Explicit construction and parameters of projective toric codes

Jade Nardi

JC2
November, 2020

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

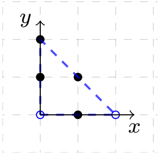
Classical toric code: Span of the evaluation on $(\mathbb{F}_q^*)^2$ of monomials

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

HOMOGENISATION: choose variety & degree

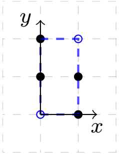
2 on $\mathbb{P}^2$ $[X, Y, Z]$

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



$(1,2)$ 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

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

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

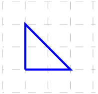
$(a, b) \in \mathbb{F}_q^2$

Polygon $\leftrightarrow$ variety & degree

Classical/Projective toric codes

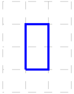
An integral polytope $P \subset \mathbb{R}^N$ (vertices in $\mathbb{Z}^N$) defines an abstract toric variety $\mathbf{X}_P$ with a divisor D and a monomial basis of $L(D)$ (set of polynomials of a certain *degree*).

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



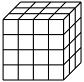
$\mathbb{P}^2$

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 $\rightarrow$ PRM:

1. length $\nearrow$, minimum distance $\nearrow$ with roughly the same dimension.
2. Strenghten the geometric interpretation

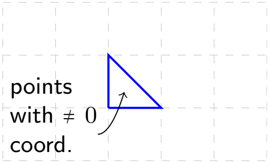
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

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

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 $\mathbb{P}^2$



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

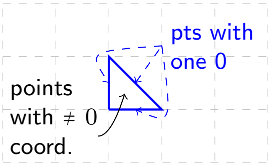
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

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

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 $\mathbb{P}^2$



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

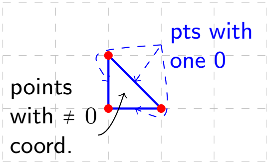
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

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

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 $\mathbb{P}^2$



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

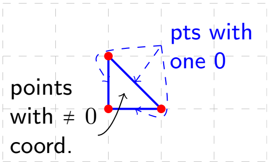
The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$ with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q}$

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

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

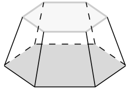
$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^N + \sum_{i=0}^{N-1} (\text{nb of } i\text{-dim faces}) \times (q-1)^i.$$

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

$\overbrace{}^{\substack{(q-1)^2 \text{ torus points} \\ (a,b,1)}}$ $\overbrace{\underbrace{}_{\substack{q-1\\\text{points}}} \ \ldots \ \ldots}^{\substack{(1,a,0),\ (1,0,a),\ (0,1,a) \\ r \text{ edges}}}$ $\overbrace{}^{\substack{(1,0,0)\\(0,1,0)\\(0,0,1)\\ r \text{ vertices}}}$

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

$m \in F_1^\circ$ — 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 $(N = 2)$

Q° = interior of the face Q

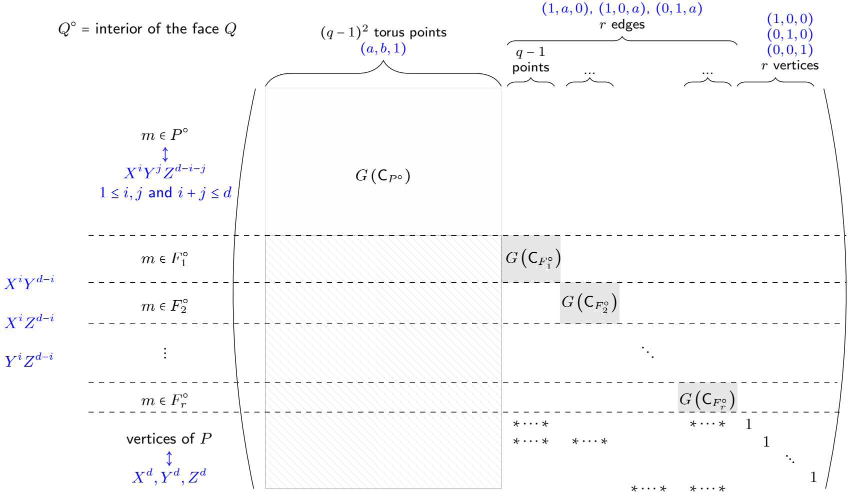


Figure: "Generator" matrix of PC_P when P is a polygon $(N = 2)$

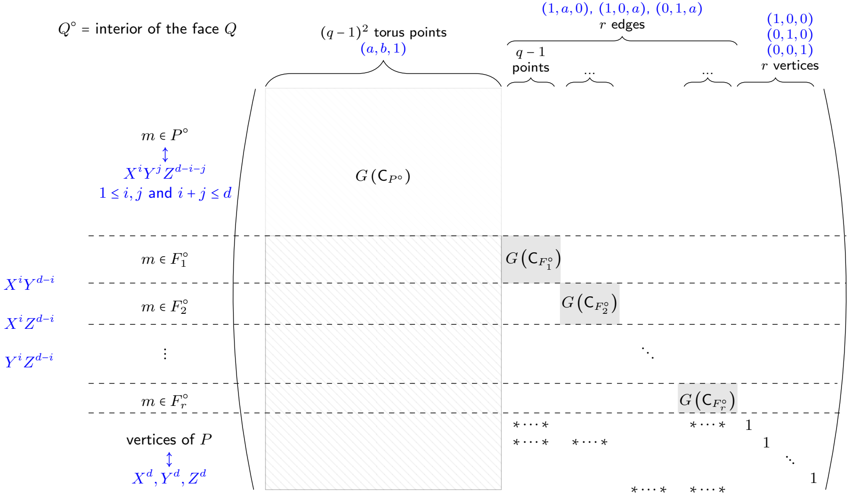


Figure: "Generator" matrix of PC_P when P is a polygon $(N = 2)$

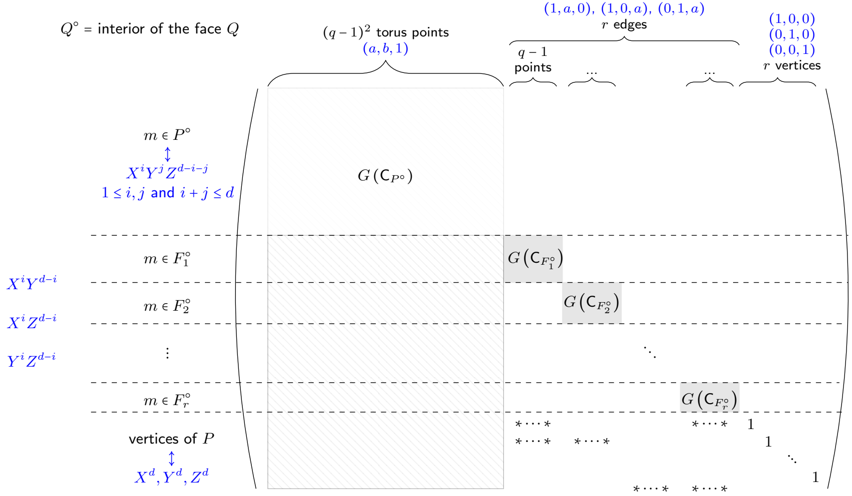


Figure: "Generator" matrix of PC_P when P is a polygon $(N=2)$

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 = $\sum_Q \dim \mathsf{C}_{Q^\circ}$

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).

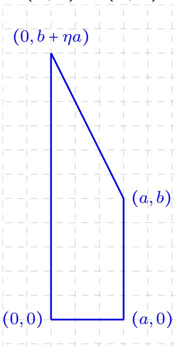
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

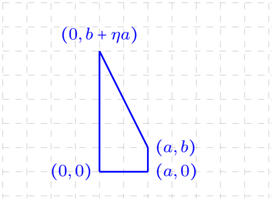
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

↳ 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 $P(\eta) = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
$\to \mathbf{X}_{P(\eta)}$ called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).

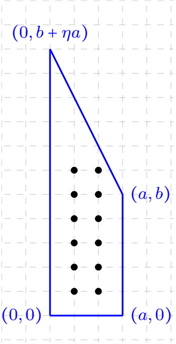
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

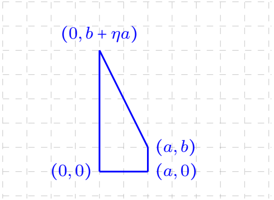
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

↳ 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).

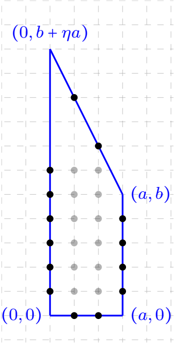
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ Reduce P modulo $q-1=6$.

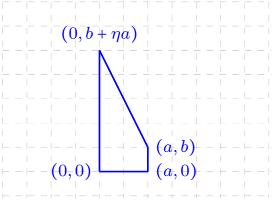
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).

↳ 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).

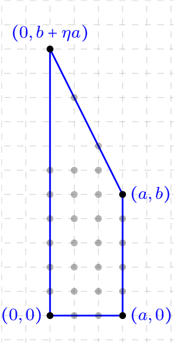
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ 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).

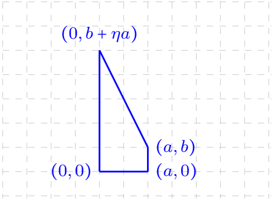
↳ Reduce the interior of each face modulo $q-1=6$.

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



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

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



Example of computation of the dimension of PC_P and C_P

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

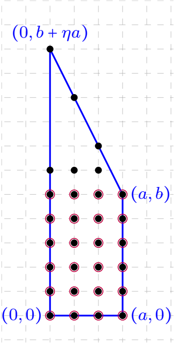
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ 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).

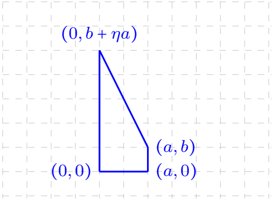
↳ Reduce the interior of each face modulo $q-1=6$.

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



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

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



Example of computation of the dimension of PC_P and C_P

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

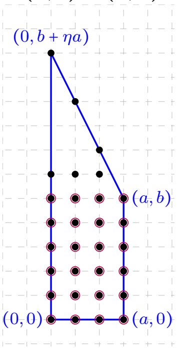
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ 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).

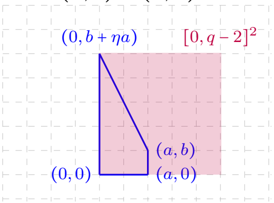
↳ Reduce the interior of each face modulo $q-1=6$.

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



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

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



Example of computation of the dimension of PC_P and C_P

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

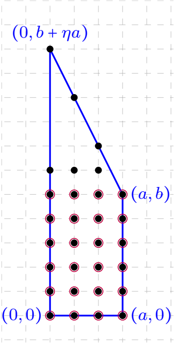
$$\mathbf{X}_{P(\eta)}(\mathbb{F}_q) = (q-1)^2 + 4(q-1) + 4 = (q+1)^2.$$

↱ 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).

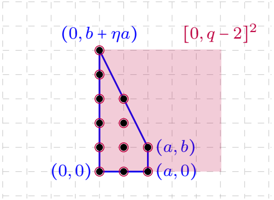
↳ Reduce the interior of each face modulo $q-1=6$.

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



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

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



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

Minimum distance

Lower bound on the minimum distance of PC_P more technical [CN16, Nar19]
Key ingredient: Gröbner basis of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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** (No complexity result).

Minimum distance

Lower bound on the minimum distance of PC_P more technical [CN16, Nar19]
Key ingredient: Gröbner basis of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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** (No complexity result).

What now? Investigate properties of these codes

- Local decodability
- Dual codes for application to secret sharing [Han16]

Thank you!

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.

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.