Toric Codes

John B. Little

Department of Mathematics and Computer Science, College of the Holy Cross

little@mathcs.holycross.edu

Discrete Math Day at Holy Cross

November 11, 2006

Outline of Talk

1. Coding theory basics

2. Toric codes

3. Multivariate Vandermonde matrices and estimating the minimum distance

4. Codes from simplices

Joint work with Hal Schenck (Texas A+M), and undergrad students (Ryan Schwarz HC '05, Alex Simao, HC '08).

[1] -, R. Schwarz, *On m-dimensional toric codes*, `arXiv/cs.IT/0506102` (to appear, *AAECC*)

[2] -, H. Schenck, *Toric surface codes and Minkowski sums*, `arXiv/math.AG/0507598` (to appear, SIAM J. Disc. Math.)

§1. Coding Theory Basics

A fundamental problem in coding theory is the construction of codes with "good" error-control properties.

- 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

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

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.

$RS(3, 16)$ 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.

§2. Toric codes

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 $L_P = \text{Span}\{x^\beta : \beta \in P \cap \mathbb{Z}^m\}$.

- Define
$$\begin{aligned} ev : L_P &\to \mathbb{F}_q^{(q-1)^m} \\ f &\mapsto (f(\gamma) : \gamma \in (\mathbb{F}_q^*)^m) \end{aligned}$$
Image is the toric code $C_P(\mathbb{F}_q)$.

Note $RS(k, q)$ is the case $P = [0, k-1] \subset \mathbb{R}$ since $L_k = \text{Span}\{1, x, \ldots, x^{k-1}\}$.

Why are these interesting?

- Have many 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 D. Joyner (USNA) $\sim$ 2000 showed that some very good $m = 2$ toric codes exist (better than any previously known codes in standard databases).

- A number of other isolated very good examples found too.

Searching for good toric codes?

Theorem 1 ([1) *] Let P, P' be polytopes as above.*

1. *If P and P' are lattice equivalent polytopes then $C_P(\mathbb{F}_q)$ and $C_{P'}(\mathbb{F}_q)$ are monomially equivalent codes.*

2. *Similarly, viewing $[0, q-2]^m \cap \mathbb{Z}^m$ as $(\mathbb{Z}_{q-1})^m$, if $S = P \cap \mathbb{Z}^m$ and $S' = T(S)$ for some $T = \mathrm{AGL}(m, \mathbb{Z}_{q-1})$, the resulting evaluation code from S' is monomially equivalent to $C_P(\mathbb{F}_q)$.*

Monomial equivalence: There is an $n \times n$ permutation matrix Π and a $n \times n$ invertible diagonal matrix Q such that $G' = GQ\Pi$; implies that parameters are the same.

Note: In the second case, S' may not be $P' \cap \mathbb{Z}^m$ for a convex polytope P'.

Small needles in huge haystacks

For $m = 3$, $q = 5$, for instance, using the usual *cycle index* polynomial for $G = \mathrm{AGL}(3, \mathbb{Z}_4)$ we can compute the generating function for the number of G-orbits on subsets of $\mathbb{Z}_4^3$ of size k:

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

The "middle term" here is:

$$333347580600x^{32}$$

"Most" of these subsets give quite uninteresting codes. But for instance, *one* of the 2128 orbits of size $k = 8$ consists of codes with $d = 42$ (better than best previously known $d = 41$ according to Brouwer's table). Clearly need some other tools(!)

Tools from Algebraic Geometry

The case $m = 2$ is connected with the theory of toric surfaces.

Main results of paper *Toric surface codes and Minkowski sums* ([2]) show that for q sufficiently large, $d(C_P(\mathbb{F}_q))$ can be bounded above and below by looking at subpolygons $P' \subseteq P$ that decompose as *Minkowski sums*.

Theorem 2 *Let ℓ be the largest positive integer such that there is some $P' \subseteq P$ that decomposes as a Minkowski sum $P' = P_1 + P_2 + \cdots + P_\ell$ with nontrivial P_i. For all $q >> 0$, there is some $P' \subseteq P$ of this form such that*

$$d(C_P(\mathbb{F}_q)) \geq \sum_{i=1}^{\ell} d(C_{P_i}(\mathbb{F}_q)) - (\ell - 1)(q - 1)^2.$$

Ideas behind this

The polygon P specifies a normal fan $\Sigma = \Sigma(P)$, hence an abstract toric variety $X = X_\Sigma$, and a line bundle $\mathcal{L}$ on X. Subpolytopes P_i correspond to subspaces of $H^0(X, \mathcal{L})$.

Minkowski-reducible subpolygons $\leftrightarrow$ *reducible sections* (Newton polygon of product of polynomials is a Minkowski sum).

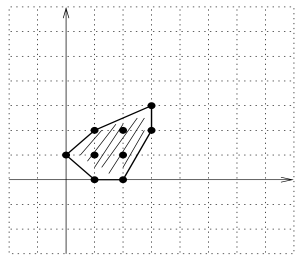
Hasse-Weil upper and lower bounds for a curve Y:

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

$\Rightarrow$ when $q >$ (a crude but explicit lower bound), reducible curves with ℓ components must have more $\mathbb{F}_q$-rational points than those with $m < \ell$ components.

An Example

Consider P as below



$P \subset [0, q-2]^2$ for all $q \geq 5$.

Note that 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, and no Minkowski summands with interior lattice points. Theorem 1 above $\Rightarrow$

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

for $q > \#(P) + 3 = 12$.

Example, cont.

Both subpolygons give rise to reducible curves on the corresponding toric surface. From P' we obtain curves $x(x-a)(y-b)(y-c) = 0$. If $a, b, c \in \mathbb{F}_q^*$ and $b \neq c$, then s has $3(q-1) - 2$ zeroes in $(\mathbb{F}_q^*)^2$. Hence,

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

Computations using Magma show that

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

The dimension is $k = \#(P) = 9$ in each case ($^{(*)}$ code over $\mathbb{F}_5$ is best known for $n = 16, k = 9$).

The case $q = 8$

We may ask: 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

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

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 $1 + x^2y^3 + (x^2y^3)^3$ has exactly the same zeroes in $(\mathbb{F}_8^*)^2$ as $x + x^3y^3 + y^2$.

The case $q = 8$, continued

$1 + u + u^3$ 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 $1 + x^2y^3 + (x^2y^3)^3 =$

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

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.

§3. Enter the Vandermonde matrices

Now turn to m-dimensional toric codes, any $m \geq 2$.

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.)

Multivariate generalizations

Let P be an integral convex polytope, and suppose $P \cap \mathbb{Z}^m = \{e(i) : 1 \le i \le \#(P)\}$, listed in some particular order. Let $S = \{p_j : 1 \le j \le \#(P)\}$ be any set of $\#(P)$ points in $(\mathbb{F}_q^*)^m$, also ordered.

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.

An Example

Let $P = \text{conv}\{(0,0),(2,0),(0,2)\}$ 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 $V(P;S) =$

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

Estimating d of a toric code

We have the following result:

Theorem 3 *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 $d(C_P) \geq d$.*

Idea of proof: For all S, $\det V(P;S) \neq 0 \Rightarrow$ the homogeneous linear system obtained 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.

§4. Codes from simplices

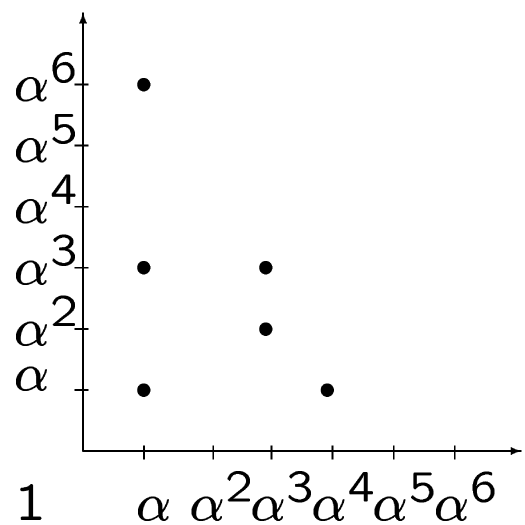
Consider $C_{P_\ell(m)}$ for $P_\ell(m)$ an m-dimensional simplex of the form

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

where the $\mathbf{e}_i$ are the standard basis vectors in $\mathbb{R}^m$. The monomials corresponding to the $\binom{m+\ell}{\ell}$ integer lattice points in $P_\ell(m)$ are all of the monomials in m variables of total degree $\leq \ell$. (The corresponding Vandermonde matrices arise in the study of multivariate Lagrange interpolation using polynomials of bounded total degree.)

Simplicial configurations – an example

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



A 2-dimensional simplicial configuration of order 2 in $(\mathbb{F}_8^*)^2$.

Definition

Definition 1 *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 $x_i = a_j$. (Note that*

$$\binom{m+\ell}{\ell} = \sum_{j=1}^{\ell+1} \binom{m-1+j-1}{j-1}$$

   by a standard binomial coefficient identity.)

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 $j - 1$.*

Some observations

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

A recurrence

Theorem 4 *Let* $P_\ell(m)$ *be as above and let* S *be an* ℓ*th order simplicial configuration of* $\binom{m+\ell}{\ell}$ *points as in the paragraph above. Then writing* $p = (p_1, \ldots, p_m)$ *for points* $p \in (\mathbb{F}_q^*)^m$,

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

(The recurrence was suggested by a computation of the determinant in a paper on multivariate interpolation by Chui and Lai, where corresponding sets of points in $\mathbb{R}^m$ are identified as "poised sets" for interpolation by polynomials of degree bounded bounded by ℓ.)

An illustrative example

Consider all polynomials of degree ≤ 2 in three variables and the Vandermonde matrix $V(P_2(3); S)$. For notational simplicity, write points in a 3-dimensional simplicial configuration $S \subset (\mathbb{F}_q^*)^3$ of order 2 as (x_i, y_i, z_i), for $i = 1, \ldots, 10 = \binom{3+2}{2}$. Here S' consists of the first four points in S, and S'' consists of the other six points. Under the hypothesis that S is a simplicial configuration, we have $z_5 = z_6 = \cdots = z_{10} = c$ for some c.

Consequences

Corollary 1 *Let* $P_\ell(m)$ *be as above and let* S *be an* ℓ*th order simplicial configuration of* $\binom{m+\ell}{\ell}$ *points. Then* $\det V(P_\ell(m); S) \neq 0$.

Theorem 5 *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 result on Vandermondes is used to show $d(C_{P_\ell(m)}) \geq (q-1)^m - \ell(q-1)^{m-1}$ via Theorem 3. 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 $(x_m - a_1)\ldots(x_m - a_\ell)$.

Concluding Comments

- Can get similar results for other families of polytopes (e.g. parallelotopes see [1])

- *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.