Toric Codes

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross

Joint work with Hal Schenck (U. Illinois), Ryan Schwarz (U. Connecticut), Alex Simao (Holy Cross)

AMS Special Session on Linear Codes Over Rings and Modules – Kalamazoo, October 17, 2008

Outline

The Definition And A First Example

Introduced by J. Hansen $\sim$ 1997 – elementary description:

- Let P be an integral convex polytope in $\mathbb{R}^m$, $m \geq 1$.

The Definition And A First Example

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)

The Definition And A First Example

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

The Definition And A First Example

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

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

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

The Definition And A First Example

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

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

  Image is the toric code $C_P(\mathbb{F}_q)$.
- Example: $RS(k, q)$ is the case $P = [0, k-1] \subset \mathbb{R}$ since $L_P = \mathrm{Span}\{1, x, \ldots, x^{k-1}\}$.

Why Are They 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).

Why Are They 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) 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.

Why Are They 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) 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.
- (debatable, maybe!) Can apply lots of nice algebraic geometry to study their properties (toric varieties, intersection theory, line bundles, Riemann-Roch theorems)

When Are Toric Codes Equivalent?
Usually take $P \subset [0, q-2]^m \simeq (\mathbb{Z}_{q-1})^m$.

Theorem

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 $C_P(\mathbb{F}_q)$.

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

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

Small Needles In Huge Haystacks!

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

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

Small Needles In Huge Haystacks!

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

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

- The "middle term" here is $333347580600x^{32}$.

Small Needles In Huge Haystacks!

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

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

- The "middle term" here is $333347580600x^{32}$.
- "Most" of these subsets give quite uninteresting codes.

Small Needles In Huge Haystacks!

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

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

- The “middle term” here is $333347580600x^{32}$.
- “Most” of these subsets give quite uninteresting codes.
- But *one* of the 2128 orbits for $k = 8$ gives codes with $d = 42$ (best previously known: $d = 41$ according to Grassl’s table).

Toric Codes And Toric Varieties

- A polytope P specifies a normal fan $\Sigma = \Sigma_P$, hence an abstract toric variety $X = X_\Sigma$.

Toric Codes And Toric Varieties

- A polytope P specifies a normal fan $\Sigma = \Sigma_P$, hence an abstract toric variety $X = X_\Sigma$.
- Also get a line bundle $\mathcal{L} = \mathcal{L}_P$ on X specified by P.

Toric Codes And Toric Varieties

- A polytope P specifies a normal fan $\Sigma = \Sigma_P$, hence an abstract toric variety $X = X_\Sigma$.
- Also get a line bundle $\mathcal{L} = \mathcal{L}_P$ on X specified by P.
- Subpolytopes P_i correspond to subspaces of $H^0(X, \mathcal{L})$.

Toric Codes And Toric Varieties

- A polytope P specifies a normal fan $\Sigma = \Sigma_P$, hence an abstract toric variety $X = X_\Sigma$.
- Also get a line bundle $\mathcal{L} = \mathcal{L}_P$ on X specified by P.
- Subpolytopes P_i correspond to subspaces of $H^0(X, \mathcal{L})$.
- In case $m = 2$, main results of L. and Schenck *"Toric surface codes and Minkowski sums"* 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*.

The Lower Bound

Theorem

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

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

Intuition For Proof

- Minkowski-decomposable subpolygons $\Leftrightarrow$ *reducible sections* $f_1 f_2$ (Newton polygon of a product is the Minkowski sum).

Intuition For Proof

- Minkowski-decomposable subpolygons $\Leftrightarrow$ *reducible sections* $f_1 f_2$ (Newton polygon of a product is the 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

Intuition For Proof

- Minkowski-decomposable subpolygons $\Leftrightarrow$ *reducible sections* $f_1 f_2$ (Newton polygon of a product is the Minkowski sum).
- Hasse-Weil upper and lower bounds for a curve Y:

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

  $\Rightarrow$ 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
- Bounds have been improved by Soprounov and Soprounova.

An Interesting Polygon

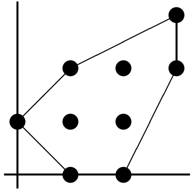

Figure: The polygon P

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

- 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
- $\Rightarrow$ for $q > \#(P) + 3 = 12$,

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

Reducible Curves From P' we obtain $x(x-a)(y-b)(y-c) = 0$. If $a, b, c \in \mathbb{F}_q^*$ and $b \neq c$, then $3(q-1) - 2$ zeroes in $(\mathbb{F}_q^*)^2$. Hence,

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

and $d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - 3(q-1), q >> 0$. Computations using Magma show that

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

($^{(*)}$ code over $\mathbb{F}_5$ is best known for $n = 16, k = 9$)

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 Note: $1 + u + u^3$ 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.

Motivation – Reed-Solomon Case

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

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

General Vandermondes

- Let P be an integral convex polytope, and suppose $P \cap \mathbb{Z}^m = \{e(i) : 1 \leq i \leq \#(P)\}$.

General Vandermondes

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

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.

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 From L., Schwarz, *"Toric Codes and Vandermonde Matrices"*

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, $\det V(P; S) \neq 0 \Rightarrow$ homogeneous linear system 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, etc.

- Consider simplices of form $P_\ell = \mathrm{Conv}(\ell e_i : i = 1, \ldots, m)$.

Codes From Simplices, etc.

- Consider simplices of form $P_\ell = \mathrm{Conv}(\ell e_i : i = 1, \ldots, m)$.
- Via a recursive determinant identity, $\det V(P_\ell; S) \neq 0$ for "simplicial configurations" of points S (essentially: sets of points that look *combinatorially* like the lattice points in a simplex of the same dimension, same ℓ)

Codes From Simplices, etc.

- Consider simplices of form $P_\ell = \mathrm{Conv}(\ell e_i : i = 1, \ldots, m)$.
- Via a recursive determinant identity, $\det V(P_\ell; S) \neq 0$ for "simplicial configurations" of points S (essentially: sets of points that look *combinatorially* like the lattice points in a simplex of the same dimension, same ℓ)
- Such "simplicial configurations" exist in any T as before with $|T| = \ell(q-1)^m + 1$, so $d(C_{P_\ell}) = (q-1)^m - \ell(q-1)^{m-1}$.

Codes From Simplices, etc.

- Consider simplices of form $P_\ell = \mathrm{Conv}(\ell e_i : i = 1, \ldots, m)$.
- Via a recursive determinant identity, $\det V(P_\ell; S) \neq 0$ for "simplicial configurations" of points S (essentially: sets of points that look *combinatorially* like the lattice points in a simplex of the same dimension, same ℓ)
- Such "simplicial configurations" exist in any T as before with $|T| = \ell(q-1)^m + 1$, so $d(C_{P_\ell}) = (q-1)^m - \ell(q-1)^{m-1}$.
- Can do something very similar for paralellotopes.

Codes From Simplices, etc.

- Consider simplices of form $P_\ell = \mathrm{Conv}(\ell e_i : i = 1, \ldots, m)$.
- Via a recursive determinant identity, $\det V(P_\ell; S) \neq 0$ for "simplicial configurations" of points S (essentially: sets of points that look *combinatorially* like the lattice points in a simplex of the same dimension, same ℓ)
- Such "simplicial configurations" exist in any T as before with $|T| = \ell(q-1)^m + 1$, so $d(C_{P_\ell}) = (q-1)^m - \ell(q-1)^{m-1}$.
- Can do something very similar for paralellotopes.
- Also implies results for codes from many subpolytopes of these.

Summary

- Toric codes are interesting and accessible (even for undergraduate projects!)

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.

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 and apparently subtle problem to determine criteria for polytopes (or subsets of the lattice points in a polytope) that yield good evaluation codes.

For Further Reading

J. Little and H. Schenck,
Toric Codes and Minkowski Sums
SIAM Journal of Discrete Mathematics **20** (2006), 999–1014.

J. Little and R. Schwarz,
Toric Codes and Vandermonde Matrices
AAECC **18** (2007), 349–367.