A bound for the number of $\mathbb{F}_q$ points on a curve embedded in the biprojective space

Jade NARDI

Tuesday 13 March

Member of the **Manta** project, which members are working at INRIA Saclay–Île-de-France, Télécom ParisTech and Mathematics institute of Toulouse. The geometry team of this project studies new research directions in algebraic geometry and coding theory, e.g. codes built over higher dimensional varieties.

Aim of error-correcting codes: Improve/Preserve the quality of data transmission through space (e.g. telephone networks, satellite communication) and time (e.g. magnetic tape, flash drive).

Aim of error-correcting codes: Improve/Preserve the quality of data transmission through space (e.g. telephone networks, satellite communication) and time (e.g. magnetic tape, flash drive).

A message m is sent through a noisy channel. It may be altered but we want receivers to be able to *check consistency of the delivered message*, and perhaps to *recover data* that has been determined to be corrupted.
General idea: Add some **redundancy** to a message.

Example 1: French social security system - personal number

2	93	01	13	155	363	83
Sex	Birth year	Month	Depart.	Town	Rank	Key

Example 1: French social security system - personal number

2	93	01	13	155	363	83
Sex	Birth year	Month	Depart.	Town	Rank	Key

Key $\equiv -N\ [97]$ where N is the number formed by the 13 first digits.

Example 1: French social security system - personal number

2	93	01	13	155	363	83
Sex	Birth year	Month	Depart.	Town	Rank	Key

Key $\equiv -N$ $[97]$ where N is the number formed by the 13 first digits.
If there is one error, let's say $2\,93\,01\,1\mathbf{5}\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ and $68 + 83 \not\equiv 0$ $[97]$
Short key + / - Cannot correct

Example 1: French social security system - personal number

2	93	01	13	155	363	83
Sex	Birth year	Month	Depart.	Town	Rank	Key

Key $\equiv -N$ $[97]$ where N is the number formed by the 13 first digits.
If there is one error, let's say $2\,93\,01\,1\mathbf{5}\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ and $68 + 83 \not\equiv 0$ $[97]$
Short key + / - Cannot correct

Example 2: Send three times in a row
I want to send 001. I send $m = 001001001$.

Example 1: French social security system - personal number

2	93	01	13	155	363	83
Sex	Birth year	Month	Depart.	Town	Rank	Key

Key $\equiv -N$ $[97]$ where N is the number formed by the 13 first digits.
If there is one error, let's say $2\,93\,01\,1\mathbf{5}\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ and $68 + 83 \not\equiv 0$ $[97]$
Short key + / - Cannot correct

Example 2: Send three times in a row
I want to send 001. I send $m = 001001001$.
If there is one error and $\tilde{m} = 001\mathbf{1}01001$ is received, it can be recovered.

Example 1: French social security system - personal number

2	93	01	13	155	363	83
Sex	Birth year	Month	Depart.	Town	Rank	Key

Key $\equiv -N\ [97]$ where N is the number formed by the 13 first digits.
If there is one error, let's say $2\,93\,01\,1\mathbf{5}\,155\,363\,83$
$N' = 2930115155363 = 30207372735 \times 97 + 68$ and $68 + 83 \not\equiv 0\ [97]$
Short key + / - Cannot correct

Example 2: Send three times in a row
I want to send 001. I send $m = 001001001$.
If there is one error and $\tilde{m} = 001\mathbf{1}01001$ is received, it can be recovered.
If there are more than two errors, the message cannot be recovered any more. If $\tilde{m} = \mathbf{1}01\mathbf{1}01\mathbf{0}01$, m or 101101101 ?
Correct one error + / - Message length

Définition

A *linear code* C on $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$ of dimension k.

Définition

A *linear code* C on $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$ of dimension k.
Let $x \in C$ be a codeword. Its weight is defined by

$$\omega(x) = \#\{i \in \{1, \ldots, n\},\ x_i \neq 0\}$$

Définition

A *linear code* C on $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$ of dimension k.
Let $x \in C$ be a codeword. Its weight is defined by

$$\omega(x) = \#\{i \in \{1, \dots, n\},\ x_i \neq 0\}$$

Let x, $y \in C$. The *Hamming distance* between x and y is defined by

$$d(x, y) = \#\{i \in \{1, \dots, n\},\ x_i \neq y_i\}$$

Définition

A *linear code* C on $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$ of dimension k.
Let $x \in C$ be a codeword. Its weight is defined by

$$\omega(x) = \#\{i \in \{1, \ldots, n\},\ x_i \neq 0\}$$

Let $x,\ y \in C$. The *Hamming distance* between x and y is defined by

$$d(x,y) = \#\{i \in \{1, \ldots, n\},\ x_i \neq y_i\} = \omega(x-y)$$

Définition

A *linear code* C on $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$ of dimension k.
Let $x \in C$ be a codeword. Its weight is defined by

$$\omega(x) = \#\{i \in \{1, \ldots, n\},\ x_i \neq 0\}$$

Let $x,\ y \in C$. The *Hamming distance* between x and y is defined by

$$d(x, y) = \#\{i \in \{1, \ldots, n\},\ x_i \neq y_i\} = \omega(x - y)$$

The *minimum distance* of the code C is defined by

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\}$$

Définition

A *linear code* C on $\mathbb{F}_q$ of length n is a vector subspace $\mathbb{F}_q^n$ of dimension k.
Let $x \in C$ be a codeword. Its weight is defined by

$$\omega(x) = \#\{i \in \{1, \ldots, n\},\ x_i \neq 0\}$$

Let $x,\ y \in C$. The *Hamming distance* between x and y is defined by

$$d(x, y) = \#\{i \in \{1, \ldots, n\},\ x_i \neq y_i\} = \omega(x - y)$$

The *minimum distance* of the code C is defined by

$$d(C) = \min\{d(x, y) \mid x, y \in C,\ x \neq y\} = \min_{x \in C} \omega(x)$$

A linear code of length n, dimension k and minimum distance d is called a $[n, k, d]$-code.

Transmission rate: $\kappa = \frac{k}{n}$
Relative distance: $\delta = \frac{d}{n}$
We want both κ and δ big, this is not to much redundancy and a good correcting capacity. But you can't have the best of both worlds...

Transmission rate: $\kappa = \frac{k}{n}$
Relative distance: $\delta = \frac{d}{n}$
We want both κ and δ big, this is not to much redundancy and a good correcting capacity. But you can't have the best of both worlds...

Singleton bound : $\delta + \kappa \leq 1 + \frac{1}{n}$.

Transmission rate: $\kappa = \frac{k}{n}$
Relative distance: $\delta = \frac{d}{n}$
We want both κ and δ big, this is not to much redundancy and a good correcting capacity. But you can't have the best of both worlds...

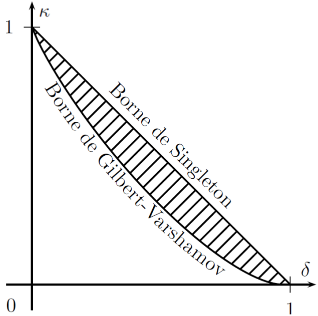
Singleton bound : $\delta + \kappa \leq 1 + \frac{1}{n}$.

Gilbert-Varshamov bound : Fix q. When $n \to +\infty$,
$\sup_{C\ q-\text{ary}} \{\kappa(C) \mid \delta(C) = \delta\} \geq 1 - H_q(\delta)$ where
$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$.

Transmission rate: $\kappa = \frac{k}{n}$
Relative distance: $\delta = \frac{d}{n}$
We want both κ and δ big, this is not to much redundancy and a good correcting capacity. But you can't have the best of both worlds...

Singleton bound : $\delta + \kappa \leq 1 + \frac{1}{n}$.

Gilbert-Varshamov bound : Fix q. When $n \to +\infty$,
$\sup_{C\ q-\text{ary}} \{\kappa(C) \mid \delta(C) = \delta\} \geq 1 - H_q(\delta)$ where
$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta)$.



Best codes are known to be **algebraic geometric codes**. Among them, let us focus on projective Reed-Muller codes.

Best codes are known to be **algebraic geometric codes**. Among them, let us focus on projective Reed-Muller codes.

On $\mathbb{P}^r$, fix a degree s. Take $\mathcal{F} \subset \mathbb{F}_q[X_0, X_1, \dots, X_r]$ a vector subspace of homogeneous polynomial of degree s. Fix a set of n points $\mathbb{F}_q$-rationnels $\mathcal{P} = \{P_1, \dots, P_n\} \subset \mathbb{P}^r(\mathbb{F}_q)$,

Given $f \in \mathcal{F}$ and P a point of $\mathbb{P}^r$, we define the evaluation of f at P as $f(P) := f(p_0, \dots, p_r)$, where $(p_0 : \dots : p_r)$ is the system of homogeneous coordinates of P such that the first nonzero coordinate starting from the left is set to 1, i.e. is of the form $(0 : \dots : 0 : 1 : p_i : \dots : p_n)$.

Best codes are known to be **algebraic geometric codes**. Among them, let us focus on projective Reed-Muller codes.

On $\mathbb{P}^r$, fix a degree s. Take $\mathcal{F} \subset \mathbb{F}_q[X_0, X_1, \dots, X_r]$ a vector subspace of homogeneous polynomial of degree s. Fix a set of n points $\mathbb{F}_q$-rationnels $\mathcal{P} = \{P_1, \dots, P_n\} \subset \mathbb{P}^r(\mathbb{F}_q)$,

Given $f \in \mathcal{F}$ and P a point of $\mathbb{P}^r$, we define the evaluation of f at P as $f(P) := f(p_0, \dots, p_r)$, where $(p_0 : \cdots : p_r)$ is the system of homogeneous coordinates of P such that the first nonzero coordinate starting from the left is set to 1, i.e. is of the form $(0 : \cdots : 0 : 1 : p_i : \cdots : p_n)$.
We can define a linear code as the range of the map

$$\mathrm{ev}_s : \left\{ \begin{array}{ccc} \mathcal{F} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \dots, f(P_n)) \end{array} \right.$$

Its length is n. Its dimension is the one of the quotient $\mathcal{F}/\ker \mathrm{ev}_s$.
Assume $\mathcal{P} = \mathbb{P}^r(\mathbb{F}_q)$. Take a codeword $\mathrm{ev}_s(f)$ and consider the hypersurface H_f defined by $f = 0$. Then

$$\omega(\mathrm{ev}_s(f)) = n - \#H_f(\mathbb{F}_q)$$

Then lowerbounding the minimum distance is equivalent to upperbound the number of $\mathbb{F}_q$-points of such hypersurfaces.

Theorem [K. Stöhr, F. Voloch]

Let $f \in \mathbb{F}_q[x,y]$ be an absolutely irreducible polynomial of degree $d \geq 2$ with coefficients in $\mathbb{F}_q$ (characteristic not 2) and denote by $\mathcal{C}$ the curve in $\mathbb{A}^2$ defined by $f = 0$. Then

$$\#\mathcal{C}(\mathbb{F}_q) \leq \frac{1}{2} d(d+q-1)$$

if at least one of the points of $\mathcal{C}$ is not an inflection point.

Idea of the proof: Consider the polynomial $h \in \mathbb{F}_q[x,y]$ defined by

$$h(x,y) = (x^q - x)f_x + (y^q - q)f_y$$

of degree $d+q-1$ and $\mathcal{H}$ the curve defined by $h = 0$.

$$\mathcal{H} \cap \mathcal{C} = \{P \in \mathcal{C} \mid \Phi(P) \in T_P\mathcal{C}\}$$

If $\mathcal{H}$ and $\mathcal{C}$ have no commun components, Bezout's Theorem gives

$$\sum_{P \in \mathcal{C} \cap \mathcal{H}} i(P;\mathcal{H},\mathcal{C}) \leq \deg f \times \deg h$$

We can prove that for any $\mathbb{F}_q$-point $P \in \mathcal{C}(\mathbb{F}_q)$ on $\mathcal{C}$, $i(P,\mathcal{H} \cap \mathcal{C}) \geq 2$.
It is true if P is singular. If P is a regular point on $\mathcal{C}$, it is enough to check that $\mathcal{H}$ and $\mathcal{C}$ have the same tangent line at P. Then

$$2\#C(\mathbb{F}_q) \leq d(d-1+q).$$

Proposition

Let $F \in \mathbb{F}_q[X_0, X_1, X_2]$ be an absolutely irreducible homogeneous polynomial of degree $d \geq 2$ with coefficients in $\mathbb{F}_q$ (characteristic not 2) and denote by $\mathcal{C}$ the curve in $\mathbb{P}^2(k)$ defined by $F = 0$. Then

$$\mathcal{C}(\mathbb{F}_q) \leq \frac{1}{2}d(d+q-1)$$

if there exists a point of $\mathcal{C}$ that is not an inflection point.

Proposition

Let $F \in \mathbb{F}_q[X_0, X_1, X_2]$ be an absolutely irreducible homogeneous polynomial of degree $d \geq 2$ with coefficients in $\mathbb{F}_q$ (characteristic not 2) and denote by $\mathcal{C}$ the curve in $\mathbb{P}^2(k)$ defined by $F = 0$. Then

$$\mathcal{C}(\mathbb{F}_q) \leq \frac{1}{2} d(d + q - 1)$$

if there exists a point of $\mathcal{C}$ that is not an inflection point.

Idea of the proof: Consider the polynomial $H \in \mathbb{F}_q[X_0, X_1, X_2]$ defined by

$$H = X_0^q F_{X_0} + X_1^q F_{X_1} + X_2^q F_{X_2}$$

and $\mathcal{H}$ the curve defined by $H = 0$. Using Euler Identity

$$dF = X_0 F_{X_0} + X_1 F_{X_1} + X_2 F_{X_2},$$

we can see that on each affine chart $(x_i \neq 0)$, we are back to study the intersection of f and $h(x, y) = (x^q - x) f_x + (y^q - q) f_y$.

Proposition

Let $F \in \mathbb{F}_q[X_0, X_1, Y_0, Y_1]$ be a absolutely irreducible bihomogeneous polynomial of bidegree (δ_X, δ_Y) with coefficients in the finite field $\mathbb{F}_q$ of characteristic different from 2.
Assume $\delta_X,\ \delta_Y \geq 1$.
Let $\mathcal{C}$ be the curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined by $F = 0$. Then

$$\#\mathcal{C}(\mathbb{F}_q) \leq \delta_X \delta_Y + \frac{q+1}{2}(\delta_X + \delta_Y).$$

Proposition

Let $F \in \mathbb{F}_q[X_0, X_1, Y_0, Y_1]$ be a absolutely irreducible bihomogeneous polynomial of bidegree (δ_X, δ_Y) with coefficients in the finite field $\mathbb{F}_q$ of characteristic different from 2. Assume $\delta_X,\ \delta_Y \geq 1$.
Let $\mathcal{C}$ be the curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined by $F = 0$. Then

$$\#\mathcal{C}(\mathbb{F}_q) \leq \delta_X \delta_Y + \frac{q+1}{2}(\delta_X + \delta_Y).$$

Recall: Let $\mathcal{C}$ and $\mathcal{D}$ be two curves in $\mathbb{P}^1 \times \mathbb{P}^1$ of bidegree (δ_X, δ_Y) and (δ'_X, δ'_Y). If they have no common component, the number of intersection points, counted with multiplicity, is equal to

$$\mathcal{C} \cdot \mathcal{D} = \delta_X \delta'_Y + \delta'_X \delta_Y$$

The main idea is to *homogenize* the polynomial

$$h(x,y) = (x^q - x)f_x + (y^q - q)f_y.$$

It seems to be possible to generalize this idea to a family of surfaces, **toric surfaces**. $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ are toric surfaces.

Toric surfaces are naturally endowed with a graded coordinate ring of polynomials and Euler identities, two essential ingredients in this method.

The main idea is to *homogenize* the polynomial

$$h(x, y) = (x^q - x)f_x + (y^q - q)f_y.$$

It seems to be possible to generalize this idea to a family of surfaces, **toric surfaces**. $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ are toric surfaces.

Toric surfaces are naturally endowed with a graded coordinate ring of polynomials and Euler identities, two essential ingredients in this method.

Thank you for your attention !