Explicit construction and parameters of projective toric codes

Jade Nardi

INRIA Saclay, LIX

March, 2021
Institut de Mathématiques de Bordeaux
Séminaire de Théorie Algorithmique des Nombres

https://arxiv.org/abs/2003.10357

Example of classical/Projective toric code

Classical toric code: Span of the evaluation on $(\mathbb{F}_q^*)^2$ of monomials

$$\begin{array}{cc} y^2 & \\ y & xy \\ & x \end{array}$$

HOMOGENISATION: choose variety & degree

2 on $\mathbb{P}^2$ $[X, Y, Z]$

$$\begin{array}{ccc} Y^2 & & \\ YZ & XY & \\ Z^2 & XZ & X^2 \end{array}$$

$(1,2)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ $[X_0, X_1, Y_0, Y_1]$

$$\begin{array}{cc} X_0Y_1^2 & X_1Y_1^2 \\ X_0Y_0Y_1 & X_1Y_0Y_1 \\ X_0Y_0^2 & X_1Y_0^2 \end{array}$$

Projective toric code: Span of the evaluation of monomials on rational points of the *whole* variety

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

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

$(1, a, 0, 1)$ $(0, 1, 0, 1)$

$(a, b) \in \mathbb{F}_q^2$

Example of classical/Projective toric code

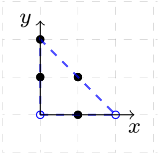
Classical toric code: Span of the evaluation on $(\mathbb{F}_q^*)^2$ of monomials

$$\begin{array}{cc} y^2 & \\ y & xy \\ & x \end{array}$$

HOMOGENISATION: choose variety & degree

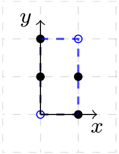
2 on $\mathbb{P}^2$ $[X, Y, Z]$

$$\begin{array}{ccc} Y^2 & & \\ YZ & XY & \\ Z^2 & XZ & X^2 \end{array}$$



$(1,2)$ on $\mathbb{P}^1 \times \mathbb{P}^1$ $[X_0, X_1, Y_0, Y_1]$

$$\begin{array}{cc} X_0Y_1^2 & X_1Y_1^2 \\ X_0Y_0Y_1 & X_1Y_0Y_1 \\ X_0Y_0^2 & X_1Y_0^2 \end{array}$$



Projective toric code: Span of the evaluation of monomials on rational points of the *whole* variety

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

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

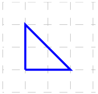
$(a, b) \in \mathbb{F}_q^2$

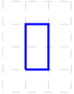
Polygon $\leftrightarrow$ variety & degree

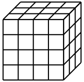
Classical/Projective toric codes

An integral polytope $P \subset \mathbb{R}^N$ (vertices in $\mathbb{Z}^N$) defines an abstract toric variety $\mathbf{X}_P$ with a divisor D and a monomial basis of $L(D)$ (set of polynomials of a certain *degree*).

Size of $P \leftrightarrow$ Degree in $L(D)$


$\mathbb{P}^2$
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**?

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

Classical toric code: $\mathsf{C}_P = \left\{(f(\mathbf{t}))_{\mathbf{t}\in\mathbb{T}_P(\mathbb{F}_q)} \mid f \in L(D)\right\}$

Hansen [Han02], Little-Schwarz [LS05], Ruano [Rua07], Soprunov-Soprunova [SS09]

Aim : Constructing and studying the **projective toric code**

$$\mathsf{PC}_P = \left\{(f(\mathbf{x}))_{\mathbf{x}\in\mathbf{X}_P(\mathbb{F}_q)} \mid f \in L(D)\right\}$$

Advantages similar to RM → PRM:

1. length ↗, minimum distance ↗ with roughly the same dimension.
2. Strenghten the geometric interpretation

Description of the toric variety $\mathbf{X}_P$ associated to the polytope P

Several ways to describe $\mathbf{X}_P$ thanks to the integral polytope P : *(under some assumptions)*

- with *fans* as an abstract variety $\oplus$ geometric properties $\ominus$ implementation

Description of the toric variety $\mathbf{X}_P$ associated to the polytope P

Several ways to describe $\mathbf{X}_P$ thanks to the integral polytope P : *(under some assumptions)*

- with *fans* as an abstract variety
  - $\oplus$ geometric properties
  - $\ominus$ implementation
- embedded into $\mathbb{P}^{\#\left(P\cap\mathbb{Z}^N\right)-1}$
  - $\oplus$ practical description
  - $\ominus$ very large ambiant

Description of the toric variety $\mathbf{X}_P$ associated to the polytope P

Several ways to describe $\mathbf{X}_P$ thanks to the integral polytope P : *(under some assumptions)*

- with *fans* as an abstract variety
  - $\oplus$ geometric properties
  - $\ominus$ implementation
- embedded into $\mathbb{P}^{\#\left(P\cap\mathbb{Z}^N\right)-1}$
  - $\oplus$ practical description
  - $\ominus$ very large ambiant
- as a quotient of a subset of $\mathbb{A}^r$ (where $r =$ nb of facets of P) by a group G *(simplicial variety)*
  - $\oplus$ more reasonable ambient
  - $\oplus$ functions of $L(D) =$ polynomials in r variables

Description of the toric variety $\mathbf{X}_P$ associated to the polytope P

Several ways to describe $\mathbf{X}_P$ thanks to the integral polytope P : *(under some assumptions)*

- with *fans* as an abstract variety
  - $\oplus$ geometric properties
  - $\ominus$ implementation
- embedded into $\mathbb{P}^{\#\left(P\cap\mathbb{Z}^N\right)-1}$
  - $\oplus$ practical description
  - $\ominus$ very large ambiant
- as a quotient of a subset of $\mathbb{A}^r$ (where $r =$ nb of facets of P) by a group G *(simplicial variety)*
  - $\oplus$ more reasonable ambient
  - $\oplus$ functions of $L(D) =$ polynomials in r variables

Example: $P = \mathrm{Conv}((0,0),(1,0),(0,1),(1,1)) \subset \mathbb{R}^2$ gives $\mathbf{X}_P = \mathbb{P}^1 \times \mathbb{P}^1$:

- embedded in $\mathbb{P}^3$ by the Segre map: $(x_0,x_1,y_0,y_1) \mapsto (x_iy_j)$,
- defined as the quotient of $\left(\mathbb{A}^2 \setminus \{(0,0)\}\right)^2 \subset \mathbb{A}^4$ by the group $(\bar{\mathbb{F}}^*)^2$ via the action

$$(\lambda,\mu)\cdot(x_0,x_1,y_0,y_1) = (\lambda x_0,\lambda x_1,\mu y_0,\mu y_1)$$

Functions= bihomogeneous polynomials

For classical toric codes, an integral point $m \in P \cap \mathbb{Z}^N$ gives a monomial $\chi^m = X_1^{m_1} \dots X_N^{m_N}$.
In the projective case, it corresponds to a monomial $\chi^{\langle m,P \rangle} \in \mathbb{F}_\mathbf{q}[\mathbf{X_1}, \dots, \mathbf{X_r}]$.

$$L(D) = \mathrm{Span}\left(\chi^{\langle m,P \rangle} \mid m \in P \cap \mathbb{Z}^N\right)$$

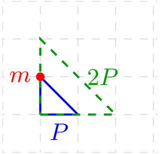
We can go from χ^m to $\chi^{\langle m,P \rangle}$ via **homogenization** process.

For classical toric codes, an integral point $m \in P \cap \mathbb{Z}^N$ gives a monomial $\chi^m = X_1^{m_1} \dots X_N^{m_N}$.
In the projective case, it corresponds to a monomial $\chi^{\langle m,P\rangle} \in \mathbb{F}_\mathbf{q}[\mathbf{X_1}, \dots, \mathbf{X_r}]$.

$$L(D) = \mathrm{Span}\left(\chi^{\langle m,P\rangle} \mid m \in P \cap \mathbb{Z}^N\right)$$

We can go from χ^m to $\chi^{\langle m,P\rangle}$ via **homogenization** process.

Example on $\mathbb{P}^2$:



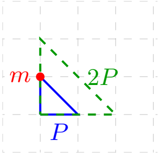
- $\chi^m = x_1^0 x_2^1 = x_2$.
- $\chi^{\langle m,P\rangle} = X_2 \leftarrow$ homogenized in degree 1
- $\chi^{\langle m,2P\rangle} = X_0 X_2 \leftarrow$ homogenized in degree 2

For classical toric codes, an integral point $m \in P \cap \mathbb{Z}^N$ gives a monomial $\chi^m = X_1^{m_1} \dots X_N^{m_N}$.
In the projective case, it corresponds to a monomial $\chi^{\langle m,P\rangle} \in \mathbb{F}_\mathbf{q}[\mathbf{X_1}, \dots, \mathbf{X_r}]$.

$$L(D) = \mathrm{Span}\left(\chi^{\langle m,P\rangle} \mid m \in P \cap \mathbb{Z}^N\right)$$

We can go from χ^m to $\chi^{\langle m,P\rangle}$ via **homogenization** process.

Example on $\mathbb{P}^2$*:*



- $\chi^m = x_1^0 x_2^1 = x_2$.
- $\chi^{\langle m,P\rangle} = X_2 \leftarrow$ homogenized in degree 1
- $\chi^{\langle m,2P\rangle} = X_0 X_2 \leftarrow$ homogenized in degree 2

$$\mathrm{PC}_P = \mathrm{Span}\left\{\left(\chi^{\langle m,P\rangle}(\mathbf{x})\right)_{\mathbf{x}\in\mathcal{P}} \in \mathbb{F}_q^n,\ m \in P \cap \mathbb{Z}^N\right\} \text{ where } n = \#\mathbf{X}_P(\mathbb{F}_q).$$

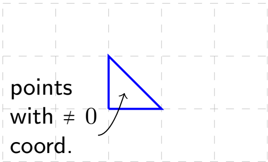
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

$$\Rightarrow \#\mathbb{T}_Q(\mathbb{F}_q) = (q-1)^{\dim Q}.$$

Number of $\mathbb{F}_q$-points of $\mathbf{X}_P$

$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^N + \sum_{i=0}^{N-1} (\text{nb of } i\text{-dim faces}) \times (q-1)^i.$$

Projective Plane $\mathbb{P}^2$



$$\#\mathbb{P}^2(\mathbb{F}_q) = (q-1)^2$$

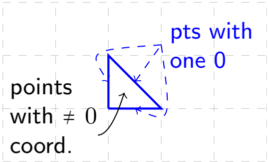
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

$$\Rightarrow \#\mathbb{T}_Q(\mathbb{F}_q) = (q-1)^{\dim Q}.$$

Number of $\mathbb{F}_q$-points of $\mathbf{X}_P$

$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^N + \sum_{i=0}^{N-1} (\text{nb of } i\text{-dim faces}) \times (q-1)^i.$$

Projective Plane $\mathbb{P}^2$



$$\#\mathbb{P}^2(\mathbb{F}_q) = (q-1)^2 + 3(q-1)$$

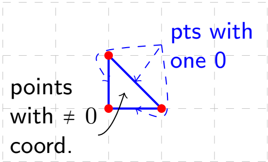
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

$\Rightarrow \#\mathbb{T}_Q(\mathbb{F}_q) = (q-1)^{\dim Q}$.

Number of $\mathbb{F}_q$-points of $\mathbf{X}_P$

$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^N + \sum_{i=0}^{N-1} (\text{nb of } i\text{-dim faces}) \times (q-1)^i.$$

Projective Plane $\mathbb{P}^2$



$$\#\mathbb{P}^2(\mathbb{F}_q) = (q-1)^2 + 3(q-1) + 3$$

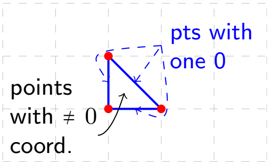
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

$$\Rightarrow \#\mathbb{T}_Q(\mathbb{F}_q) = (q-1)^{\dim Q}.$$

Number of $\mathbb{F}_q$-points of $\mathbf{X}_P$

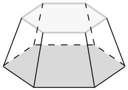
$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^N + \sum_{i=0}^{N-1} (\text{nb of } i\text{-dim faces}) \times (q-1)^i.$$

Projective Plane $\mathbb{P}^2$



$$\#\mathbb{P}^2(\mathbb{F}_q) = (q-1)^2 + 3(q-1) + 3$$

A random toric 3-fold



dim	3	2	1	0
# faces	1	8	18	12

$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^3 + 8(q-1)^2 + 18(q-1) + 12$$

✔ Length of PC_P

Dimension of classical toric code

"Recall": The integral points of P give a monomial basis of C_P and PC_P.

$$\text{Integral point } m \in P \cap \mathbb{Z}^N \leftrightarrow \mathrm{ev}\underbrace{\left(\chi^{\langle m,P\rangle}\right)}_{\text{monomial}} \in \mathsf{C}_P/\mathsf{PC}_P$$

Classical case: on $\mathbb{F}_q^*$, $x^{q-1} = 1$.
For two elements $(u,v) \in (\mathbb{Z}^N)^2$, we write $u \sim v$ if $u - v \in (q-1)\mathbb{Z}^N$.

Theorem [Ruano 07]

- $\chi^{\langle m,P\rangle}(\mathbf{t}) = \chi^{\langle m',P\rangle}(\mathbf{t})$ for every $\mathbf{t} \in \mathbb{T}_P(\mathbb{F}_q) \Leftrightarrow m \sim m'$,
- If $\overline{P}$ is a set of representatives of $P \cap \mathbb{Z}^N$ modulo $\sim$, then $\left\{(\chi^{\langle \overline{m},P\rangle}(\mathbf{t}), \mathbf{t} \in \mathbb{T}_P(\mathbb{F}_q) \mid \overline{m} \in \overline{P}\right\}$ is a basis of C_P.

Not so nice when homogenizing! On $\mathbb{P}^1(\mathbb{F}_q)$, $X_0^q \neq X_0 X_1^{q-1}$ at $[1:0]$.

Q° = interior of the face Q

$(q-1)^2$ torus points $(a,b,1)$

r edges $(1,a,0),\ (1,0,a),\ (0,1,a)$: $q-1$ points, …, …

r vertices $(1,0,0)$, $(0,1,0)$, $(0,0,1)$

$m \in P^\circ$ $\updownarrow$ $X^iY^jZ^{d-i-j}$, $1 \leq i,j$ and $i+j<d$

$m \in F_1^\circ$ — X^iY^{d-i}

$m \in F_2^\circ$ — X^iZ^{d-i}

$\vdots$ — Y^iZ^{d-i}

$m \in F_r^\circ$

vertices of P $\updownarrow$ X^d, Y^d, Z^d

Figure: "Generator" matrix of PC_P when P is a polygon $(N=2)$

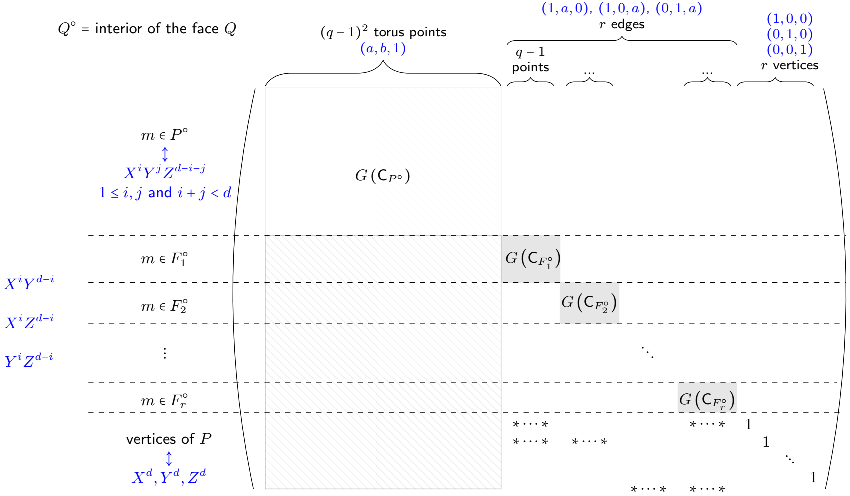


Figure: "Generator" matrix of PC_P when P is a polygon $(N = 2)$

Q° = interior of the face Q

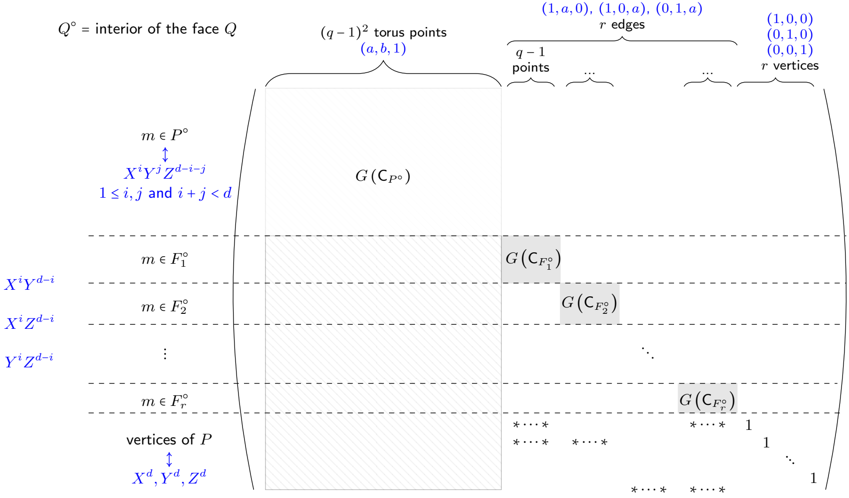


Figure: "Generator" matrix of PC_P when P is a polygon $(N=2)$

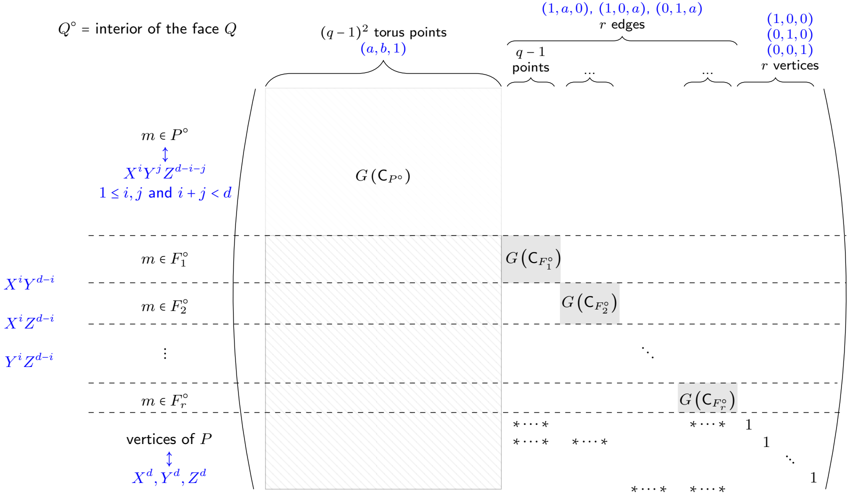


Figure: "Generator" matrix of PC_P when P is a polygon $(N=2)$

For any polytope P, there is a *generator matrix* of PC_P with such a triangular block structure.

✔ Explicit construction of PC_P

Dimension and reduction modulo $q-1$

Dimension of PC_P = rank of the previous matrix = $\sum_Q \dim \mathrm{C}_{Q^\circ}$

Projective case: Reduction of P **face by face**.

On $P \cap \mathbb{Z}^N$, we write $m \sim_P m'$ if there exists a face Q of P s.t. $m, m' \in Q^\circ$ and $m - m' \in (q-1)\mathbb{Z}^N$.

Theorem [N. 20]

- $\chi^{\langle m,P \rangle}(\mathbf{x}) = \chi^{\langle m',P \rangle}(\mathbf{x})$ for every $\mathbf{x} \in \mathbf{X}_P(\mathbb{F}_q) \Leftrightarrow m \sim_P m'$,
- If $\mathrm{Red}(P)$ is a set of representatives of $P \cap \mathbb{Z}^N$ modulo $\sim_P$, then $\left\{ \mathrm{ev}_P(\chi^{\langle \overline{m},P \rangle}) \mid \overline{m} \in \mathrm{Red}(P) \right\}$ is a basis of PC_P.

✔ Dimension of PC_P

Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
$\rightarrow \mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

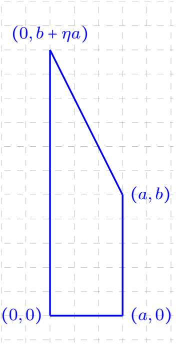
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

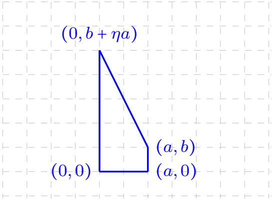
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b) = (3,5)$



$(a,b) = (2,1)$



Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ $\mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

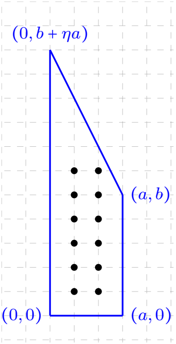
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

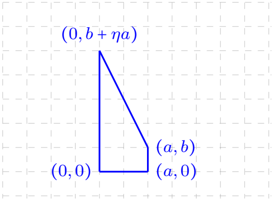
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b)=(3,5)$



$(a,b)=(2,1)$



Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
$\rightarrow$ $\mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

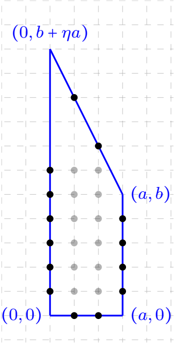
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

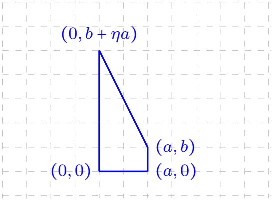
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b) = (3,5)$



$(a,b) = (2,1)$



Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
$\rightarrow \mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

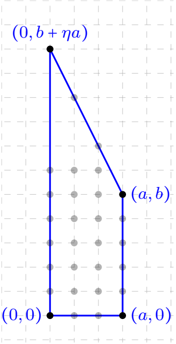
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

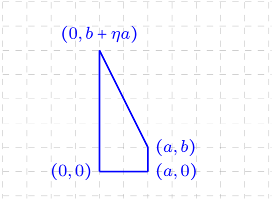
↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b) = (3,5)$



$\dim \mathsf{PC}_P = 30$

$(a,b) = (2,1)$



Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ $\mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

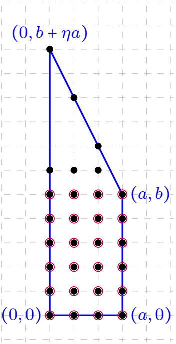
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

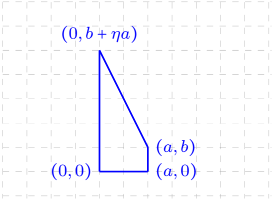
↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b) = (3,5)$



$\dim \mathsf{PC}_P = 30$
$\dim \mathsf{C}_P = 24$

$(a,b) = (2,1)$



Example of computation of the dimension of PC_P and C_P

Let $a,\ b,\ \eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ $\mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

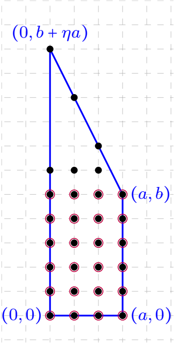
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

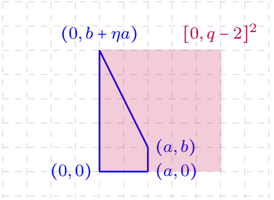
↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b) = (3,5)$



$\dim \mathsf{PC}_P = 30$
$\dim \mathsf{C}_P = 24$

$(a,b) = (2,1)$



Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ $\mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

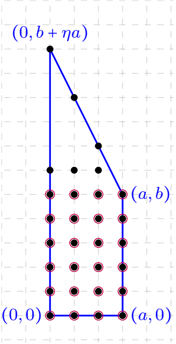
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

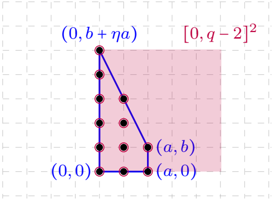
↳ Reduce the interior of each face modulo $q-1=6$.

$(a,b) = (3,5)$



$\dim \mathsf{PC}_P = 30$
$\dim \mathsf{C}_P = 24$

$(a,b) = (2,1)$



$\dim \mathsf{PC}_P = \dim \mathsf{C}_P = \# P \cap \mathbb{Z}^2 = 12$

Minimum distance

Lower bound on the minimum distance of PC_P more technical [CN16, Nar19]
Key ingredient: (theorical) **Gröbner basis** of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$
$\rightarrow$ no problem from the exponential growth in #variables of the complexity of its actual computation.

In conclusion, this work provides a general framework for studying AG codes on toric varieties. Given a polytope P, we can

- compute exactly the dimension of the code PC_P,
- get a lowerbound on the minimum distance (not always sharp),

provided that we have **a good algorithm to determine the integral points of a polytope**.

$\tilde{O}\left(\left(s^{\lceil \frac{N}{2} \rceil} + V\right) \log \delta\right)$ for a polytope of dim. N of vol. V with s vertices, and where δ is the maximum modulus of the coordinates of the vertices of P [SV13, Prop. 3.5].

Brown and Kasprzyk [BK13] systematically investigated (generalized) toric codes associated to small polygons → good codes acheiving/beating the best-known parameters.

Given a champion toric code C_P,

⊖ PC_P is unlikely to be a champion code itself,

⊕ indicate how to extend C_P while keeping good parameters.

Champion generalizing toric code $[49, 14, 26]$ over $\mathbb{F}_8$ [BK13]
Cannot consider its convex hull (~~simplicial~~ toric variety on $\mathbb{F}_8$)
→ projective toric code on $\mathbf{X}_P$ but PC_P is $[87, 14, 34]_8$.

Let us puncture this code!

$$\text{Torus points}\quad \left.\begin{array}{l} + 2 \text{ other points} = [51, 14, 27]_8 \\ + 2 \text{ other points} = [53, 14, 28]_8. \end{array}\right\} \text{Best known parameters}$$

$$+ 3 \text{ other points} = [56, 14, 29]_8$$

$$\text{Best known : } [54, 14, 29]_8$$

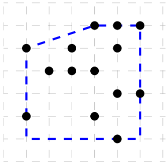
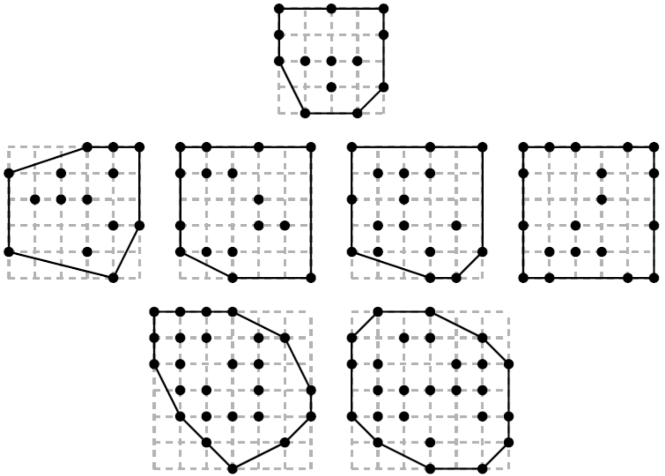


Figure: A polygon containing the points defining a champion generalized toric code $[49, 14, 26]$ over $\mathbb{F}_8$ [BK13]

7 ways to get non Hamming-equivalent (generalized) $[49, 14, 26]_8$ toric codes [BK13]



What now?

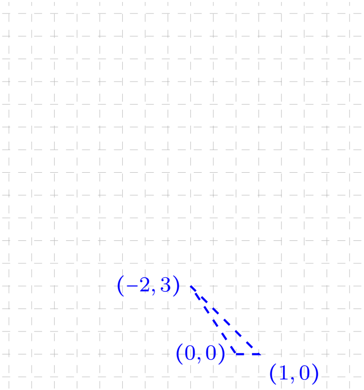
- Looking for new champion codes this way...
- Investigate properties of these codes : Local decodability [LN20],dual codes for application to secret sharing [Han16]

Thank you!

Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

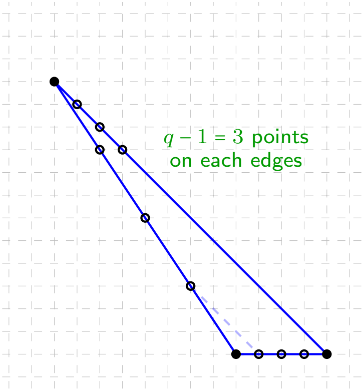
1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\# \mathrm{Red}(Q^\circ) = (q-1)^{\dim Q}$
   (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**.
   Representative $=$ smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

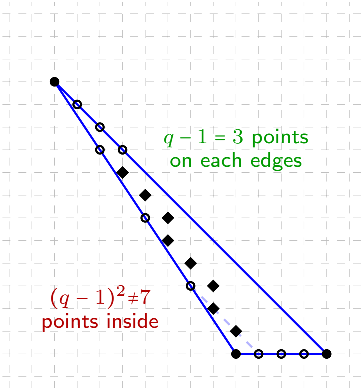
1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\#\,\mathrm{Red}(Q^\circ) = (q-1)^{\dim Q}$ (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 4$?
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**.
   Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

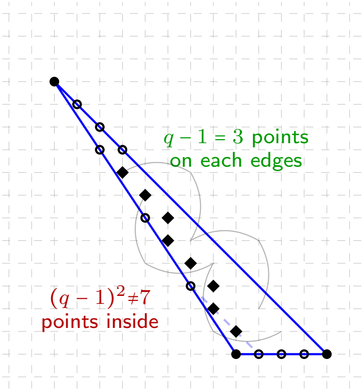
1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\#\operatorname{Red}(Q^\circ) = (q-1)^{\dim Q}$ (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 4$?
3. Compute $\operatorname{Red}(P)$ and $\operatorname{Red}(\lambda P)$ **taking into account the order**.
   Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

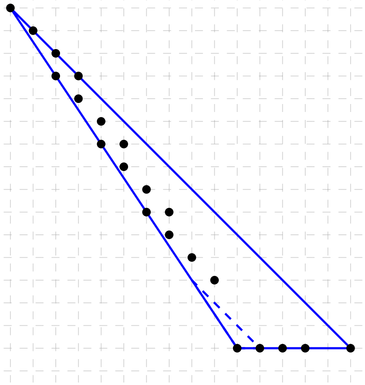
1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) : lexicographic
2. Find λ s.t. for every face Q of λP, $\#\,\mathrm{Red}(Q^\circ) = (q-1)^{\dim Q}$ (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$) $\lambda = 4$?
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**. Representative $=$ smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

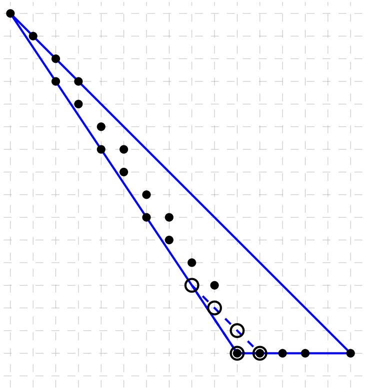
1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\# \mathrm{Red}(Q^\circ) = (q-1)^{\dim Q}$
   (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 5$
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**.
   Representative $=$ smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\#\,\mathrm{Red}(Q^\circ) = (q-1)^{\dim Q}$ (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 5$
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**.
   Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



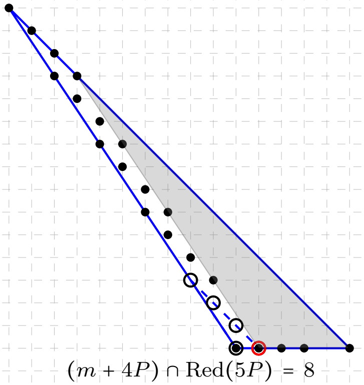
Theorem [N. 20]

$$d(\mathrm{PC}_P) \geq \min_{m \in \mathrm{Red}_<(P)} \#\left((m + P_{\mathsf{surj}} - P) \cap \mathrm{Red}_<(P_{\mathsf{surj}})\right).$$

Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\#\,\mathrm{Red}(Q^\circ) = (q-1)^{\dim Q}$
   (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 5$
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**.
   Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



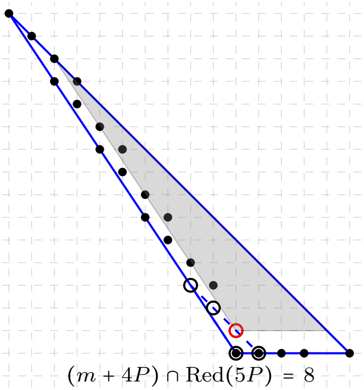
Theorem [N. 20]

$$d(\mathrm{PC}_P) \geq \min_{m \in \mathrm{Red}_<(P)} \#\left((m + P_{\mathsf{surj}} - P) \cap \mathrm{Red}_<(P_{\mathsf{surj}})\right).$$

Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

KEY INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$ [CN16, Nar19]

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) :
   lexicographic
2. Find λ s.t. for every face Q of λP, $\#\operatorname{Red}(Q^\circ) = (q-1)^{\dim Q}$ (*i.e.* $\mathrm{PC}_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 5$
3. Compute $\operatorname{Red}(P)$ and $\operatorname{Red}(\lambda P)$ **taking into account the order**.
   Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$
   $\rightarrow$ PC_P is $[21, 4, 8]_4$



Theorem [N. 20]

$$d(\mathrm{PC}_P) \geq \min_{m \in \operatorname{Red}_<(P)} \#\left((m + P_{\text{surj}} - P) \cap \operatorname{Red}_<(P_{\text{surj}})\right).$$

Gavin Brown and Alexander M. Kasprzyk.
Seven new champion linear codes.
Lms Journal of Computation and Mathematics, 16:109–117, 2013.

Cicero Carvalho and Victor G. L. Neumann.
Projective Reed-Muller type codes on rational normal scrolls.
Finite Fields Appl., 37:85–107, 2016.

Johan P. Hansen.
Toric varieties Hirzebruch surfaces and error-correcting codes.
Appl. Algebra Engrg. Comm. Comput., 13(4):289–300, 2002.

Johan P. Hansen.
Secret sharing schemes with strong multiplication and a large number of players from toric varieties.
Contemporary Mathematics, 03 2016.

Julien Lavauzelle and Jade Nardi.
Weighted lifted codes: Local correctabilities and application to robust private information retrieval.
IEEE Transactions on Information Theory, pages 1–1, 2020.

John Little and Ryan Schwarz.
On m-dimensional toric codes, 2005.

Jade Nardi.
Algebraic geometric codes on minimal hirzebruch surfaces.
Journal of Algebra, 535:556 – 597, 2019.

Diego Ruano.
On the parameters of r-dimensional toric codes.
Finite Fields Appl., 13(4):962–976, 2007.

Ivan Soprunov and Jenya Soprunova.
Toric surface codes and Minkowski length of polygons.
SIAM J. Discrete Math., 23(1):384–400, 2008/09.

Steven I Sperber and John Voight.
Computing zeta functions of nondegenerate hypersurfaces with few monomials.
Lms Journal of Computation and Mathematics, 16:9–44, 2013.