Toric Varieties in Error-Control Coding Theory
Math in the Mountains Tutorial

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross

July 29-31, 2013

A bit of history

- Beginning of coding theory as a mathematical and engineering subject came with a paper “A Mathematical Theory of Communication” by Claude Shannon (1948).
- Shannon lived from 1916 t0 2001, and spent most of his working career at Bell Labs and MIT.
- He also made fundamental contributions to cryptography and the design of computer circuitry in earlier work coming from his Ph.D. thesis.
- Other interests – inventing gadgets, juggling, unicycles, chess(!)

Shannon's conceptual communication set-up

$$\begin{array}{ccccccccc} \text{message} & & & & \boxed{\text{noise}} & & & & \\ \downarrow & & & & \downarrow & & & & \\ \boxed{\text{encoder}} & \longrightarrow & \boxed{\text{trans.}} & \longrightarrow & \boxed{\text{channel}} & \longrightarrow & \boxed{\text{rec.}} & \longrightarrow & \boxed{\text{decoder}} \\ & & & & & & & & \downarrow \\ & & & & & & & & \text{message} \end{array}$$

Examples

This is a *very general* framework, incorporating examples such as

- communication with deep space exploration craft (Mariner, Voyager, etc. – the most important early application)
- storing/retrieving information in computer memory
- storing/retrieving audio information (CDs)
- storing/rerieving video information (DVD and Blu-Ray disks)
- wireless communication

A main goal of coding theory is the design of coding schemes that achieve *error control*: ability to detect and correct errors in received messages.

The case we will look at

- We'll consider "linear block codes" – vector subspaces C of $\mathbb{F}_q^n$ for some n.
- parameters: n, $k = \dim_{\mathbb{F}_q}(C)$,

$$d = \min_{x \neq y \in C} d(x, y) = \min_{x \neq 0 \in C} \mathrm{weight}(x)$$

  (*Hamming minimum distance/weight*)
- $t = \lfloor \frac{d-1}{2} \rfloor \Rightarrow$ all errors of weight $\leq t$ can be corrected by "nearest neighbor decoding"
- Good codes: k/n not too small (so not extremely redundant), but at same time d or d/n not too small.

Reed-Solomon codes

- Pick a primitive element α for $\mathbb{F}_q$ (i.e. generator of the cyclic multiplicative group of field), and write the nonzero elements of $\mathbb{F}_q$ as $1, \alpha, \ldots, \alpha^{q-2}$.
- Let $L_k = \{f \in \mathbb{F}_q[x] : \deg f < k\}$. Then

$$\begin{array}{rcl} ev : L_k & \rightarrow & \mathbb{F}_q^{q-1} \\ f & \mapsto & (f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \end{array}$$

  is linear and one-to-one if $k < q$. The image is called $RS(k, q)$.
- All f of degree $< k$ have at most $k - 1$ roots in $\mathbb{F}_q$ (and some have exactly that many)

$$\Rightarrow d = (q - 1) - (k - 1) = n - k + 1.$$

  (Singleton bound: $d \leq n - k + 1$.)

An example

Using the standard monomial basis for L_k:

$$\{1, x, x^2, x^3, \ldots, x^{k-1}\}$$

The Reed-Solomon code $RS(3, 16)$ (parameters: $n = 15, k = 3, d = 13$ over $\mathbb{F}_{16}$, so $16^3 = 4096$ distinct codewords) has generator matrix:

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^7 & \alpha^8 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{14} & \alpha & \cdots & \alpha^{13} \end{pmatrix}$$

(means: the rows of G form a basis for $C = RS(3, 16)$).

How Reed-Solomon codes are used

- Reed-Solomon codes are among the most useful codes in engineering practice in situations where errors tend to occur in "bursts" rather than randomly.
- E.g., $RS(3, 16)$ has $d = 13$, corrects any error vector of weight $\leq \lfloor \frac{13-1}{2} \rfloor = 6$ in a received word over $\mathbb{F}_{16} \cong \mathbb{F}_2^4$.
- A "burst" of up to 20 consecutive bit errors would affect *at most 6* of the symbols of the message thought of as elements of $\mathbb{F}_{16}$. $RS(3, 16)$ can correct any 20 or fewer *consecutive* bit errors in a codeword.
- Also very efficient algebraic decoding algorithms (Berlekamp-Massey).
- Basis for the error-control coding used, for example, in the CD audio system, in communications with deep-space exploration craft like *Voyager*, etc.

Toric code basics

Introduced by J. Hansen $\sim$ 1997. Elementary description:

- Let P be an integral convex polytope in $\mathbb{R}^m$, $m \geq 1$.
- Points β in the finite set $P \cap \mathbb{Z}^m$ correspond to monomials x^β (multi-index notation)
- Let $L_P = \mathrm{Span}\{x^\beta : \beta \in P \cap \mathbb{Z}^m\}$.
- Then consider the *toric evaluation map*

$$\begin{aligned} ev : L_P &\rightarrow \mathbb{F}_q^{(q-1)^m} \\ f &\mapsto (f(\gamma) : \gamma \in (\mathbb{F}_q^*)^m) \end{aligned}$$

Image is the toric code $C_P(\mathbb{F}_q)$.

First example, and "generalized" toric codes

- Example: The Reed-Solomon code $RS(k, q)$ is obtained with this construction by taking $P = [0, k-1] \subset \mathbb{R}$, since $P \cap \mathbb{Z} = \{0, 1, \ldots, k\}$ and $L_P = \mathrm{Span}\{1, x, \ldots, x^{k-1}\}$.
- Can also do the same construction for any $S \subseteq P \cap \mathbb{Z}^m$
- Get *subcodes* of $C_P(\mathbb{F}_q)$ in this way; will denote them by $C_S(\mathbb{F}_q)$
- Also very natural to consider these more general codes for several reasons (more on this later)

Why are they interesting?

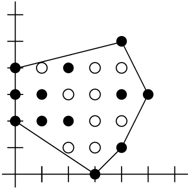
- All $C_S(\mathbb{F}_q)$ have properties parallel to RS codes, e.g. they are "m-dimensional cyclic" codes (set of codewords is closed under a large automorphism group).
- Computer searches by L-, students, and most systematically and recently, Brown and Kasprzyk [BK] have showed that some very good $m = 2$ generalized toric codes exist (better than any previously known codes in standard databases).
- (No argument about this, here, I hope!) Can apply lots of nice algebraic geometry to study their properties (toric varieties, intersection theory, line bundles, Riemann-Roch theorems)

Best known codes from this construction

- an $m = 2$ generalized toric code over $\mathbb{F}_8$ with parameters $[49, 8, 34]$ – found by one group at MSRI-UP REU in 2009
- different $m = 3$ generalized toric codes over $\mathbb{F}_5$ with parameters $[64, 8, 42]$ – another group at MSRI-UP REU in 2009 and Alex Simao
- Seven new "champions" over $\mathbb{F}_8$ found by Brown and Kasprzyk, reported in [BK], apparently motivated by the following one L- found in 2011.
- With hindsight, all can be described in other ways too; toric construction gave a framework for finding them, though.

A typical "current champion"

Over $\mathbb{F}_8$, take *S* given by filled circles ($P = \mathrm{conv}(S)$ shown):



Get a $[49, 12, 28]$ code – best previously known for $n = 49$, $k = 12$ over $\mathbb{F}_8$ was $d = 27$.

How were these found?

- Nicest way to say it – exhaustive ([BK]) and/or "heuristic" (L-, etc.) *search* through space of possible S
- Not very satisfying, though!
- There are general theoretical lower and upper bounds on d that apply to these codes (esp. work of D. Ruano, P. Beelen) *but*
- Not very easy to apply, and rarely sharp
- Need some additional tools to make progress!

A useful equivalence relation

Take $S \subset [0, q-2]^m \simeq (\mathbb{Z}_{q-1})^m$, so corresponding monomials are linearly independent as functions on $(\mathbb{F}_q^*)^m$.

Theorem

If $S' = T(S)$ for some $T = \mathrm{AGL}(m, \mathbb{Z}_{q-1})$, $C_{S'}(\mathbb{F}_q)$ is monomially equivalent to $C_S(\mathbb{F}_q)$.

Monomial equivalence: There is an $n \times n$ permutation matrix Π and an $n \times n$ invertible diagonal matrix Q such that $G' = GQ\Pi$. This implies $d(C_S) = d(C_{S'})$.

Comments

Note: Even when we take $S = P \cap \mathbb{Z}^m$ for a polytope, S' may not be $P' \cap \mathbb{Z}^m$ for any P', so also *need to* study "generalized" toric codes from arbitrary S to make use of this idea.

[BK] uses this in a crucial way – idea was enumerate the affine equivalence classes of S contained in squares $[0, \ell] \times [0, \ell]$

There are also cases where $C_S(\mathbb{F}_q)$ and $C_{S'}(\mathbb{F}_q)$ are monomially equivalent, but S and S' come from different affine equivalence classes. The implication in the theorem only goes the way stated.

Small needles in huge haystacks!

For $m = 3$, $q = 5$, the generating function for number of $\mathrm{AGL}(3, \mathbb{Z}_4)$-orbits on k-sets in $\mathbb{Z}_4^3$:

$$1 + x + 2x^2 + 4x^3 + 16x^4 + 37x^5 + 147x^6 + 498x^7 + 2128x^8 + 8790x^9 + 39055x^{10} + 165885x^{11} + 678826x^{12} + 2584627x^{13} + \cdots$$

The "middle term" here is $333347580600x^{32}$(!)

"Most" of these subsets give quite uninteresting codes. But *one* of the 2128 orbits of size $k = 8$ consists of codes with $d = 42$, the "champion" mentioned before.

From algebraic geometry

- A lattice polytope P defines a toric variety X_P.
- Also get a line bundle $\mathcal{L} = \mathcal{L}_P$ specified by P, with basis of sections given by monomials corresponding to the lattice points in P.
- Subsets of $P \cap \mathbb{Z}^m$ correspond to subspaces of $H^0(X, \mathcal{L})$.
- Codewords come by evaluation, and the issue is: how many $\mathbb{F}_q$-rational zeroes can a section have?
- In case $m = 2$, main results of [LS1] show that for q sufficiently large $d(C_P(\mathbb{F}_q))$, can be bounded above and below by looking at subpolytopes $P' \subseteq P$ that decompose as *Minkowski sums*.

Intuition for proof

- Minkowski-reducible subpolygons $\leftrightarrow$ *reducible sections* (Newton polygon of a product is Minkowski sum of Newton polygons of factors).
- Hasse-Weil upper and lower bounds for an irreducible curve Y:

$$q + 1 - 2p_a(Y)\sqrt{q} \leq |Y(\mathbb{F}_q)| \leq q + 1 + 2p_a(Y)\sqrt{q}$$

- Using this, some intersection theory, and Riemann-Roch on the toric surface defined by P, [LS1] bounds number of $\mathbb{F}_q$-rational points on any reducible section of $\mathcal{L}_P$ in $(\mathbb{F}_q^*)^2 \subset X_P$
- $\Rightarrow$ when $q >$ (a crude but explicit lower bound), reducible curves with more components must have more $\mathbb{F}_q$-rational points than those with fewer components.

From lattice polytopes

- Idea was tightened and extended in [SS1] – d for $C_P(\mathbb{F}_q)$ is connected with $L(P) =$ *full Minkowski length* of P – the maximum number of summands in a Minkowski sum decomposition $Q = Q_1 + \cdots + Q_L$ for $Q \subseteq P$.
- In [SS1], Soprunov and Soprunova showed that in the plane, every Minkowski-indecomposable polygon is lattice equivalent to either
  (a) the unit lattice segment $\mathrm{conv}\{(0,0),(1,0)\}$,
  (b) the unit lattice simplex $\mathrm{conv}\{(0,0),(1,0),(0,1)\}$, or
  (c) the “exceptional triangle” $T_0 = \mathrm{conv}\{(0,0),(1,2),(2,1)\}$

The Soprunov-Soprunova Theorem

Theorem (SS1)

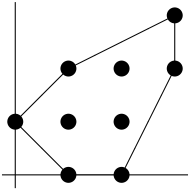
If q is larger than an explicit (smaller than in [LS1]) lower bound depending on $L(P)$ and the area of P, then

$$d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - L(P)(q-1) - \lfloor 2\sqrt{q} \rfloor + 1, \tag{1}$$

and if no maximally decomposable $Q \subset P$ contains an exceptional triangle, then

$$d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - L(P)(q-1). \tag{2}$$

An interesting polygon for $q \geq 5$



- P contains $P' = \text{conv}\{(1,0),(2,0),(1,2),(2,2)\}$ $(= P_1 + P_2 + P_3$, P_i line segments) and $P'' = \text{conv}\{(1,0),(1,1),(3,2),(3,3)\}$ (similar).
- No other decomposable $Q \subset P$ with more than three Minkowski summands

Reducible curves

Bounds from [LS1] or [SS1] $\Rightarrow$ for q suff. large

$$d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - 3(q-1).$$

From P' above, obtain reducible sections of L_P:
$s = x(x-a)(y-b)(y-c)$, with $3(q-1)-2$ zeroes in $(\mathbb{F}_q^*)^2$ if $a, b, c \in \mathbb{F}_q^*$, $b \neq c$. Hence,

$$d(C_P(\mathbb{F}_q)) \leq (q-1)^2 - 3(q-1) + 2.$$

Minimum distances over different fields

Magma computations (package written by D. Joyner) show:

$$\begin{aligned} d(C_P(\mathbb{F}_5)) = 6 &\quad \textit{vs.} \quad 4^2 - 3\cdot 4 + 2 = 6 \\ d(C_P(\mathbb{F}_7)) = 20 &\quad \textit{vs.} \quad 6^2 - 3\cdot 6 + 2 = 20 \\ d(C_P(\mathbb{F}_8)) = 28 &\quad \textit{vs.} \quad 7^2 - 3\cdot 7 + 2 = 30 \\ d(C_P(\mathbb{F}_9)) = 42 &\quad \textit{vs.} \quad 8^2 - 3\cdot 8 + 2 = 42 \\ d(C_P(\mathbb{F}_{11})) = 72 &\quad \textit{vs.} \quad 10^2 - 3\cdot 10 + 2 = 72. \end{aligned}$$

More on $q = 8$

Where does a codeword with $49 - 28 = 21$ zero entries come from? Magma: exactly 49 such words. One of them comes, for instance, from the evaluation of

$$\begin{aligned} y + x^3y^3 + x^2 &\equiv y(1 + x^3y^2 + x^2y^6) \\ &\equiv y(1 + x^3y^2 + (x^3y^2)^3) \end{aligned}$$

Here congruences are mod $\langle x^7 - 1, y^7 - 1\rangle$, the ideal of the $\mathbb{F}_8$-rational points of the 2-dimensional torus. So $1 + x^3y^2 + (x^3y^2)^3$ has exactly the same zeroes in $(\mathbb{F}_8^*)^2$ as $y + x^3y^3 + x^2$.

Arithmetic of $\mathbb{F}_8$ matters!

$1 + u + u^3$ is one of the two irreducible polynomials of degree 3 in $\mathbb{F}_2[u]$, hence

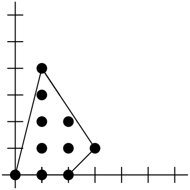
$$\mathbb{F}_8 \cong \mathbb{F}_2[u]/\langle 1 + u + u^3 \rangle.$$

If β is a root of $1 + u + u^3 = 0$ in $\mathbb{F}_8$, then $1 + x^3y^2 + (x^3y^2)^3 =$

$$(x^3y^2 - \beta)(x^3y^2 - \beta^2)(x^3y^2 - \beta^4)$$

and there are exactly $3 \cdot 7 = 21$ points in $(\mathbb{F}_8^*)^2$ where this is zero. Still a sort of *reducibility* that produces a section with the largest number of zeroes here, even though the reducibility only appears when we look modulo the ideal $\langle x^7 - 1, y^7 - 1 \rangle$ (!). Similar phenomena in many other cases for small q.

Another Example: $P = \mathrm{conv}\{(0,0),(2,0),(3,1),(1,4)\}$

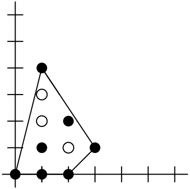


Have $L(P) = 4$, and P contains just one Minkowski sum of 4 indecomposable polygons, namely the line segment $Q = \mathrm{conv}\{(1,0),(1,4)\}$. Expect for q sufficiently large,

$$d(C_P(\mathbb{F}_q)) = (q-1)^2 - 4(q-1).$$

Leaving out lattice points

Now, study $C_S(\mathbb{F}_q)$ for S contained in P from before:



What happens? $k = 7$ only (not $k = 10$), and ...

Example, continued

$$
\begin{array}{rcll}
d(C_S(\mathbb{F}_7)) = 18 & \text{vs.} & 6^2 - 4 \cdot 6 = 12 & \\
d(C_S(\mathbb{F}_8)) = 33 & \text{vs.} & 7^2 - 4 \cdot 7 = 21 & \\
d(C_S(\mathbb{F}_9)) = 32 & = & 8^2 - 4 \cdot 8 = 32 & \\
d(C_S(\mathbb{F}_{11})) = 70 & \text{vs.} & 10^2 - 4 \cdot 10 = 60 & \\
d(C_S(\mathbb{F}_{13})) = 96 & = & 12^2 - 4 \cdot 12 = 96 & \\
d(C_S(\mathbb{F}_{16})) = 165 & = & 15^2 - 4 \cdot 15 = 165 & \\
d(C_S(\mathbb{F}_{17})) = 192 & = & 16^2 - 4 \cdot 16 = 192 & \\
d(C_S(\mathbb{F}_{19})) = 270 & \text{vs.} & 18^2 - 4 \cdot 18 = 252 & \\
d(C_S(\mathbb{F}_q)) & = & (q-1)^2 - 4(q-1) & \text{all } q \geq 23(?)
\end{array}
$$

The minimum weight words

- $C_S(\mathbb{F}_q) \subset C_P(\mathbb{F}_q)$, so $d(C_S(\mathbb{F}_q)) \geq d(C_P(\mathbb{F}_q))$ and
- Conjecture: $d(C_P(\mathbb{F}_q)) = (q-1)^2 - 4(q-1)$ for all $q \geq 23$. Evidence: SS Theorem implies $\geq$, but the C_P code contains the words $\mathrm{ev}(x(y^4 + a_3 y^3 + a_2 y^2 + a_1 y + a_0))$ for all $a_i \in \mathbb{F}_q$.
- Some of those quartic polynomials factor $(y - \beta_1) \cdots (y - \beta_4)$ for β_j distinct $\in \mathbb{F}_q^*$, so $4(q-1)$ zeroes in $(\mathbb{F}_q^*)^2$.
- In $\mathbb{F}_q$ for q sufficiently large, there are *also* polynomials of the form $y^4 + a_1 y + a_0$ that factor this way; bounds not explicit enough to yield $q \geq 23$, though!

Two ways to think about this ...

- First (the "glass is half-empty" point of view): leaving lattice points out of $P \cap \mathbb{Z}^m$ is only likely to improve d dramatically for toric codes when q is small
- Second (the "glass is half-full" point of view): over larger fields, for many sets of lattice points S with $\mathrm{conv}(S) = P$, can often include *all* of the lattice points in $P \cap \mathbb{Z}^m$ and get toric codes of the same minimum distance and larger dimension

Taking toric codes "to the next dimension(s)"

- This whole general area has only started to be explored
- Intersection theory on higher-dimensional varieties is more subtle and not so obvious how to apply it
- Questions about polytopes and toric varieties in higher dimensions are also more subtle (e.g. classification of Minkowski-irreducible polytopes)
- Some preliminary work in [LS2] and [SS2]

A different approach

Square submatrices of the generator matrix G for a Reed-Solomon code are usual (one-variable) Vandermonde matrices:

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \cdots & \alpha^{j_k} \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^{j_1})^{k-1} & (\alpha^{j_2})^{k-1} & \cdots & (\alpha^{j_k})^{k-1} \end{pmatrix}$$

(Well-known and standard observation for studying these codes – implies the rows of G are linearly independent, for instance.)

General Vandermondes

- Let P be an integral convex polytope, and suppose $P \cap \mathbb{Z}^m = \{e(i) : 1 \le i \le \#(P)\}$.
- Let $S = \{p_j : 1 \le j \le \#(P)\}$ be any set of $\#(P)$ points in $(\mathbb{F}_q^*)^m$.
- Picking orderings, define $V(P; S)$, the *Vandermonde matrix* associated to P and S, to be the $\#(P) \times \#(P)$ matrix

$$V(P; S) = \left(p_j^{e(i)}\right),$$

where $p_j^{e(i)}$ is the value of the monomial $x^{e(i)}$ at the point p_j.

Other uses

Interestingly enough, the multivariate Vandermonde matrices have also made appearances in the study of

- multivariate polynomial interpolation
- polynomial equation solving
- Gröbner basis theory
- multipolynomial resultants

An Example

Let $P = \mathrm{conv}\{(0,0),(2,0),(0,2)\}$ in $\mathbb{R}^2$, and $S = \{(x_j, y_j)\}$ be any set of 6 points in $(\mathbb{F}_q^*)^2$. For one particular choice of ordering of the lattice points in P, we have $V(P;S) =$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 & x_5^2 & x_6^2 \\ x_1y_1 & x_2y_2 & x_3y_3 & x_4y_4 & x_5y_5 & x_6y_6 \\ y_1^2 & y_2^2 & y_3^2 & y_4^2 & y_5^2 & y_6^2 \end{pmatrix}$$

Minimum Distance Theorem, [LS2]

Theorem

Let $P \subset \mathbb{R}^m$ be an integral convex polytope. Let d be a positive integer and assume that in every set $T \subset (\mathbb{F}_q^*)^m$ with $|T| = (q-1)^m - (d-1)$ there exists some $S \subset T$ with $|S| = \#(P)$ such that $\det V(P; S) \neq 0$. Then the minimum distance satisfies $d(C_P) \geq d$.

Proof: For all S, $\det V(P; S) \neq 0 \Rightarrow$ the homogeneous linear system obtained from the generator matrix, in columns corresponding to S, has only the trivial solution so there are no nonzero codewords with $(q-1)^m - (d-1)$ zero entries. Hence every nonzero codeword has $\geq d$ nonzero entries.

Codes from simplices

Consider $C_{P_\ell(m)}$ for $P_\ell(m)$ an m-dimensional simplex of the form

$$P_\ell(m) = \text{conv}\{\mathbf{0}, \ell\mathbf{e}_1, \ldots, \ell\mathbf{e}_m\},$$

where the $\mathbf{e}_i$ are the standard basis vectors in $\mathbb{R}^m$. (Corresponding toric variety is the degree ℓ Veronese embedding of $\mathbb{P}^m$. The corresponding Vandermonde matrices also arise in the study of multivariate interpolation using polynomials of bounded total degree.)

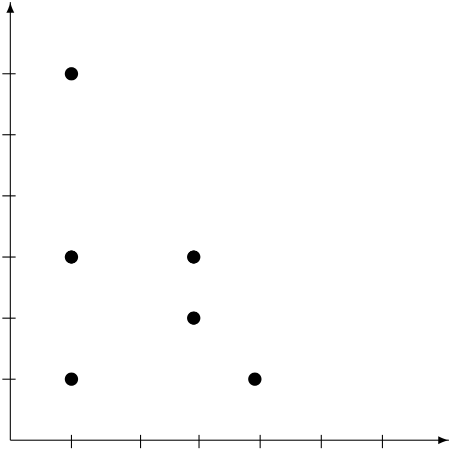
Need to identify S for which $\det(V(P_\ell(m); S)) \neq 0$.

Definition

If $m = 1$, an ℓth order **simplicial configuration** *is any collection of $\binom{1+\ell}{\ell}$ distinct points in $\mathbb{F}_q^*$. For $m \geq 2$, we will say that a collection S of $\binom{m+\ell}{\ell}$ points in $(\mathbb{F}_q^*)^m$ is an m-dimensional ℓth order* **simplicial configuration** *if the following conditions hold:*

1. *For some i, $1 \leq i \leq m$, there are hyperplanes $x_i = a_1, x_i = a_2, \ldots, x_i = a_{\ell+1}$ such that for each $1 \leq j \leq \ell + 1$, S contains exactly $\binom{m-1+j-1}{j-1}$ points with $x_i = a_j$.*
2. *For each j, $1 \leq j \leq \ell + 1$, the points in $x_i = a_j$ form an $(m-1)$-dimensional simplicial configuration of order $j - 1$.*

A “simplicial configuration” of order 2 in $(\mathbb{F}_8^*)^2$ – “log plot”.



Some observations

- Let S be an m-dimensional ℓth order simplicial configuration consisting of $\binom{m+\ell}{\ell}$ points, in hyperplanes $x_m = a_1, \ldots, x_m = a_{\ell+1}$.
- Write $S = S' \cup S''$ where S' is the union of the points in $x_i = a_1, \ldots, a_\ell$, and S'' is the set of points in $x_i = a_{\ell+1}$.
- Let $\pi : \mathbb{F}_q^m \to \mathbb{F}_q^{m-1}$ be the projection on the first $m-1$ coordinates.
- Both S' and $\pi(S'')$ are themselves simplicial configurations: S' dimension m and order $\ell - 1$; $\pi(S'')$ dimension $m-1$ and order ℓ.

A recurrence

Theorem (LS2)

Let $P_\ell(m)$ be as above and let S be an ℓth order simplicial configuration of $\binom{m+\ell}{\ell}$ points. Then writing $p = (p_1, \ldots, p_m)$ for points $p \in (\mathbb{F}_q^*)^m$,

$$\begin{aligned} \det V(P_\ell(m); S) &= \pm \prod_{p \in S'} (p_m - a_{\ell+1}) \\ &\quad \cdot \det V(P_{\ell-1}(m); S') \\ &\quad \cdot \det V(P_\ell(m-1); \pi(S'')) \end{aligned}$$

(Suggested by a computation in a paper on multivariate interpolation by Chui and Lai – "poised sets" for interpolation by polynomials of degree bounded bounded by ℓ.)

Consequences

Corollary

Let $P_\ell(m)$ be as above and let S be an ℓth order simplicial configuration of $\binom{m+\ell}{\ell}$ points. Then $\det V(P_\ell(m); S) \neq 0$.

Theorem

Let $\ell < q - 1$, and let $P_\ell(m)$ be the simplex in $\mathbb{R}^m$ defined above. Then the minimum distance of the toric code $C_{P_\ell(m)}$ is given by

$$d(C_{P_\ell(m)}) = (q-1)^m - \ell(q-1)^{m-1}.$$

The idea of the proof

The result on Vandermondes is used to show $d(C_{P_\ell(m)}) \geq (q-1)^m - \ell(q-1)^{m-1}$.

A pigeon-hole principle argument constructs simplicial configurations $S \subset T$ for every T with $|T| = \ell(q-1)^m + 1$.

Other inequality comes from reducibles $(x_m - a_1) \ldots (x_m - a_\ell)$.

Summary

- Toric codes are interesting and accessible (even for undergraduate projects!)
- But the results on toric codes from simplices and parallelotopes show that d is often quite *small* relative to k.
- It is an interesting problem to determine criteria for polytopes (or subsets of the lattice points in a polytope) that yield good evaluation codes.

References for further study

- BK G. Brown and A. Kasprzyk, *Seven new champion linear codes*, LMS Journal of Computation and Mathematics, 16 (2013), 109-117.
- LS1 J. Little and H. Schenck *Toric codes and Minkowski sums*, SIAM J. of Discrete Math. **20** (2006), 999-1014.
- LS2 J. Little and R. Schwarz, *Toric Codes and Vandermonde matrices*, AAECC **18** (2007), 349-367.
- SS1 Soprunov, I. and Soprunova, J. *Toric surface codes and Minkowski length of polygons.* SIAM J. Discrete Math. **23**, 384-400.
- SS2 Soprunov, I.; Soprunova, J. *Bringing toric codes to the next dimension*. SIAM J. Discrete Math. 24 (2010), 655-665.