Self-dual codes from smooth Fano polytopes

AMS Meeting, Chicago IL

Ivan Soprunov

Cleveland State University

October 3, 2015

Motivation

Joint project with Pinar Celebi Demirarslan

- Apply methods/results of Newton Polytopes and Residues theory to Coding theory

Motivation

Joint project with Pinar Celebi Demirarslan

- Apply methods/results of Newton Polytopes and Residues theory to Coding theory
- Dual Codes:
  - generalize duality of $\mathcal{L}$- and Ω-constructions (Tsfasman et al) from curves to toric varieties
  - application: combinatorics of polytopes

Evaluation Codes

Let $\mathbb{K} = \mathbb{F}_q$, for q large enough.
Fix $S = \{p_1, \ldots, p_n\}$ in $(\mathbb{K}^*)^m$ (or in $\mathbb{K}^m$, or in $\mathbb{P}^m_{\mathbb{K}}$).
Fix $\mathcal{L}(A) =$ a space of m-variate polynomials over $\mathbb{K}$ with monomial exponents lying in $A \cap \mathbb{Z}^m$.

Evaluation Codes

Let $\mathbb{K} = \mathbb{F}_q$, for q large enough.
Fix $S = \{p_1, \ldots, p_n\}$ in $(\mathbb{K}^*)^m$ (or in $\mathbb{K}^m$, or in $\mathbb{P}^m_{\mathbb{K}}$).
Fix $\mathcal{L}(A)$ = a space of m-variate polynomials over $\mathbb{K}$ with monomial exponents lying in $A \cap \mathbb{Z}^m$.

Evaluation Map:

$$\mathrm{ev}_S : \mathcal{L}(A) \to \mathbb{K}^n \quad f \mapsto (f(p_1), \ldots, f(p_n))$$

Evaluation Code:

$$\mathcal{C}_{S,A} = \mathrm{ev}_S(\mathcal{L}(A))$$

Examples: Reed–Solomon codes, Reed–Muller codes, AG codes, Toric codes, etc.

What is S for TCI codes?

Let $f_1,\dots,f_d \in \mathbb{K}[t_1^{\pm 1},\dots,t_d^{\pm 1}]$ with Newton polytopes $P_1,\dots,P_d$ and

$$S = \{p \in (\bar{\mathbb{K}}^*)^n \mid f_1(p) = \cdots = f_d(p) = 0\},$$

a toric complete intersection, that is ...

What is S for TCI codes?

Let $f_1, \ldots, f_d \in \mathbb{K}[t_1^{\pm 1}, \ldots, t_d^{\pm 1}]$ with Newton polytopes $P_1, \ldots, P_d$ and

$$S = \{p \in (\bar{\mathbb{K}}^*)^n \mid f_1(p) = \cdots = f_d(p) = 0\},$$

a toric complete intersection, that is ...

- $|S| = V(P_1, \ldots, P_m)$ (normalized mixed volume),
  i.e. BKK bound is attained
- $S \subseteq (\mathbb{K}^*)^m$

What is S for TCI codes?

Let $f_1, \dots, f_d \in \mathbb{K}[t_1^{\pm 1}, \dots, t_d^{\pm 1}]$ with Newton polytopes $P_1, \dots, P_d$ and

$$S = \{p \in (\bar{\mathbb{K}}^*)^n \mid f_1(p) = \cdots = f_d(p) = 0\},$$

a toric complete intersection, that is ...

- $|S| = V(P_1, \dots, P_m)$ (normalized mixed volume), i.e. BKK bound is attained
- $S \subseteq (\mathbb{K}^*)^m$

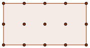
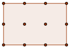
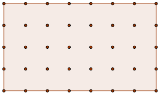
What is $\mathcal{L}(A)$ for TCI codes?

Choose $A \subseteq P^\circ = \text{interior}\,(P_1 + \cdots + P_d)$. Then

$$\mathcal{L}(A) = \text{span}_{\mathbb{K}}\{x^a \mid a \in A \cap \mathbb{Z}^m\}.$$

Example [Demirarslan–S., FFA'15]

Let $\mathbb{K} = \mathbb{F}_{16}$ and $m = 2$.

Newton polytopes: $A =$  $P_1 =$  $P_2 =$ 

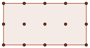
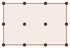
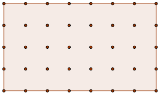
Choose polynomials to define S:

$$\begin{aligned} f_1 &= x^3y^2 + t^4x^3y + x^3 + t^5x^2y^2 + t^2x^2y + x^2 + t^{11}xy^2 + txy + x + y^2 + y + 1 \\ f_2 &= x^7y^4 + t^{10}x^7y + t^2x^7 + t^{12}x^6y + t^8x^6 + t^{10}x^5y + t^3x^5 + t^{13}x^4y + t^{13}x^4 + t^9x^3y + t^{13}x^3 + \\ &\quad t^{11}x^2y^3 + t^8x^2y^2 + t^{12}x^2y + t^{14}x^2 + xy^4 + t^6xy^3 + t^3xy^2 + t^{12}x + t^6y^4 + t^9y^2 + t^{13}y + t^5 \end{aligned}$$

TCI code $\mathcal{C}_{S,A}$ has parameters $[26, 13, 12]$.

Example [Demirarslan–S., FFA'15]

Let $\mathbb{K} = \mathbb{F}_{16}$ and $m = 2$.

Newton polytopes: $A =$  $P_1 =$  $P_2 =$ 

Choose polynomials to define S:

$$
\begin{aligned}
f_1 &= x^3y^2 + t^4x^3y + x^3 + t^5x^2y^2 + t^2x^2y + x^2 + t^{11}xy^2 + txy + x + y^2 + y + 1 \\
f_2 &= x^7y^4 + t^{10}x^7y + t^2x^7 + t^{12}x^6y + t^8x^6 + t^{10}x^5y + t^3x^5 + t^{13}x^4y + t^{13}x^4 + t^9x^3y + t^{13}x^3 + \\
&\quad t^{11}x^2y^3 + t^8x^2y^2 + t^{12}x^2y + t^{14}x^2 + xy^4 + t^6xy^3 + t^3xy^2 + t^{12}x + t^6y^4 + t^9y^2 + t^{13}y + t^5
\end{aligned}
$$

TCI code $\mathcal{C}_{S,A}$ has parameters $[26, 13, 12]$.

- $n = |S| = V(P_1, P_2) = 26$ intersection points in $(\mathbb{F}_{16}^*)^2$ of two curves $f_1 = 0$ and $f_2 = 0$
- $k = \dim \mathcal{L}(A) - \dim \mathrm{Ker}(ev_S) = |A \cap \mathbb{Z}^2| - |(A - P_1) \cap \mathbb{Z}^2| = 15 - 2 = 13$

In fact, $\mathcal{C}_{S,A}$ is isodual!

Duality

Recall: for $y \in (\mathbb{K}^*)^n$ define
$\mathcal{C}^{\perp_y} = \{v \in \mathbb{K}^n \mid (u \cdot v)_y = 0, \forall u \in \mathcal{C}\}$, for $(u \cdot v)_y = \sum_{i=1}^n y_i u_i v_i$.

Duality

Recall: for $y \in (\mathbb{K}^*)^n$ define
$\mathcal{C}^{\perp_y} = \{v \in \mathbb{K}^n \mid (u \cdot v)_y = 0, \forall u \in \mathcal{C}\}$, for $(u \cdot v)_y = \sum_{i=1}^n y_i u_i v_i$.

Theorem (Demirarslan–S., FFA'15)

Let S be a toric complete intersection given by $f_1 = \cdots = f_m = 0$. Let A, B be subsets of P° such that $A + B \subseteq P^\circ$. Then

$$\mathcal{C}_{S,B} \subseteq \mathcal{C}_{S,A}^{\perp_y}.$$

In particular, if $|S|$ is even, $2A \subseteq P^\circ$, and $\dim(\mathcal{C}_{S,A}) = |S|/2$ then $\mathcal{C}_{S,A}$ is a quasi-self-dual code.

Duality

Recall: for $y \in (\mathbb{K}^*)^n$ define
$\mathcal{C}^{\perp_y} = \{v \in \mathbb{K}^n \mid (u \cdot v)_y = 0, \forall u \in \mathcal{C}\}$, for $(u \cdot v)_y = \sum_{i=1}^n y_i u_i v_i$.

Theorem (Demirarslan–S., FFA'15)

Let S be a toric complete intersection given by $f_1 = \cdots = f_m = 0$. Let A, B be subsets of P° such that $A + B \subseteq P^\circ$. Then

$$\mathcal{C}_{S,B} \subseteq \mathcal{C}_{S,A}^{\perp_y}.$$

In particular, if $|S|$ is even, $2A \subseteq P^\circ$, and $\dim(\mathcal{C}_{S,A}) = |S|/2$ then $\mathcal{C}_{S,A}$ is a quasi-self-dual code.

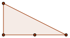
Remark: It follows from Toric Euler–Jacobi Residue formula [Khovanskii, 1978], the vector y consists of local residues at S.

Constructing quasi self-dual TCI codes

Special case: $P_1 = c_1 Q$, $P_2 = c_2 Q$ for some lattice polytope Q and $c_i \in \mathbb{N}$.

Theorem (Demirarslan–S., FFA'15)

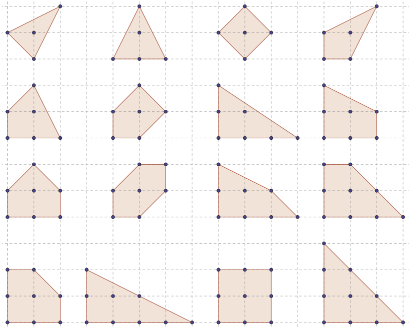
Let S be a toric complete intersection with polygons $m_1 Q$, $m_2 Q$. Let $A = aQ$. Then $\mathcal{C}_{S,A}$ is quasi self-dual if and only if

1. *Q is lattice-equivalent to*  *and $a = (c_1 + c_2 - 3)/2$; or*
2. *Q is lattice-equivalent to either*  *or* *, and $a = (c_1 + c_2 - 2)/2$;*

or ...

Constructing quasi self-dual TCI codes

3. *Q is lattice-equivalent to one of the sixteen reflexive Fano polygons and $a = (c_1 + c_2 - 1)/2$.*



Question: Does this hold in higher dimensions?

Smooth Fano polytopes

Let Q be a lattice polytope in $\mathbb{R}^m$.

- (polar) dual $\check{Q} = \{y \in \mathbb{R}^m \mid (x \cdot y) \geq -1, x \in Q\}$

Smooth Fano polytopes

Let Q be a lattice polytope in $\mathbb{R}^m$.

- (polar) dual $\check{Q} = \{y \in \mathbb{R}^m \mid (x \cdot y) \geq -1, x \in Q\}$
- $\check{Q}$ is a smooth Fano polytope if
  - 0 lies in the interior of $\check{Q}$
  - the vertices of each facet form a basis for $\mathbb{Z}^m$

Smooth Fano polytopes

Let Q be a lattice polytope in $\mathbb{R}^m$.

- (polar) dual $\check{Q} = \{y \in \mathbb{R}^m \mid (x \cdot y) \geq -1, x \in Q\}$
- $\check{Q}$ is a smooth Fano polytope if
  - 0 lies in the interior of $\check{Q}$
  - the vertices of each facet form a basis for $\mathbb{Z}^m$
- then Q and $\check{Q}$ are lattice polytopes, so both are reflexive polytopes

Smooth Fano polytopes

Let Q be a lattice polytope in $\mathbb{R}^m$.

- (polar) dual $\check{Q} = \{y \in \mathbb{R}^m \mid (x \cdot y) \geq -1, x \in Q\}$
- $\check{Q}$ is a smooth Fano polytope if
  - 0 lies in the interior of $\check{Q}$
  - the vertices of each facet form a basis for $\mathbb{Z}^m$
- then Q and $\check{Q}$ are lattice polytopes, so both are reflexive polytopes
- the Ehrhart polynomial of $L_Q(t)$ satisfies functional equation

$$L_Q(t) = (-1)^m L_Q(-t-1),$$

where $L_Q(t) = |tQ \cap \mathbb{Z}^m|$ for $t \in \mathbb{N}$.

Smooth Fano varieties

Let X_Q toric variety corresponding to Q, where $\check{Q}$ smooth Fano polytope.
Let $f_1, \dots, f_m$ be polynomials with polytopes $c_1 Q, \dots, c_m Q$, where $c_i \in \mathbb{N}$

- X_Q is smooth with ample anticanonical divisor $-K_{X_Q}$
- $f_1, \dots, f_m$ correspond to sections of ample line bundles
- the Hilbert function of $I = \langle f_1, \dots, f_m \rangle$ can be computed from the Koszul resolution

Smooth Fano varieties

Let X_Q toric variety corresponding to Q, where $\check{Q}$ smooth Fano polytope. Let $f_1, \dots, f_m$ be polynomials with polytopes $c_1 Q, \dots, c_m Q$, where $c_i \in \mathbb{N}$

- X_Q is smooth with ample anticanonical divisor $-K_{X_Q}$
- $f_1, \dots, f_m$ correspond to sections of ample line bundles
- the Hilbert function of $I = \langle f_1, \dots, f_m \rangle$ can be computed from the Koszul resolution

This produces (see Tuitman and Wulcan)

$$\dim \mathcal{C}_{S,A} = \sum_{I \subseteq [m]} (-1)^{|I|} L_Q(a - c_I),$$

where $A = aQ$, $[m] = \{1, \dots, m\}$, and $c_I = \sum_{i \in I} c_i$.

Self-dual TCI codes from Fano polytopes

Newton polytopes: $c_1 Q, \dots, c_m Q$, and $A = aQ$, where $a, c_i \in \mathbb{N}$ and Q is dual to a smooth Fano polytope.

Let S be a toric complete intersection given by $f_1 = \cdots = f_m = 0$. Then $n = |S| = V(c_1 Q, \dots, c_m Q) = m! c_1 \cdots c_m \operatorname{Vol}(Q)$.

Self-dual TCI codes from Fano polytopes

Newton polytopes: $c_1 Q, \dots, c_m Q$, and $A = aQ$, where $a, c_i \in \mathbb{N}$ and Q is dual to a smooth Fano polytope.

Let S be a toric complete intersection given by $f_1 = \cdots = f_m = 0$. Then $n = |S| = V(c_1 Q, \dots, c_m Q) = m! c_1 \cdots c_m \mathrm{Vol}(Q)$.

Theorem [S.] Put $a = (c_1 + \cdots + c_m - 1)/2$. Suppose the c_i satisfy

1. $a \in \mathbb{N}$ and $2 | c_1 \cdots c_m$
2. if m is odd then $c_{I^c} \le c_I$ for all $I \subseteq [m]$ with $|I| > m/2$
3. if m is even then $c_{I^c} \le c_I$ for all $I \subseteq [m]$ with either $|I| > m/2$ or $|I| = m/2$ and $I \ni m$

Self-dual TCI codes from Fano polytopes

Newton polytopes: $c_1 Q, \dots, c_m Q$, and $A = aQ$, where $a, c_i \in \mathbb{N}$ and Q is dual to a smooth Fano polytope.

Let S be a toric complete intersection given by $f_1 = \cdots = f_m = 0$.
Then $n = |S| = V(c_1 Q, \dots, c_m Q) = m! c_1 \cdots c_m \operatorname{Vol}(Q)$.

Theorem [S.] Put $a = (c_1 + \cdots + c_m - 1)/2$. Suppose the c_i satisfy

1. $a \in \mathbb{N}$ and $2 | c_1 \cdots c_m$
2. if m is odd then $c_{I^c} \le c_I$ for all $I \subseteq [m]$ with $|I| > m/2$
3. if m is even then $c_{I^c} \le c_I$ for all $I \subseteq [m]$ with either $|I| > m/2$ or $|I| = m/2$ and $I \ni m$

Then

$$\dim \mathcal{C}_{S,A} = \sum_{I \subseteq [m]} (-1)^{|I|} L_Q(a - c_I) = \frac{1}{2} m! c_1 \cdots c_m \operatorname{Vol}(Q) = n/2,$$

and hence $\mathcal{C}_{S,A}$ is quasi self-dual.

Remarks

- We may assume that $c_1 \leq c_2 \leq \cdots \leq c_m$. Then the conditions 2.-3. above are satisfied
  - always for $m = 2$
  - if and only if $c_3 \leq c_1 + c_2$ for $m = 3$
  - if and only if $-c_1 + c_2 + c_3 \leq c_4 \leq c_1 + c_2 + c_3$ for $m = 4$

Remarks

- We may assume that $c_1 \leq c_2 \leq \cdots \leq c_m$. Then the conditions 2.-3. above are satisfied
  - always for $m = 2$
  - if and only if $c_3 \leq c_1 + c_2$ for $m = 3$
  - if and only if $-c_1 + c_2 + c_3 \leq c_4 \leq c_1 + c_2 + c_3$ for $m = 4$
- it seems plausible that the formula for $\dim \mathcal{C}_{S,A}$ holds without assuming X_Q smooth. In this case we can take any reflexive polytope Q (as in $m = 2$)

Remarks

- We may assume that $c_1 \leq c_2 \leq \cdots \leq c_m$. Then the conditions 2.-3. above are satisfied
  - always for $m = 2$
  - if and only if $c_3 \leq c_1 + c_2$ for $m = 3$
  - if and only if $-c_1 + c_2 + c_3 \leq c_4 \leq c_1 + c_2 + c_3$ for $m = 4$
- it seems plausible that the formula for $\dim \mathcal{C}_{S,A}$ holds without assuming X_Q smooth. In this case we can take any reflexive polytope Q (as in $m = 2$)

— The End —