Explicit construction and parameters of projective toric codes

Jade Nardi

March 27, 2020

by teleworking
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 $X_P$ and a divisor $D$.

Toric code $=$ evaluating every $f \in L(D)$ at some of the rational points of $X_P$. 
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 $X_P$ and a divisor $D$.

Toric code = evaluating every $f \in L(D)$ at some of the rational points of $X_P$.

Aim: evaluating these functions 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. Strengthen the geometric interpretation

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

Explicit construction and parameters of projective toric codes

Jade Nardi
Description of the toric variety $X_P$ associated to the polytope $P$

$P$ integral polytope of dimension $N \rightarrow$ toric variety $X_P$ of dimension $N$

Several ways to describe $X_P$: (*under some assumptions*)

- with *fans* as an abstract variety
- geometric properties
- implementation

Example:

$P = \text{Conv}((0,0), (1,0), (0,1), (1,1)) \subset \mathbb{R}^2$ gives $X_P = P_1 \times P_1$:

- embedded in $P_3$ by the Segre map: $(x_0, x_1, y_0, y_1)/\text{uni21A6}(x_i, y_j)$
- defined as the quotient of $A_2/\{ (0,0) \}$ by the group $(\overline{F^*})_2$ 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
Description of the toric variety $X_P$ associated to the polytope $P$

$P$ integral polytope of dimension $N \rightarrow$ toric variety $X_P$ of dimension $N$

Several ways to describe $X_P$: (under some assumptions)

- with fans as an abstract variety  
  + geometric properties
  - implementation

- embedded into $\mathbb{P}^\#(P \cap \mathbb{Z}^N) - 1$  
  + practical description
  - very large ambient

Explicit construction and parameters of projective toric codes Jade Nardi
Description of the toric variety $X_P$ associated to the polytope $P$

$P$ integral polytope of dimension $N \rightarrow$ toric variety $X_P$ of dimension $N$

Several ways to describe $X_P$: (*under some assumptions*)

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

$P$ integral polytope of dimension $N \to$ toric variety $X_P$ of dimension $N$

Several ways to describe $X_P$: *(under some assumptions)*

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

**Example**: $P = \text{Conv}((0,0), (1,0), (0,1), (1,1)) \subset \mathbb{R}^2$ gives $X_P = \mathbb{P}^1 \times \mathbb{P}^1$:

- **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** $(\mathbb{A}^2 \setminus \{0,0\})^2 \subset \mathbb{A}^4$ by the group $(\overline{\mathbb{F}}^*)^2$ 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
\[ \chi^m = X_1^{m_1} \cdots X_N^{m_N}. \]
In the projective case, it corresponds to a monomial $\chi^{(m,P)} \in \mathbb{F}_q[X_1, \ldots, X_r].$

\[ L(D) = \text{Span} \left( \chi^{(m,P)} \mid m \in P \cap \mathbb{Z}^N \right) \]

We can go from $\chi^m$ to $\chi^{(m,P)}$ via \textbf{homogenization} process.
For classical toric codes, an integral point \( m \in P \cap \mathbb{Z}^N \) gives a monomial \( \chi^m = X_1^{m_1} \ldots X_N^{m_N} \).

In the projective case, it corresponds to a monomial \( \chi^{(m, P)} \in \mathbb{F}_q[X_1, \ldots, X_r] \).

\[
L(D) = \text{Span} \left( \chi^{(m, P)} \mid m \in P \cap \mathbb{Z}^N \right)
\]

We can go from \( \chi^m \) to \( \chi^{(m, P)} \) via \textit{homogenization} process.

\textit{Example on} \( \mathbb{P}^2 \):

- \( \chi^m = x_1^0 x_2^1 = x_2 \).
- \( \chi^{(m, P)} = X_2 \leftarrow \text{homogenize in degree 1} \)
- \( \chi^{(m, 2P)} = X_0 X_2 \leftarrow \text{homogenize in degree 2} \)
For classical toric codes, an integral point \( m \in P \cap \mathbb{Z}^N \) gives a monomial \( \chi^m = X_1^{m_1} \cdots X_N^{m_N} \).

In the projective case, it corresponds to a monomial \( \chi^{(m,P)} \in \mathbb{F}_q[X_1, \ldots, X_r] \).

\[
L(D) = \text{Span} \left( \chi^{(m,P)} \mid m \in P \cap \mathbb{Z}^N \right)
\]

We can go from \( \chi^m \) to \( \chi^{(m,P)} \) via homogenization process.

**Example on \( \mathbb{P}^2 \):**

- \( \chi^m = x_1^0 x_2^1 = x_2 \).
- \( \chi^{(m,P)} = X_2 \leftarrow \text{homogenize in degree 1} \)
- \( \chi^{(m,2P)} = X_0 X_2 \leftarrow \text{homogenize in degree 2} \)

**Definition (Projective toric code)**

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

\[
PC_P = \text{Span} \left\{ \left( \chi^{(m,D)}(x) \right)_{x \in \mathcal{P}} \in \mathbb{F}_q^n, \ m \in P \cap \mathbb{Z}^N \right\}
\]

where \( n = \#X_P(\mathbb{F}_q) \).
The variety $X_P$ is the disjoint union of tori: $X_P = \bigsqcup Q T_Q^Q$ with $T_Q = (\mathbb{F}_q^*)^{\dim Q} \Rightarrow \#T_Q(\mathbb{F}_q) = (q - 1)^{\dim Q}$.

### Examples

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

$\#\mathbb{P}(1, a, b)(\mathbb{F}_q) = (q - 1)^2$
The variety $X_P$ is the disjoint union of tori: 
$$X_P = \bigsqcup_{Q \text{ faces of } P} T_Q$$
with $T_Q = (\mathbb{F}_q^*)^\dim Q \Rightarrow \# T_Q(\mathbb{F}_q) = (q - 1)^\dim Q$.

**Examples**

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

Number of \(\mathbb{F}_q\)-points of \(X_P\)
\[
\# \mathbb{P}(1, a, b)(\mathbb{F}_q) = (q-1)^2 + 3(q-1)
\]
The variety $X_P$ is the disjoint union of tori: $X_P = \bigsqcup_{Q \text{ faces of } P} T_Q$

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

**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 $X_P$ is the disjoint union of tori: $X_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$

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

**Examples**

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

Points with $\neq 0$ coord. 

$(0, b)$ pts with one 0

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

**A random toric 3-fold**

$\# X_P(\mathbb{F}_q) = (q - 1)^3 + 8(q - 1)^2 + 18(q - 1) + 12$
The variety $X_P$ is the disjoint union of tori: $X_P = \bigsqcup_{Q \text{ faces of } P} \mathbb{T}_Q$

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

**Examples**

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

- Points with $\neq 0$ coord.
- Points with one 0

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

**A random toric 3-fold**

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

**Number of $\mathbb{F}_q$-points of $X_P$**

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

Explicit construction and parameters of projective toric codes Jade Nardi
\[ X_P = \bigcup_{Q \text{ faces of } P} T_Q \]

What does a codeword of PC_P look like when restricting on points of a torus \( T_Q \)?

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

**Lemma**

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

$Q^\circ = \text{interior of the face } Q$

$m \in P^\circ$

$m \in F_1^\circ$

$m \in F_2^\circ$

$\vdots$

$m \in F_r^\circ$

vertices of $P$

$(q - 1)^2$ torus points

$q - 1$ points

$\ldots$

$\ldots$

$r$ edges

$r$ vertices

Figure: Matrix of the evaluation map associated to a polygon $P$ ($N = 2$)
For a face $Q$ of $P$, puncturing of $PC_P$ outside $\mathbb{T}_Q \simeq C_Q$.

$Q^o = \text{interior of the face } Q$

$(q - 1)^2$ torus points

$r$ edges

$q - 1$ points

... ... $r$ vertices

$m \in P^o$

$m \in F_1^o$

$m \in F_2^o$

...vertices of $P$

$G(C_P^o)$

Figure: Matrix of the evaluation map associated to a polygon $P$ ($N = 2$)
For a face $Q$ of $P$, puncturing of $PC_P$ outside $T_Q \cong C_Q$.

$Q^o = \text{interior of the face } Q$

$(q - 1)^2 \text{ torus points}$

$r \text{ edges}$

$q - 1 \text{ points}$

$\ldots$

$\ldots$

$r \text{ vertices}$

Figure: Matrix of the evaluation map associated to a polygon $P$ ($N = 2$)
For a face $Q$ of $P$, puncturing of $\mathbb{P}C_P$ outside $\mathbb{T}_Q \simeq C_Q$.

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

For any polytope $P$, there is a generator matrix of $\mathbb{P}C_P$ with such a triangular block structure.
Dimension and reduction modulo $q - 1$

Dimension of $PC_P = \text{rank of the previous matrix}$

$$= \sum_Q \dim C_Q^\circ$$

**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

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

Explicit construction and parameters of projective toric codes Jade Nardi
Handling a toric variety

**Dimension and reduction modulo** $q-1$

Dimension of $PC_P = \text{rank of the previous matrix} = \sum_Q \dim C_{Q^\circ}$

**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

- $\chi^m(t) = \chi^{m'}(t)$ for every $t \in (\mathbb{F}_q^*)^N \Leftrightarrow m \sim m'$,
- $\{(\chi^\overline{m}(t), t \in (\mathbb{F}_q^*)^N) \mid \overline{m} \in \overline{P}\}$ 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 $\text{Red}(P)$ be a set of representatives of $P \cap \mathbb{Z}^N$ modulo $\sim_P$. Then

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

Explicit construction and parameters of projective toric codes Jade Nardi
Example of computation of the dimension of $\mathbb{PC}_P$ and $\mathbb{C}_P$

Let $a$, $b$, $\eta \in \mathbb{N}^*$ and $P = \text{Conv}((0,0), (a,0), (a,b), (0,b + \eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a \textit{Hirzebruch surface} + a divisor of \textit{bidegree} $(a,b)$.

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

$\rightarrow$ 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 $\text{PC}_P$ and $C_P$

Let $a$, $b$, $\eta \in \mathbb{N}^*$ and $P = \text{Conv}((0,0), (a,0), (a,b), (0,b+\eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a *Hirzebruch surface* $+$ a divisor of bidegree $(a,b)$.

Let us compare the $\dim \text{PC}_P$ and $\dim C_P$ 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 $P = \text{Conv}((0, 0), (a, 0), (a, b), (0, b + \eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a *Hirzebruch surface* + a divisor of *bidegree* $(a, b)$.

Let us compare the $\dim PC_P$ and $\dim C_P$ 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 $P = \text{Conv}((0, 0), (a, 0), (a, b), (0, b + \eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a Hirzebruch surface + a divisor of bidegree $(a, b)$.

Let us compare the $\dim PC_P$ and $\dim C_P$ on $\mathbb{F}_7$ for different $(a, b)$.

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

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

$$
\dim PC_P = 30
$$

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

Explicit construction and parameters of projective toric codes Jade Nardi
Example of computation of the dimension of $PC_P$ and $C_P$

Let $a, b, \eta \in \mathbb{N}^*$ and $P = \text{Conv}((0,0), (a,0), (a,b), (0,b+\eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a *Hirzebruch surface* + a divisor of bidegree $(a,b)$.

Let us compare the $\dim PC_P$ and $\dim C_P$ on $\mathbb{F}_7$ for different $(a,b)$.

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

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

$\dim PC_P = 30 > \dim C_P = 24$
Example of computation of the dimension of $PC_P$ and $C_P$

Let $a, b, \eta \in \mathbb{N}^*$ and $P = \text{Conv}((0, 0), (a, 0), (a, b), (0, b + \eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a \textit{Hirzebruch surface} + a divisor of \textit{bidegree} $(a, b)$.

Let us compare the $\dim PC_P$ and $\dim C_P$ on $\mathbb{F}_7$ for different $(a, b)$.

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

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

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

$\dim PC_P = 30 > \dim C_P = 24$
Example of computation of the dimension of $PC_P$ and $C_P$

Let $a, b, \eta \in \mathbb{N}^*$ and $P = \text{Conv}((0, 0), (a, 0), (a, b), (0, b + \eta a))$.

→ Toric surface parametrized by the integer $\eta$ called a *Hirzebruch surface* $+ a$ divisor of *bidegree* $(a, b)$.

Let us compare the $\dim PC_P$ and $\dim C_P$ on $\mathbb{F}_7$ for different $(a, b)$.

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

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

$\dim PC_P = 30 > \dim C_P = 24$

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

$\dim PC_P = \dim C_P = \#P \cap \mathbb{Z}^2 = 12$
Lowerbound on the minimum distance on a toy example on $\mathbb{F}_4$

**Secret ingredient:** *Gröbner basis* of the vanishing ideal of $X_P(\mathbb{F}_q)$

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility) : lexicographic

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$,
   $\#\text{Red}(Q^\circ) = (q - 1)^{\dim Q}$
   (*i.e.* $PC_{\lambda P} = \mathbb{F}_q^n$)

3. Compute $\text{Red}(P)$ and $\text{Red}(\lambda P)$ taking into account the order.
   Representative $=$ smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$

Theorem [N. 20]

$$d(PC_P) \geq \min_{m \in \text{Red}_<(P)} \#((m + P_{\text{surj}} - P) \cap \text{Red}_<(P_{\text{surj}})) .$$
SECRET INGREDIENT:  \textit{Gröbner basis} of the vanishing ideal of $X_P(\mathbb{F}_q)$

1. Choose a \textit{nice} total order $<$ on $\mathbb{Z}^N$ (addition compatibility): lexicographic.

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$, 
   $\# \text{Red}(Q^\circ) = (q-1)^{\dim Q}$
   (i.e. $PC_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 4$?

3. Compute Red($P$) and Red($\lambda P$) taking into account the order.
   Representative = smallest element wrt $<$ among a class modulo $\sim(\lambda)P$

Theorem [N. 20]

$$d(\text{PC}_P) \geq \min_{m \in \text{Red}_<(P)} \#((m + P_{\text{surj}} - P) \cap \text{Red}_<(P_{\text{surj}})) .$$
SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $X_P(\mathbb{F}_q)$

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility):
   lexicographic

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$,
   $\# \text{Red}(Q^\circ) = (q - 1)^{\dim Q}$
   (*i.e.* $PC_{\lambda P} = \mathbb{F}_q^n$)
   $\lambda = 4~?$

3. Compute $\text{Red}(P)$ and $\text{Red}(\lambda P)$
   taking into account the order.
   Representative = smallest element
   wrt $<$ among a class modulo $\sim_{\lambda P}$

Theorem [N. 20]

$$d(PC_P) \geq \min_{m \in \text{Red}_<(P)} \#((m + P_{\text{surj}} - P) \cap \text{Red}_<(P_{\text{surj}})).$$
**SECRET INGREDIENT:** \textit{Gröbner basis} of the vanishing ideal of $X_P(\mathbb{F}_q)$

1. Choose a \textit{nice} total order $<$ on $\mathbb{Z}^N$ (addition compatibility):
   lexicographic

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$,
   $\# \text{Red}(Q^\circ) = (q - 1)^{\dim Q}$
   \textit{(i.e. } PC_{\lambda P} = \mathbb{F}_q^n)\text{)
   $\lambda = 4$ ?

3. Compute $\text{Red}(P)$ and $\text{Red}(\lambda P)$ \textbf{taking into account the order}.
   Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$

---

**Theorem [N. 20]**

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

---

Explicit construction and parameters of projective toric codes

Jade Nardi
**SECRET INGREDIENT:** *Gröbner basis* of the vanishing ideal of $X_P(F_q)$

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility):
   lexicographic

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$,
   $\# \text{Red}(Q^\circ) = (q - 1)^{\dim Q}$
   (i.e. $PC_{\lambda P} = F_q^n$)
   $\lambda = 5$

3. Compute $\text{Red}(P)$ and $\text{Red}(\lambda P)$
   taking into account the order.
   Representative $=$ smallest element wrt $<$ among a class modulo $\sim_{(\lambda) P}$

---

**Theorem [N. 20]**

$$d(PC_P) \geq \min_{m \in \text{Red}_<(P)} \# ((m + P_{\text{surj}} - P) \cap \text{Red}_<(P_{\text{surj}})).$$
Secret ingredient: *Gröbner basis* of the vanishing ideal of $X_P(\mathbb{F}_q)$

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility):
   - lexicographic

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$,
   - $\# \text{Red}(Q^\circ) = (q - 1)^{\dim Q}$
   - (i.e. $PC_\lambda P = \mathbb{F}_q^n$)
   - $\lambda = 5$

3. Compute $\text{Red}(P)$ and $\text{Red}(\lambda P)$
   - taking into account the order.
   - Representative = smallest element wrt $<$ among a class modulo $\sim_{(\lambda) P}$

---

**Theorem [N. 20]**

$$d(PC_P) \geq \min_{m \in \text{Red}_<(P)} \# ((m + P_{\text{surj}} - P) \cap \text{Red}_<(P_{\text{surj}})).$$
SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $X_P(\mathbb{F}_q)$

1. Choose a *nice* total order $<$ on $\mathbb{Z}^N$ (addition compatibility): lexicographic

2. Find $\lambda$ s.t. for every face $Q$ of $\lambda P$,
   
   $\# \text{Red}(Q^\circ) = (q - 1)^\dim Q$

   (*i.e.* $PC_{\lambda P} = \mathbb{F}_q^n$)

   $\lambda = 5$

3. Compute $\text{Red}(P)$ and $\text{Red}(\lambda P)$ taking into account the order. Representative $=$ smallest element wrt $<$ among a class modulo $\sim_{(\lambda)P}$

Theorem [N. 20]

$$d(PC_P) \geq \min_{m \in \text{Red}_< (P)} \# ((m + P_{\text{surj}} - P) \cap \text{Red}_< (P_{\text{surj}})) .$$
SECRET INGREDIENT: *Gröbner basis* of the vanishing ideal of $X_P(\mathbb{F}_q)$

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

**Theorem [N. 20]**

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

Given a polytope $P$, we can

- compute exactly the dimension of the code $PC_P$,
- get a lower bound on the minimum distance,

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

- Lower on the minimum distance is not always sharp
- No complexity result

Explicit construction and parameters of projective toric codes Jade Nardi
Conclusion

Given a polytope $P$, we can

- compute exactly the dimension of the code $PC_P$,
- get a lower bound on the minimum distance,

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

- Lower on the minimum distance is not always sharp
- 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!