Explicit construction and parameters of projective toric codes

Jade Nardi

March 27, 2020

Inria by teleworking

Context

Take a polytope $P \subset \mathbb{R}^N$ with **integral vertices** (= convex hull of integer points)

Classical toric codes introduced by Hansen: Evaluating monomials $x_1^{m_1} x_2^{m_2} \ldots x_n^{m_N}$ at points $(x_1, \ldots, x_N) \in (\mathbb{F}_q^*)^N$ where $m \in P \cap \mathbb{Z}^N$.
→ Well-known parameters [Hansen, Little, Soprunov-Soprunova, Ruano].

Toric codes are **algebraic-geometric codes**:
P defines a *toric variety* $\mathbf{X}_P$ and a *divisor* D.
Toric code = evaluating every $f \in L(D)$ at **some** of the rational points of $\mathbf{X}_P$.

Context

Take a polytope $P \subset \mathbb{R}^N$ with **integral vertices** (= convex hull of integer points)

Classical toric codes introduced by Hansen: Evaluating monomials $x_1^{m_1} x_2^{m_2} \dots x_n^{m_N}$ at points $(x_1, \dots, x_N) \in (\mathbb{F}_q^*)^N$ where $m \in P \cap \mathbb{Z}^N$.
→ Well-known parameters [Hansen, Little, Soprunov-Soprunova, Ruano].

Toric codes are **algebraic-geometric codes**:
P defines a *toric variety* $\mathbf{X}_P$ and a *divisor* D.
Toric code = evaluating every $f \in L(D)$ at **some** of the rational points of $\mathbf{X}_P$.

Aim: evaluating these fonctions on the **whole** variety.
Similar to going from Reed-Muller codes to **projective** Reed-Muller codes
Advantages:

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

Main obstacle: Describe $\mathbf{X}_P$ and its $\mathbb{F}_q$-points to make the evaluation meaningful and *workable*

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

P integral polytope of dimension N → toric variety $\mathbf{X}_P$ of dimension N
Several ways to describe $\mathbf{X}_P$: *(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

P integral polytope of dimension N → toric variety $\mathbf{X}_P$ of dimension N
Several ways to describe $\mathbf{X}_P$: *(under some assumptions)*

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

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

P integral polytope of dimension $N \to$ toric variety $\mathbf{X}_P$ of dimension N
Several ways to describe $\mathbf{X}_P$: *(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
  - $\oplus$ 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

P integral polytope of dimension N → toric variety $\mathbf{X}_P$ of dimension N

Several ways to describe $\mathbf{X}_P$: *(under some assumptions)*

- with *fans* as an abstract variety
  - ⊕ geometric properties
  - ⊖ implementation
- embedded into $\mathbb{P}^{\#\left(P\cap\mathbb{Z}^N\right)-1}$
  - ⊕ practical description
  - ⊖ very large ambiant
- as a quotient of a subset of $\mathbb{A}^r$ (where $r =$ nb of facets of P) by a group G
  - ⊕ more reasonable ambient
  - ⊕ 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: $(x_0, x_1, y_0, y_1) \mapsto (x_i y_j)$,
- 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 $\chi^{\langle m,P\rangle} \in \mathbb{F}_\mathbf{q}[\mathbf{X_1}, \dots, \mathbf{X_r}]$.

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

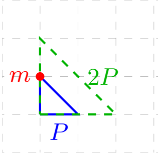
We can go from χ^m to $\chi\langle m, P\rangle$ via **homogenization** process.

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 $\mathbb{P}^2$:



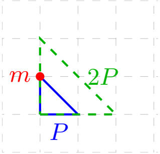
- $\chi^m = x_1^0 x_2^1 = x_2$.
- $\chi^{\langle m,P \rangle} = X_2 \leftarrow$ homogenize in degree 1
- $\chi^{\langle m,2P \rangle} = X_0 X_2 \leftarrow$ homogenize in degree 2

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 $\mathbb{P}^2$:



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

Definition (Projective toric code)

Let P be a lattice polytope, $(\mathbf{X}_P, D)$ its corresponding toric variety and divisor. Choose a set $\mathcal{P}$ of representatives of $\mathbf{X}_P(\mathbb{F}_q)$. The *projective toric code* PC_P is defined as the image of

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

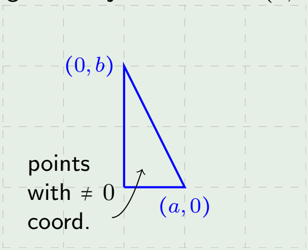
where $n = \#\mathbf{X}_P(\mathbb{F}_q)$.

The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$

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

Examples

Weighted Projective Plane $\mathbb{P}(1,a,b)$



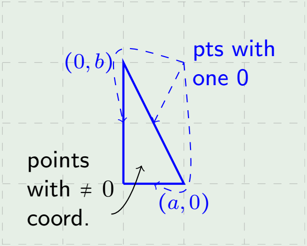
$\#\mathbb{P}(1,a,b)(\mathbb{F}_q) = (q-1)^2$

The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$

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

Examples

Weighted Projective Plane $\mathbb{P}(1,a,b)$



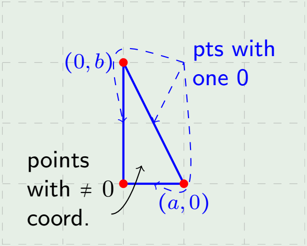
$\#\mathbb{P}(1,a,b)(\mathbb{F}_q) = (q-1)^2 + 3(q-1)$

The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$

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

Examples

Weighted Projective Plane $\mathbb{P}(1,a,b)$

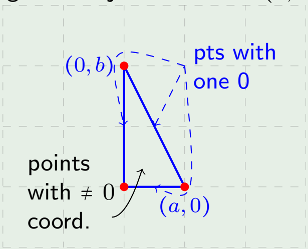


$\#\mathbb{P}(1,a,b)(\mathbb{F}_q) = (q-1)^2 + 3(q-1) + 3$

The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$
with $\mathbb{T}_Q = (\overline{\mathbb{F}_q}^*)^{\dim Q} \Rightarrow \#\mathbb{T}_Q(\mathbb{F}_q) = (q-1)^{\dim Q}$.

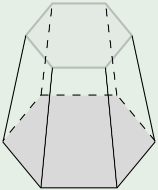
Examples

Weighted Projective Plane $\mathbb{P}(1,a,b)$



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

A random toric 3-fold



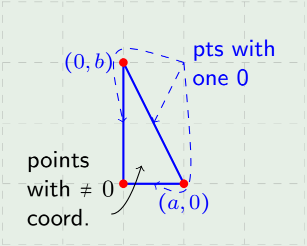
$$\#\mathbf{X}_P(\mathbb{F}_q) = (q-1)^3 + 8(q-1)^2 + 18(q-1) + 12$$

The variety $\mathbf{X}_P$ is the disjoint union of tori : $\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$

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

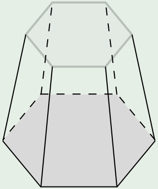
Examples

Weighted Projective Plane $\mathbb{P}(1,a,b)$



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

A random toric 3-fold



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

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

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

Evaluation

$$\mathbf{X}_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$$

What does a codeword of PC_P look like when restricting on points of a torus $\mathbb{T}_Q$?

Recall: Integral point $m \in P \cap \mathbb{Z}^N \leftrightarrow$ Monomial $\chi^{\langle m,P\rangle} \in L(D)$

Lemma

- If $m \in Q$, $\chi^{\langle m,P\rangle}(\mathbf{x}) \neq 0 \iff \mathbf{x} \in \mathbb{T}_Q$,
- For any face Q of P, the puncturing of the code PC_P at coordinates corresponding to points of outside $\mathbb{T}_Q$ is monomially equivalent to the classical toric code C_Q.

For a face Q of P, puncturing of PC_P outside $\mathbb{T}_Q \simeq \mathrm{C}_Q$.

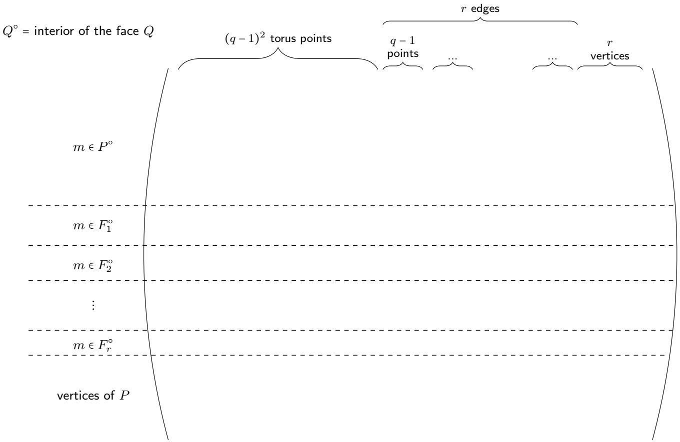


Figure: Matrix of the evaluation map associated to a polygon P $(N = 2)$

For a face Q of P, puncturing of PC_P outside $\mathbb{T}_Q \simeq \mathrm{C}_Q$.

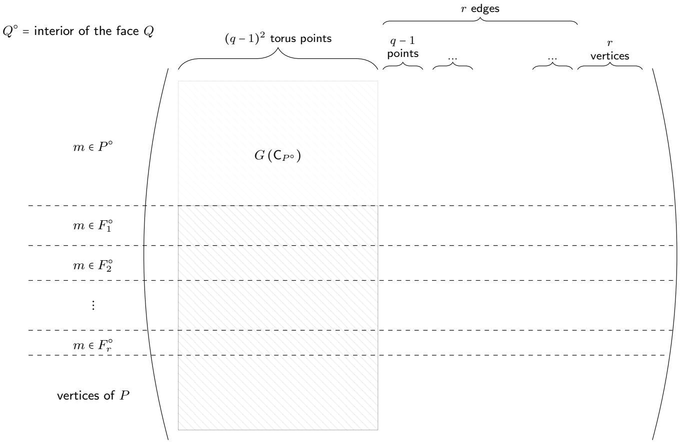


Figure: Matrix of the evaluation map associated to a polygon P $(N = 2)$

For a face Q of P, puncturing of PC_P outside $\mathbb{T}_Q \simeq \mathrm{C}_Q$.

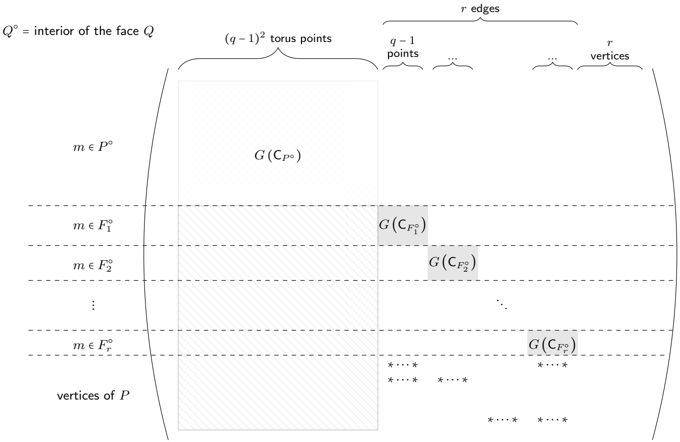


Figure: Matrix of the evaluation map associated to a polygon P $(N = 2)$

For a face Q of P, puncturing of PC_P outside $\mathbb{T}_Q \simeq \mathrm{C}_Q$.

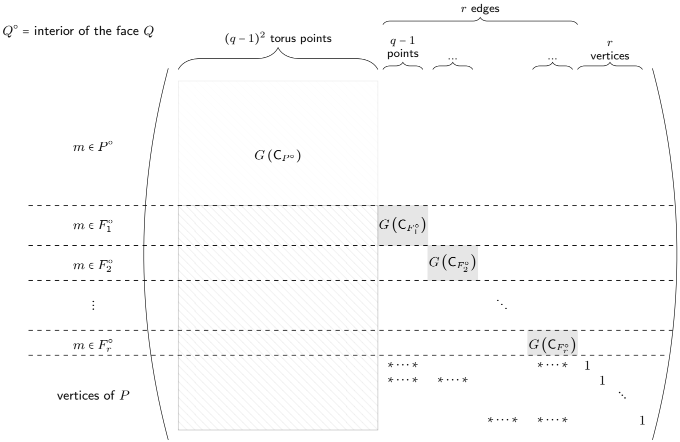


Figure: Matrix of the evaluation map associated to a polygon P ($N = 2$)

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

Dimension and reduction modulo $q-1$

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

Dimension of classical toric codes

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]

Let $\overline{P}$ be a set of representatives of $P \cap \mathbb{Z}^N$ under $\sim$. Then

- $\chi^m(\mathbf{t}) = \chi^{m'}(\mathbf{t})$ for every $\mathbf{t} \in (\mathbb{F}_q^*)^N \Leftrightarrow m \sim m'$,
- $\left\{(\chi^{\overline{m}}(\mathbf{t}),\ \mathbf{t} \in (\mathbb{F}_q^*)^N) \mid \overline{m} \in \overline{P}\right\}$ is a basis of C_P.

Dimension and reduction modulo $q-1$

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

Dimension of classical toric codes

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]

Let $\overline{P}$ be a set of representatives of $P \cap \mathbb{Z}^N$ under $\sim$. Then

- $\chi^m(\mathbf{t}) = \chi^{m'}(\mathbf{t})$ for every $\mathbf{t} \in (\mathbb{F}_q^*)^N \Leftrightarrow m \sim m'$,
- $\left\{(\chi^{\overline{m}}(\mathbf{t}),\, \mathbf{t} \in (\mathbb{F}_q^*)^N) \mid \overline{m} \in \overline{P}\right\}$ is a basis of C_P.

In the projective case, the polytope P is reduced modulo $q-1$ **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]

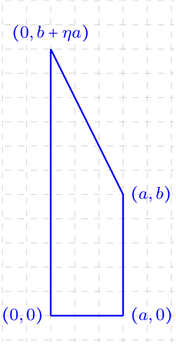
Let $\mathrm{Red}(P)$ be a set of representatives of $P \cap \mathbb{Z}^N$ modulo $\sim_P$. Then

- $\ker \mathrm{ev}_P = \mathrm{Span}\{\chi^m - \chi^{m'} : m \sim_P m'\}$,
- $\left\{\mathrm{ev}_P(\chi^{\langle \overline{m}, P\rangle}) \mid \overline{m} \in \mathrm{Red}(P)\right\}$ is a basis of PC_P.

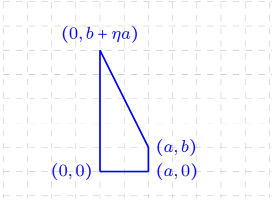
Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
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 $q-1=6$.

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



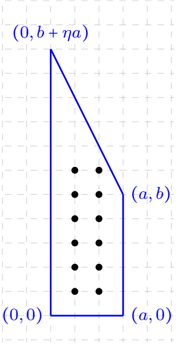
$(a,b)=(2,1)$



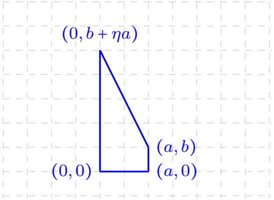
Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
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 $q-1=6$.

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



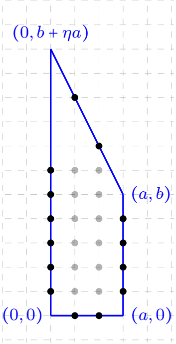
$(a,b)=(2,1)$



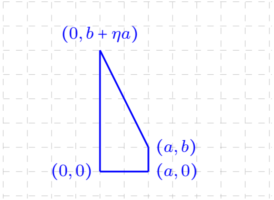
Example of computation of the dimension of PC_P and C_P

Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
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 $q-1=6$.

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



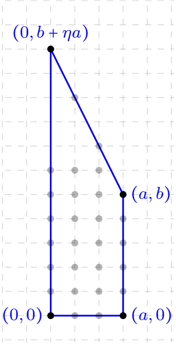
$(a,b)=(2,1)$



Example of computation of the dimension of PC_P and C_P

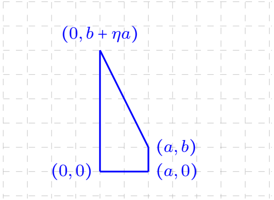
Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).
→ Reduce the interior of each face modulo $q-1=6$.

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



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

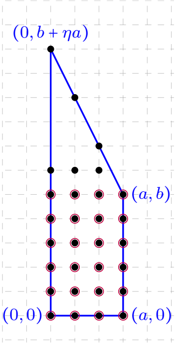
$(a,b)=(2,1)$



Example of computation of the dimension of PC_P and C_P

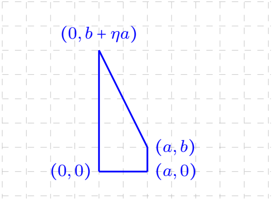
Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).
→ Reduce the interior of each face modulo $q-1=6$.

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



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

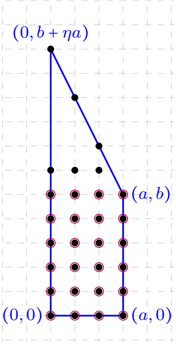
$(a,b)=(2,1)$



Example of computation of the dimension of PC_P and C_P

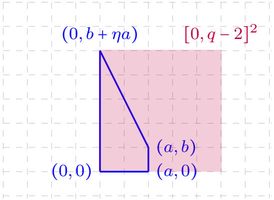
Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).
→ Reduce the interior of each face modulo $q-1=6$.

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



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

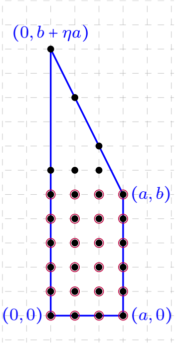
$(a,b)=(2,1)$



Example of computation of the dimension of PC_P and C_P

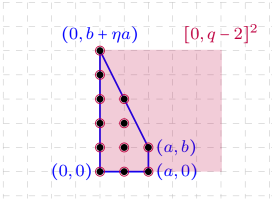
Let a, b, $\eta \in \mathbb{N}^*$ and $P = \mathrm{Conv}((0,0),(a,0),(a,b),(0,b+\eta a))$.
→ Toric surface parametrized by the integer η called a *Hirzebruch surface* + a divisor of *bidegree* (a,b).
Let us compare the $\dim \mathsf{PC}_P$ and $\dim \mathsf{C}_P$ on $\mathbb{F}_7$ for different (a,b).
→ Reduce the interior of each face modulo $q-1=6$.

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



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

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

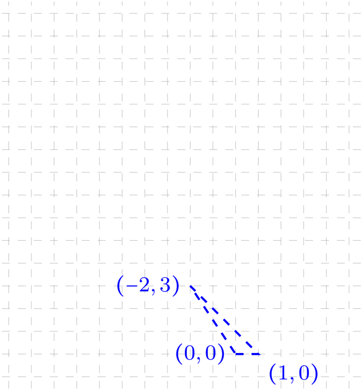


$\dim \mathsf{PC}_P = \dim \mathsf{C}_P = \#P \cap \mathbb{Z}^2 = 12$

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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 $\sim_{(\lambda)P}$



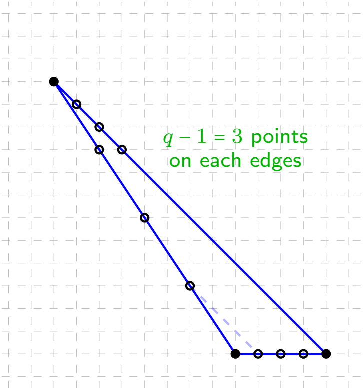
Theorem [N. 20]

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

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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 $\sim_{(\lambda)P}$



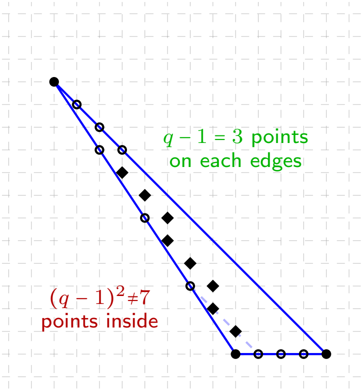
Theorem [N. 20]

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

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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 $\sim_{(\lambda)P}$



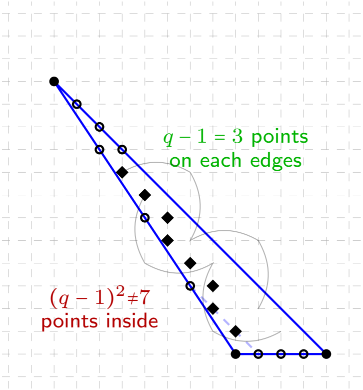
Theorem [N. 20]

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

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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.* $\mathsf{PC}_{\lambda P} = \mathbb{F}_q^n$) $\lambda = 4$?
3. Compute $\mathrm{Red}(P)$ and $\mathrm{Red}(\lambda P)$ **taking into account the order**. Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$



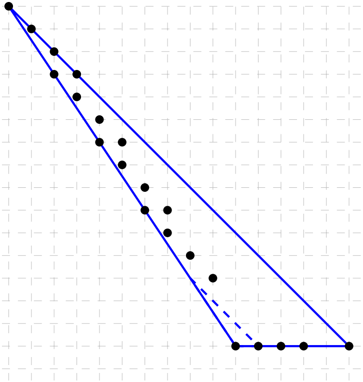
Theorem [N. 20]

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

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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 $\sim_{(\lambda)P}$



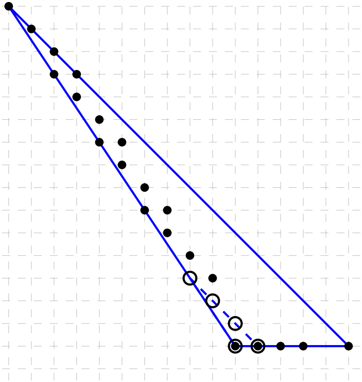
Theorem [N. 20]

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

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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 $\sim_{(\lambda)P}$



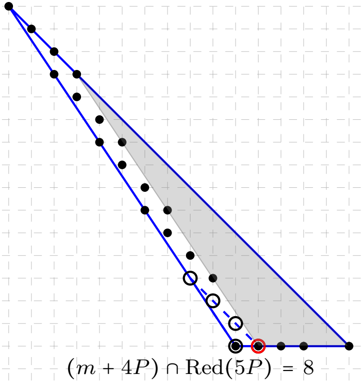
Theorem [N. 20]

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

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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]

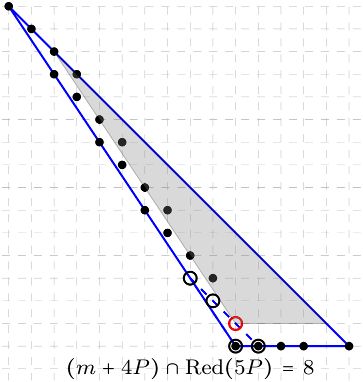
$$d(\mathrm{PC}_P) \geq \min_{m \in \mathrm{Red}_<(P)} \#\left((m + P_{\mathrm{surj}} - P) \cap \mathrm{Red}_<(P_{\mathrm{surj}})\right).$$

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

SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $\mathbf{X}_P(\mathbb{F}_q)$

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 $\sim_{(\lambda)P}$

   → PC_P has type $[21, 4, 8]$



Theorem [N. 20]

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

Conclusion

Given a polytope P, we can

- compute exactly the dimension of the code PC_P,
- get a lowerbound on the minimum distance,

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

$\ominus$ Lower on the minimum distance is not always sharp
$\ominus$ No complexity result

Conclusion

Given a polytope P, we can

- compute exactly the dimension of the code PC_P,
- get a lowerbound on the minimum distance,

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

$\ominus$ Lower on the minimum distance is not always sharp
$\ominus$ No complexity result

What now?

- Investigate properties of these codes (local decodability, dual codes)
- Application to secret sharing, generalizing one based on classical toric codes by Hansen

Thank you!