties with explicit bases of Riemann–Roch spaces: toric varieties

Toric varieties come with a handy combinatorial description.

An integral polytope $P \subset \mathbb{R}^N$ (vertices in $\mathbb{Z}^N$) defines a N-dimensional polarized toric variety $\mathcal{X}_P$, *i.e.* with a divisor G and a monomial basis of $L(G)$ (set of polynomials of a certain *degree*).

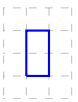
$$L(G) \simeq \mathsf{Span}\{\boldsymbol{x}^m, m \in P \cap \mathbb{Z}^N\}.$$

Size of $P \leftrightarrow$ *Degree* in $L(G)$



$\mathbb{P}^2$

Degree 2



$\mathbb{P}^1 \times \mathbb{P}^1$

Degree $(1, 2)$

$\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$

Degree $(4, 3, 3)$

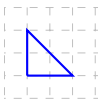
Some varieties with explicit bases of Riemann–Roch spaces: toric varieties

Toric varieties come with a handy combinatorial description.

An integral polytope $P \subset \mathbb{R}^N$ (vertices in $\mathbb{Z}^N$) defines a N-dimensional polarized toric variety $\mathcal{X}_P$, *i.e.* with a divisor G and a monomial basis of $L(G)$ (set of polynomials of a certain *degree*).

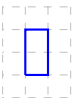
$$L(G) \simeq \mathsf{Span}\{\boldsymbol{x}^m, m \in P \cap \mathbb{Z}^N\}.$$

Size of $P \leftrightarrow$ *Degree* in $L(G)$



$\mathbb{P}^2$

Degree 2



$\mathbb{P}^1 \times \mathbb{P}^1$

Degree $(1,2)$

$\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$

Degree $(4,3,3)$

Why **toric**?

$\mathcal{X}_P$ contains a dense torus $\mathbb{T}_P \simeq \left(\overline{\mathbb{F}_q}^*\right)^N$ whose rational points are $\mathbb{T}_P(\mathbb{F}_q) \simeq (\mathbb{F}_q^*)^N$.

Toric code: $C(\mathcal{X}_P, \mathbb{T}_P(\mathbb{F}_q), G)$ (generalization of Reed–Muller codes)

Hansen (2002), Little-Schwarz (2005), Ruano (2007), Soprunov-Soprunova (2009),...

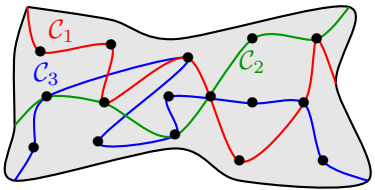
Projective toric code: $C(\mathcal{X}_P, \mathcal{X}_P(\mathbb{F}_q), G)$. (generalization of *projective* Reed–Muller codes)

Carvalho, Neumann (2014), N. (2020)...

Globally decoding via local decoding — Voloch, Zarzar (2011)

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

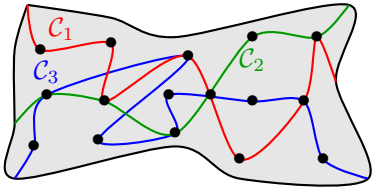
- $\mathcal{P} \subseteq \bigcup \mathcal{C}_i(\mathbb{F}_q)$ ($\mathcal{P}$–covering),
- $\boldsymbol{c} \in C \Leftrightarrow \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in C_{|\mathcal{C}_i}$. ← $C(\mathcal{C}_i, \mathcal{P} \cap \mathcal{C}_i, G \cap \mathcal{C}_i)$
  The restrictions to the curves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



Globally decoding via local decoding — Voloch, Zarzar (2011)

Consider an AG code $C = C(\mathcal{X}, \mathcal{P}, G)$ on $\mathcal{X}$.
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),
- $\boldsymbol{c} \in C \Leftrightarrow \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in C_{|\mathcal{C}_i}$. $\longleftarrow C(\mathcal{C}_i, \mathcal{P} \cap \mathcal{C}_i, G \cap \mathcal{C}_i)$
  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 $\mathbb{P}^3$;
- 👎 May fail if too many errors gather on one curve;
- 👎 Characterizing codes from restrictions may not be possible.

Table of Contents

Locality

Definition: Locally recoverable code

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

Locality

Definition: Locally recoverable code

A code C is said to be locally recoverable (LR) with locality ℓ if, for each $i \in \{1, \ldots, n\}$, there is a subset $J_i \subseteq \{1, \ldots, n\} \setminus \{i\}$, $\#J_i = \ell$ (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 LRC C with parameters $[n, k, d]$ and locality ℓ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

Locality

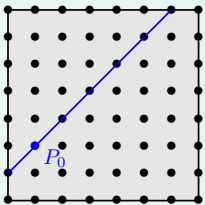
Definition: Locally recoverable code

A code C is said to be locally recoverable (LR) with locality ℓ 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 LRC C with parameters $[n, k, d]$ and locality ℓ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

Reed–Muller codes are locally recoverable of locality $\ell = q - 1$.



$$\mathrm{RM}(2, r) = \left\{ (f(P_1), f(P_2), \dots, f(P_{q^2})) \mid f \in \mathbb{F}_q[X, Y]_{\leq r} \right\}.$$

To recover the coordinate associated to a point P_0 in a word $\boldsymbol{c}$:

Locality

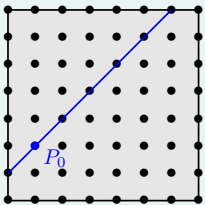
Definition: Locally recoverable code

A code C is said to be locally recoverable (LR) with locality ℓ 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 LRC C with parameters $[n, k, d]$ and locality ℓ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

Reed–Muller codes are locally recoverable of locality $\ell = q - 1$.



$$\mathrm{RM}(2, r) = \left\{ (f(P_1), f(P_2), \dots, f(P_{q^2})) \mid f \in \mathbb{F}_q[X, Y]_{\leq r} \right\}.$$

To recover the coordinate associated to a point P_0 in a word $\boldsymbol{c}$:

- Pick a $\mathbb{F}_q$–line L containing P_0 $(x = \alpha t + \beta, y = \gamma t + \delta)$,

Locality

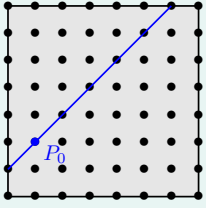
Definition: Locally recoverable code

A code C is said to be locally recoverable (LR) with locality ℓ 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 LRC C with parameters $[n, k, d]$ and locality ℓ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

Reed–Muller codes are locally recoverable of locality $\ell = q - 1$.



$$\mathrm{RM}(2, r) = \left\{ (f(P_1), f(P_2), \dots, f(P_{q^2})) \mid f \in \mathbb{F}_q[X, Y]_{\leq r} \right\}.$$

To recover the coordinate associated to a point P_0 in a word $\boldsymbol{c}$:

- Pick a $\mathbb{F}_q$–line L containing P_0 $(x = \alpha t + \beta, y = \gamma t + \delta)$,

$\Rightarrow$ $\mathrm{RM}(2, r)_{|L} = \{(f(t))_{t \in \mathbb{F}_q} \mid f \in \mathbb{F}_q[T]_{\leq r}\} = \mathrm{RS}_{r+1}(\mathbb{F}_q)$.

Locality

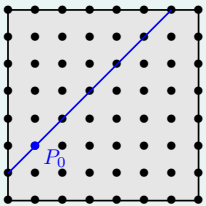
Definition: Locally recoverable code

A code C is said to be locally recoverable (LR) with locality ℓ 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 LRC C with parameters $[n, k, d]$ and locality ℓ satisfies $d \leq n - k - \left\lceil \frac{k}{\ell} \right\rceil + 2$.

Reed–Muller codes are locally recoverable of locality $\ell = q - 1$.



$$\mathrm{RM}(2, r) = \left\{ (f(P_1), f(P_2), \dots, f(P_{q^2})) \mid f \in \mathbb{F}_q[X, Y]_{\leq r} \right\}.$$

To recover the coordinate associated to a point P_0 in a word $\boldsymbol{c}$:

- Pick a $\mathbb{F}_q$–line L containing P_0 $(x = \alpha t + \beta, y = \gamma t + \delta)$,

$\Rightarrow$ $\mathrm{RM}(2, r)_{|L} = \{(f(t))_{t \in \mathbb{F}_q} \mid f \in \mathbb{F}_q[T]_{\leq r}\} = \mathsf{RS}_{r+1}(\mathbb{F}_q)$.

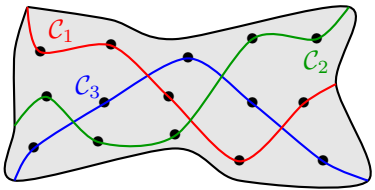
- Recover using the correction algorithm of Reed–Solomon codes.

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 ℓ, **provided that** we know how to correct in the codes $C_{|\mathcal{C}_i}$.



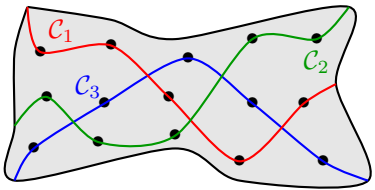
In most constructions, $\mathcal{C}_i \simeq \mathcal{C}_j$ and the restricted codes are equivalent (e.g. $G \cap \mathcal{C}_i \simeq G \cap \mathcal{C}_j$).

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 ℓ, **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

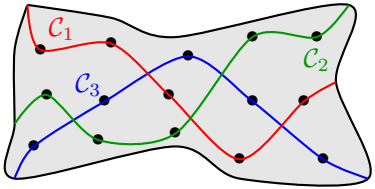
$$\{\boldsymbol{c} \in C(\mathcal{X}, \mathcal{P}, G) \mid \forall i,\ \boldsymbol{c}_{|\mathcal{C}_i} \in \phi_i(C')\}.$$

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 ℓ, **provided that** we know how to correct in the codes $C_{|\mathcal{C}_i}$.

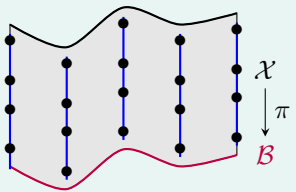


In most constructions, $\mathcal{C}_i \simeq \mathcal{C}_j$ and the restricted codes are equivalent (e.g. $G \cap \mathcal{C}_i \simeq G \cap \mathcal{C}_j$).

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

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

LRC on ruled surfaces — Salgado, Varilly-Alvarado, Voloch (2021)



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

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

Take–away

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

- we can constructed longer codes from small alphabets,
- their *richer geometry* compared to curves grants them with natural local properties which can be useful in applications (*e.g.* distributed storage),
- we have many ingredients to design new families of asymptotically good codes.

Take–away

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

- we can constructed longer codes from small alphabets,
- their *richer geometry* compared to curves grants them with natural local properties which can be useful in applications (*e.g.* distributed storage),
- we have many ingredients to design new families of asymptotically good codes.

But for the moment

- we lack generic algorithms to encode and decode,
- we have to explore families of surfaces with the right features to get the expected properties on codes,
- we need a better understanding of the classification of surfaces over finite fields.

Take–away

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

- we can constructed longer codes from small alphabets,
- their *richer geometry* compared to curves grants them with natural local properties which can be useful in applications (*e.g.* distributed storage),
- we have many ingredients to design new families of asymptotically good codes.

But for the moment

- we lack generic algorithms to encode and decode,
- we have to explore families of surfaces with the right features to get the expected properties on codes,
- we need a better understanding of the classification of surfaces over finite fields.

Thank you for your attention!