Algebraic Geometric Codes on Hirzebruch surfaces

Jade Nardi

Institute of Mathematics of Toulouse

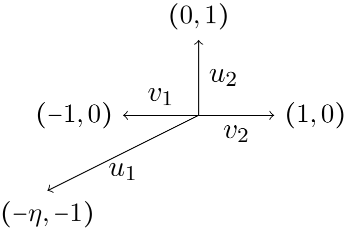
SIAM Conference on Applied Algebraic Geometry - 12/07/2019

MS185: Algebraic Geometry Codes

Definition

Let $\eta \in \mathbb{N}$. Definition of the Hirzebruch surface $\mathcal{H}_\eta$:

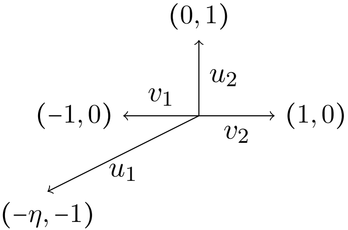
- **Toric point of view** - Toric variety associated to the fan



Definition

Let $\eta \in \mathbb{N}$. Definition of the Hirzebruch surface $\mathcal{H}_\eta$:

- **Toric point of view** - Toric variety associated to the fan



- **Quotient point of view**
  $\mathbb{G}_m \times \mathbb{G}_m$ acts on $\left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right)$ as follows.

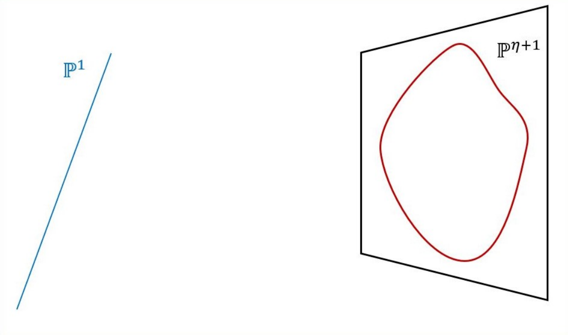
$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

$$\mathcal{H}_\eta := \left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) \times \left(\mathbb{A}^2 \smallsetminus \{(0,0)\}\right) / \mathbb{G}_m^2.$$

Example: $\mathcal{H}_0 = \mathbb{P}^1 \times \mathbb{P}^1$.

Embedded in $\mathbb{P}^{\eta+3}$ as a rational scroll

Rational curve: $\begin{cases} \mathbb{P}^1 & \to & \mathcal{C}_{\eta+1} \subset \mathbb{P}^{\eta+1} \\ [u,v] & \mapsto & [u^i v^{\eta+1-i}]_{i\in\{0,\dots,\eta+1\}} \end{cases}$

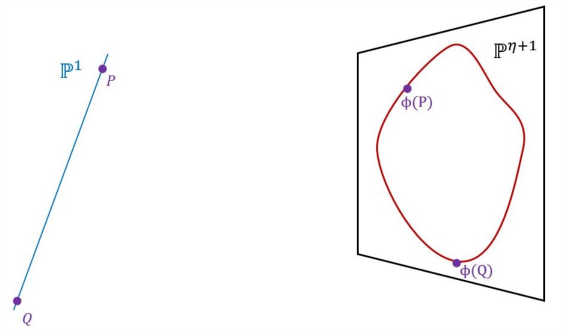


$$\#\mathcal{H}_\eta(\mathbb{F}_q) = (q+1)^2$$

Embedded in $\mathbb{P}^{\eta+3}$ as a rational scroll

Rational curve: $\begin{cases} \mathbb{P}^1 & \to & \mathcal{C}_{\eta+1} \subset \mathbb{P}^{\eta+1} \\ [u,v] & \mapsto & [u^i v^{\eta+1-i}]_{i\in\{0,\dots,\eta+1\}} \end{cases}$

Take an isomophism $\phi : \mathbb{P}^1 \to \mathcal{C}_{\eta+1}$.

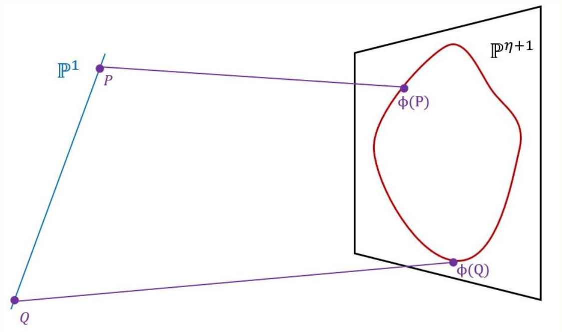


$$\#\mathcal{H}_\eta(\mathbb{F}_q) = (q+1)^2$$

Embedded in $\mathbb{P}^{\eta+3}$ as a rational scroll

Rational curve: $\begin{cases} \mathbb{P}^1 & \to & \mathcal{C}_{\eta+1} \subset \mathbb{P}^{\eta+1} \\ [u,v] & \mapsto & [u^i v^{\eta+1-i}]_{i\in\{0,\dots,\eta+1\}} \end{cases}$

Take an isomophism $\phi : \mathbb{P}^1 \to \mathcal{C}_{\eta+1}$.

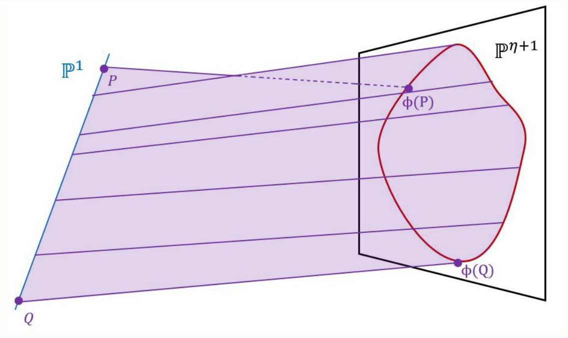


$$\#\mathcal{H}_\eta(\mathbb{F}_q) = (q+1)^2$$

Embedded in $\mathbb{P}^{\eta+3}$ as a rational scroll

Rational curve: $\begin{cases} \mathbb{P}^1 & \to & \mathcal{C}_{\eta+1} \subset \mathbb{P}^{\eta+1} \\ [u,v] & \mapsto & [u^i v^{\eta+1-i}]_{i\in\{0,\dots,\eta+1\}} \end{cases}$

Take an isomophism $\phi : \mathbb{P}^1 \to \mathcal{C}_{\eta+1}$.



$$\#\mathcal{H}_\eta(\mathbb{F}_q) = (q+1)^2$$

Coordinate ring of $\mathcal{H}_\eta$: Cox Ring

Polynomial coordinate ring of $\mathcal{H}_\eta$ over $\mathbb{F}_q$: $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
Endowed with a **graduation** inherited from the toric structure
$\rightsquigarrow$ "degree" of a polynomial

Coordinate ring of $\mathcal{H}_\eta$: Cox Ring

Polynomial coordinate ring of $\mathcal{H}_\eta$ over $\mathbb{F}_q$: $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
Endowed with a **graduation** inherited from the toric structure
$\rightsquigarrow$ "degree" of a polynomial

A monomial $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ has **bidegree** (δ_T, δ_X) if

$$\begin{cases} \delta_T & = c_1 + c_2 - \eta d_1, \\ \delta_X & = d_1 + d_2. \end{cases} \tag{1}$$

Coordinate ring of $\mathcal{H}_\eta$: Cox Ring

Polynomial coordinate ring of $\mathcal{H}_\eta$ over $\mathbb{F}_q$: $R = \mathbb{F}_q[T_1, T_2, X_1, X_2]$.
Endowed with a **graduation** inherited from the toric structure
$\rightsquigarrow$ "degree" of a polynomial

A monomial $M = T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2}$ has **bidegree** (δ_T, δ_X) if

$$\begin{cases} \delta_T &= c_1 + c_2 - \eta d_1, \\ \delta_X &= d_1 + d_2. \end{cases} \tag{1}$$

Set $R(\delta_T, \delta_X)$ the $\mathbb{F}_q$-v.s. spanned by monomials of bidegree (δ_T, δ_X).

$$R = \bigoplus_{(\delta_T, \delta_X) \in \mathbb{Z}^2} R(\delta_T, \delta_X)$$

Definition of an evaluation map on $\mathcal{H}_\eta$

Similarly to *projective Reed-Muller codes*, **evaluating polynomials**
$\rightsquigarrow$ Meaning *à la Lachaud*

Points on $\mathcal{H}_\eta \leftrightarrow$ Orbits under

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

$\mathbb{F}_q$-rational points $\leftrightarrow$ Orbits with a $\mathbb{F}_q$-rational representative.

Definition of an evaluation map on $\mathcal{H}_\eta$

Similarly to *projective Reed-Muller codes*, **evaluating polynomials**
$\rightsquigarrow$ Meaning *à la Lachaud*

Points on $\mathcal{H}_\eta \leftrightarrow$ Orbits under

$$(\lambda, \mu) \cdot (t_1, t_2, x_1, x_2) = (\lambda t_1, \lambda t_2, \mu \lambda^{-\eta} x_1, \mu x_2).$$

$\mathbb{F}_q$-rational points $\leftrightarrow$ Orbits with a $\mathbb{F}_q$-rational representative.

Evaluate a polynomial at the **unique** representative of the following forms :

$$(1, a, 1, b) \quad (0, 1, 1, b) \quad (1, a, 0, 1) \quad (0, 1, 0, 1)$$

with $a,\ b \in \mathbb{F}_q$.

Evaluation code on $\mathcal{H}_\eta$

Evaluation code $C_\eta(\delta_T, \delta_X)$ defined as the image of

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T, \delta_X) & \to & \mathbb{F}_q^{(q+1)^2} \\ F & \mapsto & (F(P))_{P \in \mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{2}$$

Evaluation code on $\mathcal{H}_\eta$

Evaluation code $C_\eta(\delta_T, \delta_X)$ defined as the image of

$$\mathrm{ev}_{(\delta_T,\delta_X)} : \left\{ \begin{array}{rcl} R(\delta_T, \delta_X) & \to & \mathbb{F}_q^{(q+1)^2} \\ F & \mapsto & (F(P))_{P \in \mathcal{H}\eta(\mathbb{F}_q)}. \end{array} \right. \tag{2}$$

Implementation: No knowledge about a Hirzeruch surface needed. Enough to build the set of polynomials and evaluate them at the $(q+1)^2$ points $(1, a, 1, b)$, $(0, 1, 1, b)$, $(1, a, 0, 1)$ and $(0, 1, 0, 1)$.

Motivation

- Leaving the case $\operatorname{rk} \operatorname{Pic} S = 1$[1] (easy case to compute the minimum distance)
- Codes on Hirzebruch surfaces: already studied by *toric codes*[2]
  Toric codes on evaluate at points on the torus (without zero coordinate)
  $\rightsquigarrow$ Affine $\to$ Projective case: increase the parameters
- Starting point: Codes on rational surface scrolls[3]

[1] Zarzar (2007), Little,Sheck (2018)
[2] Hansen (2002), Joyner (2004), Little,Sheck (2016)...
[3] Carvalho, Neumann (2016)

Motivation

- Leaving the case $\operatorname{rk}\operatorname{Pic} S = 1$[1] (easy case to compute the minimum distance)
- Codes on Hirzebruch surfaces: already studied by *toric codes*[2]
  Toric codes on evaluate at points on the torus (without zero coordinate)
  $\rightsquigarrow$ Affine $\to$ Projective case: increase the parameters
- Starting point: Codes on rational surface scrolls[3]

Aim: Study the codes $C_\eta(\delta_T, \delta_X)$ for any $(\delta_T, \delta_X) \in \mathbb{Z}^2$ on $\mathbb{F}_q$ for any size of q, taking advantage of the **toric** structure.

[1] Zarzar (2007), Little,Sheck (2018)
[2] Hansen (2002), Joyner (2004), Little,Sheck (2016)...
[3] Carvalho, Neumann (2016)

Dimension of the code

$$C_\eta(\delta_T, \delta_X)$$

$$\wr|$$

$$R(\delta_T, \delta_X) \big/ \ker \mathrm{ev}_{(\delta_T, \delta_X)}$$

Dimension of the code

$$C_\eta(\delta_T,\delta_X) \cong R(\delta_T,\delta_X) / \ker \mathrm{ev}_{(\delta_T,\delta_X)}$$

Restrict the relation on **monomials**

$M \equiv M' \iff M' - M \in \ker \mathrm{ev}_{(\delta_T,\delta_X)}$

$$\mathcal{M}(\delta_T,\delta_X) / \equiv$$

Monomials of $R(\delta_T,\delta_X)$

Dimension of the code

$$C_\eta(\delta_T,\delta_X) \cong R(\delta_T,\delta_X) / \ker \mathrm{ev}_{(\delta_T,\delta_X)}$$

Restrict the relation on **monomials**

$$M \equiv M' \iff M' - M \in \ker \mathrm{ev}_{(\delta_T,\delta_X)}$$

$$\mathcal{M}(\delta_T,\delta_X) / \equiv$$

Monomials of $R(\delta_T,\delta_X)$

$\updownarrow$

Lattice points of a polygon

Dimension of the code

Restrict the relation on **monomials**

$M \equiv M' \iff M' - M \in \ker \mathrm{ev}_{(\delta_T, \delta_X)}$

$$C_\eta(\delta_T, \delta_X) \cong R(\delta_T, \delta_X) / \ker \mathrm{ev}_{(\delta_T, \delta_X)}$$

$\mathcal{M}(\delta_T, \delta_X) / \equiv$ $\longleftarrow$ Monomials of $R(\delta_T, \delta_X)$

$\updownarrow$ Equivalence classes of points

$\updownarrow$ Lattice points of a polygon

Representation of $R(\delta_T, \delta_X)$ as a polygon

$T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \in R(\delta_T, \delta_X)$ **iff** $d_1 + d_2 = \delta_X$ and $c_1 + c_2 - \eta d_1 = \delta_T$.

Fix (δ_T, δ_X). A monomial is *uniquely determined* by the couple (d_2, c_2) in

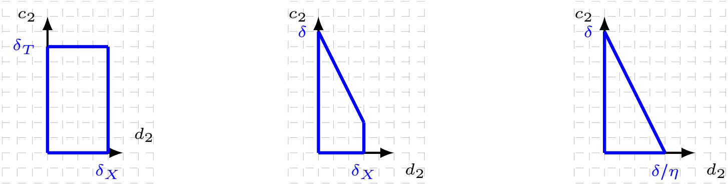
$$P(\delta_T, \delta_X) = \{(d_2, c_2) \in \mathbb{N}^2 \mid 0 \leq d_2 \leq \delta_X \text{ and } 0 \leq c_2 \leq \delta - \eta d_2\}.$$

Representation of $R(\delta_T, \delta_X)$ as a polygon

$T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \in R(\delta_T, \delta_X)$ **iff** $d_1 + d_2 = \delta_X$ and $c_1 + c_2 - \eta d_1 = \delta_T$.

Fix (δ_T, δ_X). A monomial is *uniquely determined* by the couple (d_2, c_2) in

$$P(\delta_T, \delta_X) = \{(d_2, c_2) \in \mathbb{N}^2 \mid 0 \leq d_2 \leq \delta_X \text{ and } 0 \leq c_2 \leq \delta - \eta d_2\}.$$



$\eta = 0$
e.g. $\mathcal{P}(7, 4)$

$\eta > 0,\ \delta_T > 0$
e.g. $\mathcal{P}(2, 3)$ in $\mathcal{H}_2$

$\eta > 0,\ \delta_T \leq 0$
e.g. $\mathcal{P}(-2, 5)$ in $\mathcal{H}_2$

Monomials of $R(\delta_T, \delta_X) \leftrightarrow$ Lattice points of $\mathcal{P}(\delta_T, \delta_X)$

Characterization for equivalent monomials/lattice points

Proposition

$$T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \equiv T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'}$$

$$\Updownarrow$$

$$\begin{cases} q-1 & \mid d_i - d_i', \\ q-1 & \mid c_j - c_j', \\ d_i = 0 & \Leftrightarrow d_i' = 0, \\ c_j = 0 & \Leftrightarrow c_j' = 0. \end{cases}$$

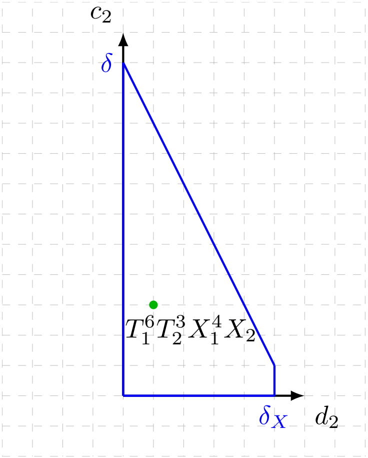
Characterization for equivalent monomials/lattice points

Proposition

$$T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \equiv T_1^{c_1'}T_2^{c_2'}X_1^{d_1'}X_2^{d_2'}$$

$$\Updownarrow$$

$$\begin{cases} q-1 & \mid d_i - d_i', \\ q-1 & \mid c_j - c_j', \\ d_i = 0 & \Leftrightarrow d_i' = 0, \\ c_j = 0 & \Leftrightarrow c_j' = 0. \end{cases}$$



$\mathcal{P}(5,5)$ on $\mathbb{F}_4$

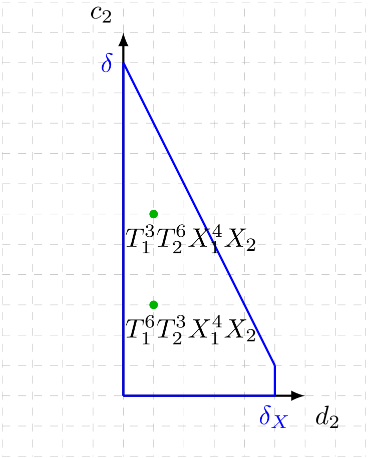
Characterization for equivalent monomials/lattice points

Proposition

$$T_1^{c_1}T_2^{c_2}X_1^{d_1}X_2^{d_2} \equiv T_1^{c_1'}T_2^{c_2'}X_1^{d_1'}X_2^{d_2'}$$

$$\Updownarrow$$

$$\begin{cases} q-1 & \mid d_i - d_i', \\ q-1 & \mid c_j - c_j', \\ d_i = 0 & \Leftrightarrow d_i' = 0, \\ c_j = 0 & \Leftrightarrow c_j' = 0. \end{cases}$$



$\mathcal{P}(5,5)$ on $\mathbb{F}_4$

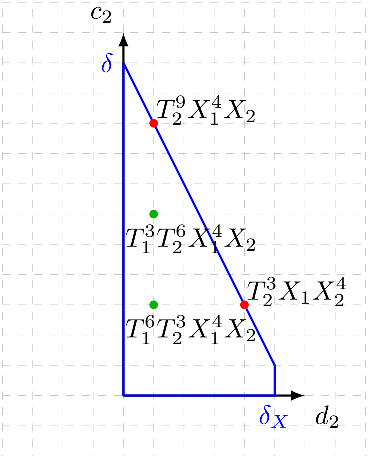
Characterization for equivalent monomials/lattice points

Proposition

$$T_1^{c_1} T_2^{c_2} X_1^{d_1} X_2^{d_2} \equiv T_1^{c_1'} T_2^{c_2'} X_1^{d_1'} X_2^{d_2'}$$

$$\Updownarrow$$

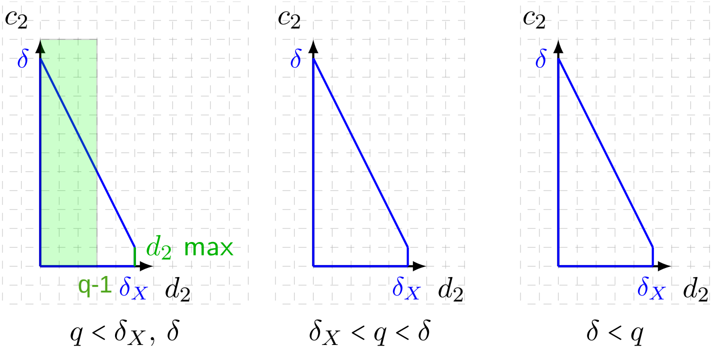
$$\begin{cases} q-1 & \mid d_i - d_i', \\ q-1 & \mid c_j - c_j', \\ d_i = 0 & \Leftrightarrow d_i' = 0, \\ c_j = 0 & \Leftrightarrow c_j' = 0. \end{cases}$$



$\mathcal{P}(5,5)$ on $\mathbb{F}_4$

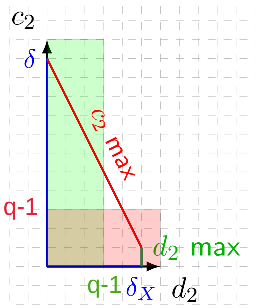
Choice of representatives among lattice points

d_2 as small as possible then c_2 as small as possible
$\sim$ Remainder modulo $q-1$ unless 0 or maximum

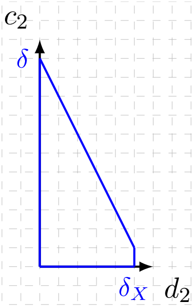


Choice of representatives among lattice points

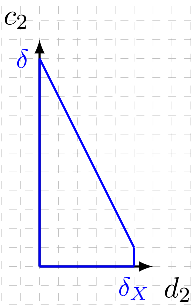
d_2 as small as possible then c_2 as small as possible
$\sim$ Remainder modulo $q-1$ unless 0 or maximum



$q < \delta_X,\ \delta$



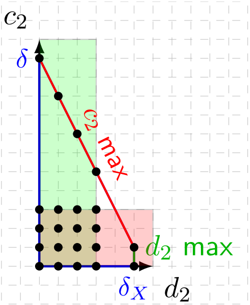
$\delta_X < q < \delta$



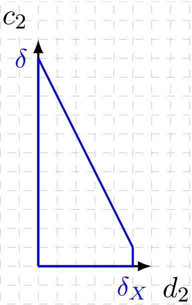
$\delta < q$

Choice of representatives among lattice points

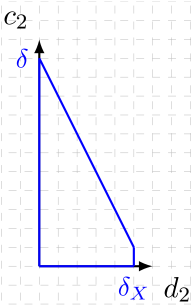
d_2 as small as possible then c_2 as small as possible
$\sim$ Remainder modulo $q-1$ unless 0 or maximum



$q < \delta_X,\ \delta$



$\delta_X < q < \delta$

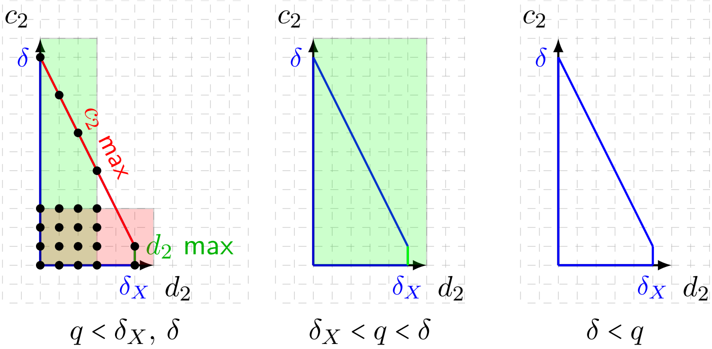


$\delta < q$

Choice of representatives among lattice points

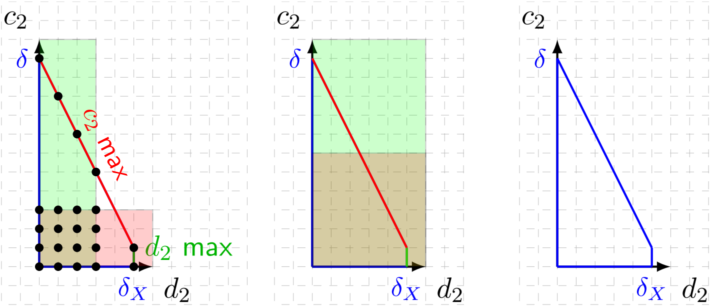
d_2 as small as possible then c_2 as small as possible

$\sim$ Remainder modulo $q-1$ unless 0 or maximum



Choice of representatives among lattice points

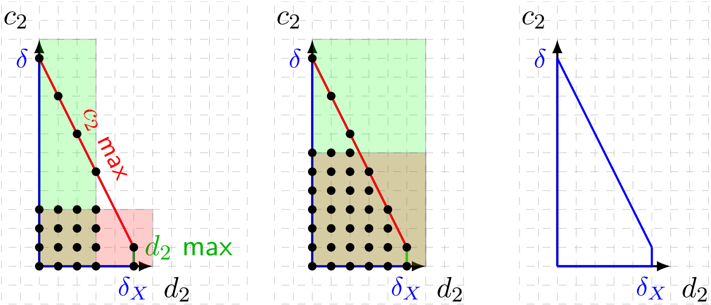
d_2 as small as possible then c_2 as small as possible
$\sim$ Remainder modulo $q-1$ unless 0 or maximum



$q < \delta_X,\ \delta$ | $\delta_X < q < \delta$ | $\delta < q$

Choice of representatives among lattice points

d_2 as small as possible then c_2 as small as possible
$\sim$ Remainder modulo $q-1$ unless 0 or maximum

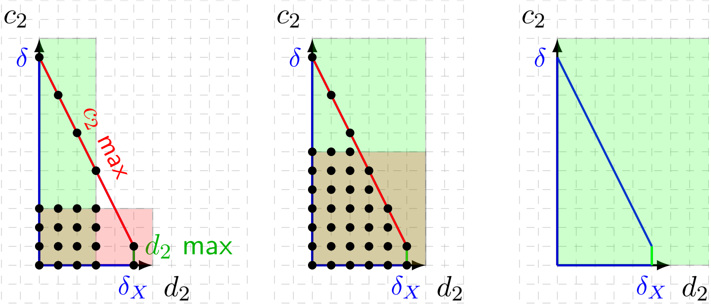


$q < \delta_X,\ \delta$ $\qquad$ $\delta_X < q < \delta$ $\qquad$ $\delta < q$

Choice of representatives among lattice points

d_2 as small as possible then c_2 as small as possible

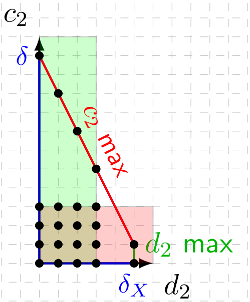
$\sim$ Remainder modulo $q-1$ unless 0 or maximum



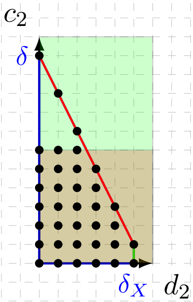
$q < \delta_X,\ \delta$ $\qquad$ $\delta_X < q < \delta$ $\qquad$ $\delta < q$

Choice of representatives among lattice points

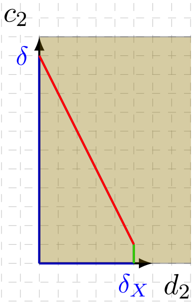
d_2 as small as possible then c_2 as small as possible
$\sim$ Remainder modulo $q-1$ unless 0 or maximum



$q < \delta_X,\ \delta$



$\delta_X < q < \delta$

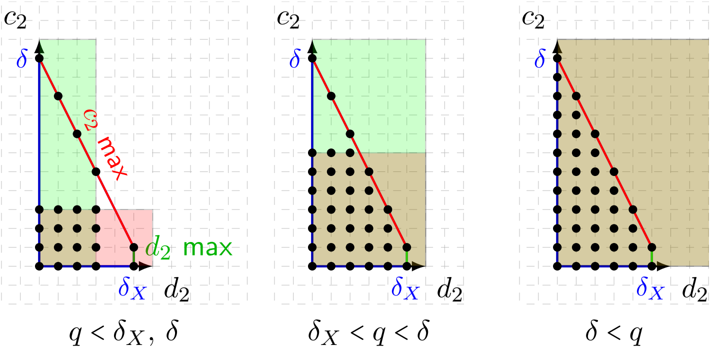


$\delta < q$

Choice of representatives among lattice points

d_2 as small as possible then c_2 as small as possible

$\sim$ Remainder modulo $q-1$ unless 0 or maximum



Explicit formula for the dimension of $C_\eta(\delta_T, \delta_X)$

Explicit formula for the dimension of $C_\eta(\delta_T, \delta_X)$

Theorem [N. - 2018]

$$\dim C_0(\delta_T, \delta_X) = (\min(\delta_T, q) + 1)\left(\min(\delta_X, q) + 1\right).$$

If $\eta \geq 2$, set $A = \min\left(\frac{\delta}{\eta}, \delta_X\right)$, $m = \min(\lfloor A \rfloor, q-1)$,

$$h = \begin{cases} \min(\delta_T, q) + 1 & \text{if } \delta_T \geq 0 \text{ and } q \leq \delta_X, \\ -1 & \text{if } \delta_T \leq 0,\ q \leq A \text{ and } \eta \mid \delta_T, \\ 0 & \text{otherwise,} \end{cases}$$

$$s = \frac{\delta - q}{\eta} \text{ and } \tilde{s} = \begin{cases} \lfloor s \rfloor & \text{if } s \in [0, m], \\ -1 & \text{if } s < 0, \\ m & \text{if } s > m. \end{cases}$$

Then

$$\dim C_\eta(\delta_T, \delta_X) = (q+1)(\tilde{s}+1) + (m - \tilde{s})\left(\delta + 1 - \eta\left(\frac{m+\tilde{s}+1}{2}\right)\right) + h.$$

Explicit formula for the minimum distance of $C_\eta(\delta_T, \delta_X)$

Theorem [N. - 2018]

- For $\eta = 0$, $d_0(\delta_T, \delta_X) = \max(q - \delta_X + 1, 1)\max(q - \delta_T + 1, 1)$.
- for $\eta \geq 2$,
  - If $q > \delta$, then
  $$d_\eta(\delta_T, \delta_X) = (q + \mathbb{1}_{\delta_X = 0})(q - \delta + 1),$$
  - If $\max\left(\frac{\delta}{\eta+1}, \delta_T\right) < q \leq \delta$, then
  $$d_\eta(\delta_T, \delta_X) = q - \left\lfloor \frac{\delta - q}{\eta} \right\rfloor,$$
  - If $q \leq \max\left(\frac{\delta}{\eta+1}, \delta_T\right)$,
  $$d_\eta(\delta_T, \delta_X) = \begin{cases} \max(q - \delta_X + 1, 1) & \text{if } \delta_T \geq 0, \\ 1 & \text{if } \delta_T < 0, \end{cases}$$

PIR Protocol

PIR Protocol

How to retrieve a datum stored on servers without giving any information about it?

$\rightsquigarrow$ Aim of **P**rivate **I**nformation **R**etrieval protocols

PIR Protocol

How to retrieve a datum stored on servers without giving any information about it?

$\rightsquigarrow$ Aim of **P**rivate **I**nformation **R**etrieval protocols

[Augot,Levy-dit-Vehel,Shikfa-14] Share the database on several servers.

PIR Protocol

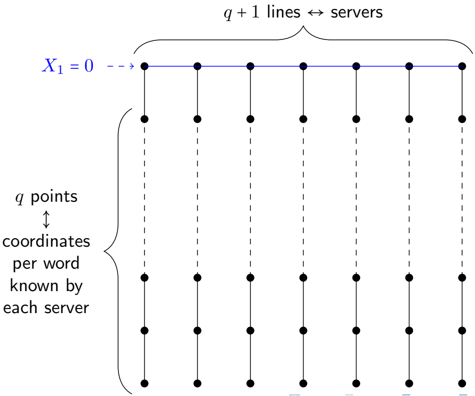
How to retrieve a datum stored on servers without giving any information about it?

$\rightsquigarrow$ Aim of **P**rivate **I**nformation **R**etrieval protocols

[Augot,Levy-dit-Vehel,Shikfa-14] Share the database on several servers.

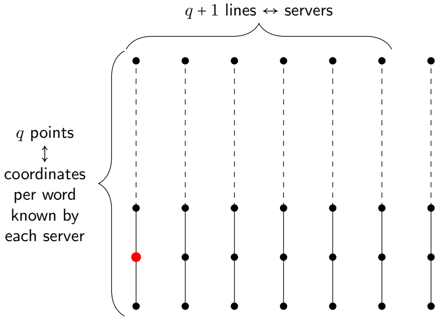
$\mathcal{H}_\eta(\mathbb{F}_q) = \bigsqcup_{i=0}^{q} L_i(\mathbb{F}_q)$
(lines of the ruling)

Database: Codewords of $C_\eta(\delta_T, \delta_X)$ *punctured* at the points lying on $X_1 = 0$ shared by $\mathbf{q+1}$ **servers**.



Local property of $C_\eta(\delta_T, \delta_X)$ and PIR Protocol on $\mathcal{H}_\eta$

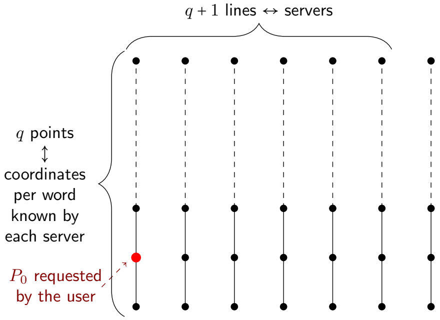
η-line:= $X_2 = X_1 F(T_1, T_2)$ with F homogeneous of degree η



Restricting a word of $C_\eta(\delta_T, \delta_X)$ along an η-line gives a word of a $\mathrm{PRS}(\delta)$.

Local property of $C_\eta(\delta_T, \delta_X)$ and PIR Protocol on $\mathcal{H}_\eta$

η-line:$=$ $X_2 = X_1 F(T_1, T_2)$ with F homogeneous of degree η

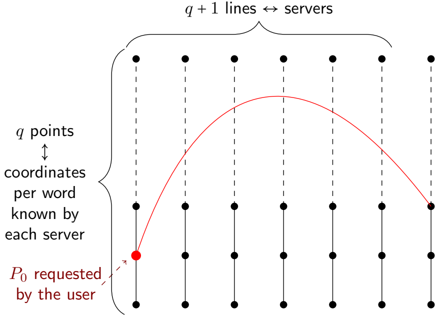


Restricting a word of $C_\eta(\delta_T, \delta_X)$ along an η-line gives a word of a $\mathrm{PRS}(\delta)$.

Wanted datum: c_{P_0} with $c \in C_\eta(\delta_T, \delta_X)$ and $\delta < q - 2$.

Local property of $C_\eta(\delta_T, \delta_X)$ and PIR Protocol on $\mathcal{H}_\eta$

η-line:= $X_2 = X_1 F(T_1, T_2)$ with F homogeneous of degree η



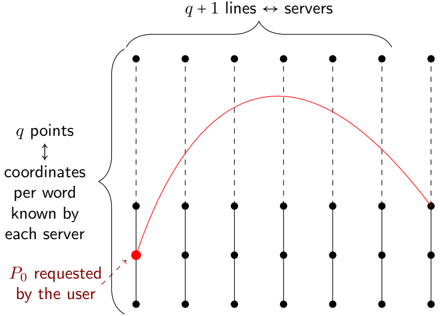
Randomly pick an η-line L containing P_0.

Restricting a word of $C_\eta(\delta_T, \delta_X)$ along an η-line gives a word of a $\mathrm{PRS}(\delta)$.

Wanted datum: c_{P_0} with $c \in C_\eta(\delta_T, \delta_X)$ and $\delta < q-2$.

Local property of $C_\eta(\delta_T, \delta_X)$ and PIR Protocol on $\mathcal{H}_\eta$

η-line:= $X_2 = X_1 F(T_1, T_2)$ with F homogeneous of degree η



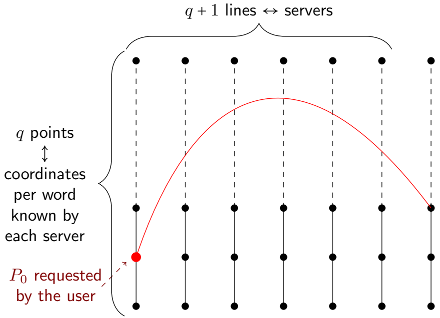
Restricting a word of $C_\eta(\delta_T, \delta_X)$ along an η-line gives a word of a $\mathrm{PRS}(\delta)$.

Wanted datum: c_{P_0} with $c \in C_\eta(\delta_T, \delta_X)$ and $\delta < q - 2$.

Randomly pick an η-line L containing P_0.
Server ↔ line not containing P_0: ask for $c_{L_i \cap L}$

Local property of $C_\eta(\delta_T, \delta_X)$ and PIR Protocol on $\mathcal{H}_\eta$

η-line:= $X_2 = X_1 F(T_1, T_2)$ with F homogeneous of degree η



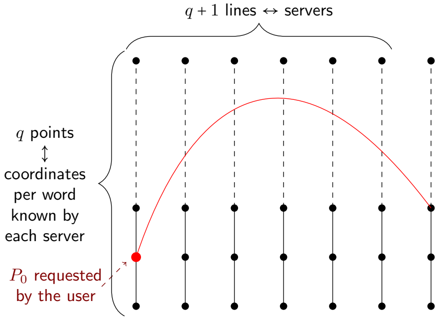
Restricting a word of $C_\eta(\delta_T, \delta_X)$ along an η-line gives a word of a $\mathrm{PRS}(\delta)$.

Wanted datum: c_{P_0} with $c \in C_\eta(\delta_T, \delta_X)$ and $\delta < q - 2$.

Randomly pick an η-line L containing P_0.
Server $\leftrightarrow$ line not containing P_0: ask for $c_{L_i \cap L}$
Server $\leftrightarrow$ line containing P_0: ask for c_{P_1} for P_1 random on this line

Local property of $C_\eta(\delta_T,\delta_X)$ and PIR Protocol on $\mathcal{H}_\eta$

η-line:= $X_2 = X_1 F(T_1,T_2)$ with F homogeneous of degree η



Restricting a word of $C_\eta(\delta_T,\delta_X)$ along an η-line gives a word of a $\mathrm{PRS}(\delta)$.

Wanted datum: c_{P_0} with $c \in C_\eta(\delta_T,\delta_X)$ and $\delta < q-2$.

Randomly pick an η-line L containing P_0.
Server $\leftrightarrow$ line not containing P_0: ask for $c_{L_i \cap L}$
Server $\leftrightarrow$ line containing P_0: ask for c_{P_1} for P_1 random on this line

$\Rightarrow$ Word of PRS(δ) with 1 error = easily correctable!

What's new?

Case $\eta = 1$ already known (PIR protocol from LDC)

Why take $\eta > 1$?

What's new?

Case $\eta = 1$ already known (PIR protocol from LDC)

Why take $\eta > 1$? What if servers communicate...?

What's new?

Case $\eta = 1$ already known (PIR protocol from LDC)

Why take $\eta > 1$? What if servers communicate...?

$\eta = 1 \Rightarrow$ the protocol does not resist to colluding servers!

$\eta > 1 \Rightarrow$ the protocol resists to the collusion of η servers!

What's new?

Case $\eta = 1$ already known (PIR protocol from LDC)

Why take $\eta > 1$? What if servers communicate...?

$\eta = 1 \Rightarrow$ the protocol does not resist to colluding servers!

$\eta > 1 \Rightarrow$ the protocol resists to the collusion of η servers!

... **Counterpart**...

What's new?

Case $\eta = 1$ already known (PIR protocol from LDC)

Why take $\eta > 1$? What if servers communicate...?

$\eta = 1 \Rightarrow$ the protocol does not resist to colluding servers!

$\eta > 1 \Rightarrow$ the protocol resists to the collusion of η servers!

... **Counterpart**... We want δ as near to q as possible and

$$\dim C_\eta(\delta_T, \delta_X) = (\delta_X + 1)\left(\frac{\delta}{\eta} - \eta\frac{\delta_X}{2} + 1\right)$$

decreases as η grows $\Rightarrow$ Loss of storage when η grows.

Can be fixed by lifting process (introduced by Guo, Kopparty, Sudan in 2013)...

More on ArXiv:

- About these codes: `https://arxiv.org/abs/1801.08407`
- About lift: `https://arxiv.org/abs/1904.08696` (joint work with Julien Lavauzelle)

Thank you for your attention!

Questions?