Toric Surface Codes – Some New Observations

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross

HC Faculty Seminar
September 8, 2011

Outline

Coding Theory Basics

- Goal: Want a provably effective way of constructing “good” linear codes over finite fields $\mathbb{F}_q$: vector subspaces C of $\mathbb{F}_q^n$ for given n

Coding Theory Basics

- Goal: Want a provably effective way of constructing “good” linear codes over finite fields $\mathbb{F}_q$: vector subspaces C of $\mathbb{F}_q^n$ for given n
- “Good” code means: *minimum distance d* of the code is large (for given n and $k = \dim_{\mathbb{F}_q} C$)

Coding Theory Basics

- Goal: Want a provably effective way of constructing "good" linear codes over finite fields $\mathbb{F}_q$: vector subspaces C of $\mathbb{F}_q^n$ for given n
- "Good" code means: *minimum distance* d of the code is large (for given n and $k = \dim_{\mathbb{F}_q} C$)
- Minimum distance:

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

where $\mathrm{wt}(x)$ is the Hamming weight (number of nonzero entries) – related to error-correction capacity when information is encoded to elements of C and transmitted over a noisy channel.

Toric Surface Codes – Original Definition

- $P \subset [0, q-2]^2 \subset \mathbb{R}^2$ an integer lattice polygon

Toric Surface Codes – Original Definition

- $P \subset [0, q-2]^2 \subset \mathbb{R}^2$ an integer lattice polygon
- $\mathbb{F}_q$ a finite field with primitive element α.

Toric Surface Codes – Original Definition

- $P \subset [0, q-2]^2 \subset \mathbb{R}^2$ an integer lattice polygon
- $\mathbb{F}_q$ a finite field with primitive element α.
- For $f \in \mathbb{Z}^2$ with $0 \leq f_i \leq q-2$, let $p_f = (\alpha^{f_1}, \alpha^{f_2})$ in $(\mathbb{F}_q^*)^2$.

Toric Surface Codes – Original Definition

- $P \subset [0, q-2]^2 \subset \mathbb{R}^2$ an integer lattice polygon
- $\mathbb{F}_q$ a finite field with primitive element α.
- For $f \in \mathbb{Z}^2$ with $0 \le f_i \le q-2$, let $p_f = (\alpha^{f_1}, \alpha^{f_2})$ in $(\mathbb{F}_q^*)^2$.
- For any $e = (e_1, e_2) \in P \cap \mathbb{Z}^2$, let x^e be the corresponding monomial and write

$$(p_f)^e = (\alpha^{f_1})^{e_1} \cdot (\alpha^{f_2})^{e_2} = \alpha^{\langle f, e \rangle}.$$

Toric Surface Codes – Original Definition

- $P \subset [0, q-2]^2 \subset \mathbb{R}^2$ an integer lattice polygon
- $\mathbb{F}_q$ a finite field with primitive element α.
- For $f \in \mathbb{Z}^2$ with $0 \le f_i \le q-2$, let $p_f = (\alpha^{f_1}, \alpha^{f_2})$ in $(\mathbb{F}_q^*)^2$.
- For any $e = (e_1, e_2) \in P \cap \mathbb{Z}^2$, let x^e be the corresponding monomial and write

$$(p_f)^e = (\alpha^{f_1})^{e_1} \cdot (\alpha^{f_2})^{e_2} = \alpha^{\langle f, e \rangle}.$$

- Toric surface code $C_P(\mathbb{F}_q)$ is the linear code of block length $n = (q-1)^2$ spanned by the $(p_f)^e$ for $e \in P \cap \mathbb{Z}^2$.

In other words, ...

- Let $L = \mathrm{Span}\{x^e : e \in P \cap \mathbb{Z}^2\}$

In other words, ...

- Let $L = \mathrm{Span}\{x^e : e \in P \cap \mathbb{Z}^2\}$
- define the evaluation mapping

$$\begin{aligned} \mathrm{ev} : L &\rightarrow \mathbb{F}_q^{(q-1)^2} \\ g &\mapsto (g(p_f) : p_f \in (\mathbb{F}_q^*)^2) \end{aligned}$$

In other words, ...

- Let $L = \mathrm{Span}\{x^e : e \in P \cap \mathbb{Z}^2\}$
- define the evaluation mapping

$$\begin{aligned} \mathrm{ev} : L &\rightarrow \mathbb{F}_q^{(q-1)^2} \\ g &\mapsto (g(p_f) : p_f \in (\mathbb{F}_q^*)^2) \end{aligned}$$

- Then $C_P(\mathbb{F}_q) = \mathrm{ev}(L)$.
- Have

$$d = (q-1)^2 - \max_{g \in L} |\{ \text{ zeroes of } g \text{ in } (\mathbb{F}_q^*)^2\}|$$

In other words, ...

- Let $L = \mathrm{Span}\{x^e : e \in P \cap \mathbb{Z}^2\}$
- define the evaluation mapping

$$\begin{aligned} \mathrm{ev} : L &\to \mathbb{F}_q^{(q-1)^2} \\ g &\mapsto (g(p_f) : p_f \in (\mathbb{F}_q^*)^2) \end{aligned}$$

- Then $C_P(\mathbb{F}_q) = \mathrm{ev}(L)$.
- Have

$$d = (q-1)^2 - \max_{g \in L} |\{ \text{ zeroes of } g \text{ in } (\mathbb{F}_q^*)^2\}|$$

- Lots of interesting properties – higher dimensional analogs of Reed-Solomon codes

Previous work

- Toric surface codes introduced by J. Hansen about 1998

Previous work

- Toric surface codes introduced by J. Hansen about 1998
- Some very good examples discovered by D. Joyner (USNA) about 2000

Previous work

- Toric surface codes introduced by J. Hansen about 1998
- Some very good examples discovered by D. Joyner (USNA) about 2000
- Undergraduates – SIMU 2001; at HC: Alex Simao, Ryan Schwarz; MSRI-UP 2009

Previous work

- Toric surface codes introduced by J. Hansen about 1998
- Some very good examples discovered by D. Joyner (USNA) about 2000
- Undergraduates – SIMU 2001; at HC: Alex Simao, Ryan Schwarz; MSRI-UP 2009
- J. Little, H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), 999–1014.

Previous work

- Toric surface codes introduced by J. Hansen about 1998
- Some very good examples discovered by D. Joyner (USNA) about 2000
- Undergraduates – SIMU 2001; at HC: Alex Simao, Ryan Schwarz; MSRI-UP 2009
- J. Little, H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), 999–1014.
- I. Soprunov, E. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. **23** (2009), 384–400.

Generalizing Toric Codes

- Can do same construction for polytopes $P \subset [0, q-2]^m \subset \mathbb{R}^m$ for any $m \geq 1$ ("m-dimensional toric codes")

Generalizing Toric Codes

- Can do same construction for polytopes $P \subset [0, q-2]^m \subset \mathbb{R}^m$ for any $m \geq 1$ ("m-dimensional toric codes")
- Can replace the set $P \cap \mathbb{Z}^m$ by an arbitrary set $S \subset \mathbb{Z}^m \cap [0, q-2]^m$.

Generalizing Toric Codes

- Can do same construction for polytopes $P \subset [0, q-2]^m \subset \mathbb{R}^m$ for any $m \geq 1$ ("m-dimensional toric codes")
- Can replace the set $P \cap \mathbb{Z}^m$ by an arbitrary set $S \subset \mathbb{Z}^m \cap [0, q-2]^m$.
- These "generalized toric codes" have many of the same properties

Best Known Codes From This Construction

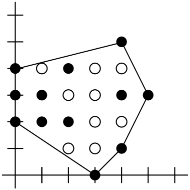
- an $m = 2$ generalized toric code over $\mathbb{F}_8$ with parameters $[49, 8, 34]$ – found by one group at MSRI-UP 2009

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 2009
- different $m = 3$ generalized toric codes over $\mathbb{F}_5$ with parameters $[64, 8, 42]$ – another group at MSRI-UP 2009 and Alex Simao

Another One Found This Summer!

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



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 – "heuristic search" :)

How Were These Found?

- Nicest way to say it – "heuristic search" :)
- Not very satisfying, though!

How Were These Found?

- Nicest way to say it – "heuristic search" :)
- 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*

How Were These Found?

- Nicest way to say it – "heuristic search" :)
- 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

Little-Schenk, Soprunov-Soprunova Approach

- Starting with LS, tightened and extended by SS, known that d for $C_P(\mathbb{F}_q)$ is highly correlated 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 $Q \subseteq P$.

Little-Schenk, Soprunov-Soprunova Approach

- Starting with LS, tightened and extended by SS, known that d for $C_P(\mathbb{F}_q)$ is highly correlated 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 $Q \subseteq P$.
- SS 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 1 (SS)

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

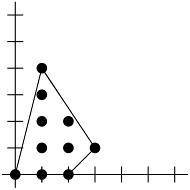
$$d(C_P(\mathbb{F}_q)) \geq (q-1)^2 - L(P)(q-1) - \lfloor 2\sqrt{q} \rfloor + 1, \tag{1}$$

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 Example

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

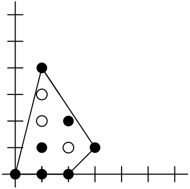


Have $L(P) = 4$, and P contains just one Minkowski sum of 4 indecomposable polygons, namely the line segment $Q = \mathrm{conv}\{(1,0),(1,4)\}$. Expect for q sufficiently large,

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

Example, Continued

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

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

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

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
- $d(C_P(\mathbb{F}_q)) = (q-1)^2 - 4(q-1)$ for all $q > 19$. (Reason: 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 $a_i \in \mathbb{F}_q$.

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
- $d(C_P(\mathbb{F}_q)) = (q-1)^2 - 4(q-1)$ for all $q > 19$. (Reason: 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 completely as $(y - \beta_1)\cdots(y - \beta_4)$ for $\beta_j \in \mathbb{F}_q^*$, so $4(q-1)$ zeroes in $(\mathbb{F}_q^*)^2$.

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
- $d(C_P(\mathbb{F}_q)) = (q-1)^2 - 4(q-1)$ for all $q > 19$. (Reason: SS Theorem implies $\geq$, but the C_P code contains the words

$$\mathrm{ev}(x(y^4 + a_3y^3 + a_2y^2 + a_1y + a_0))$$

for all $a_i \in \mathbb{F}_q$.
- Some of those quartic polynomials factor completely as $(y-\beta_1)\cdots(y-\beta_4)$ for $\beta_j \in \mathbb{F}_q^*$, so $4(q-1)$ zeroes in $(\mathbb{F}_q^*)^2$.
- Key point is: In $\mathbb{F}_q$ for q sufficiently large, there are *also* polynomials of the form $y^4 + a_1y + a_0$ that factor completely with distinct nonzero roots.

Families of Polynomials

Consider any linear family $\mathcal{F}$ of polynomials of the form

$$f(u) = u^\ell + t_1 u^{k_1} + \cdots + t_{m-1} u^{k_{m-1}} + t_m \tag{3}$$

in $\mathbb{F}_q[u]$, where

1. $p > \ell$,
2. the exponents $\ell > k_1 > \cdots > k_{m-1} > k_m = 0$ are fixed,
3. the coefficients t_i, $1 \leq i \leq m$ run over the finite field $\mathbb{F}_q$, and
4. the $\ell, k_1, \ldots, k_{m-1}$ are *not* all multiples of some fixed integer $j > 1$.

Factorization Patterns

- Say that a polynomial $f(u)$ of degree ℓ has factorization pattern
$$\lambda = 1^{a_1} 2^{a_2} \cdots \ell^{a_\ell},$$
where $\sum_{i=1}^{\ell} a_i \cdot i = \ell$, if in $\mathbb{F}_q[u]$, $f(u)$ factors as a product of a_i irreducible factors of degree i (not necessarily distinct) for each $i = 1, \ldots, \ell$.

Factorization Patterns

- Say that a polynomial $f(u)$ of degree ℓ has factorization pattern
$$\lambda = 1^{a_1} 2^{a_2} \cdots \ell^{a_\ell},$$
where $\sum_{i=1}^{\ell} a_i \cdot i = \ell$, if in $\mathbb{F}_q[u]$, $f(u)$ factors as a product of a_i irreducible factors of degree i (not necessarily distinct) for each $i = 1, \ldots, \ell$.
- Let
$$T(\lambda) = \frac{1}{a_1! \cdots a_\ell! 1^{a_1} \cdots \ell^{a_\ell}}$$
be the proportion of elements of the symmetric group S_ℓ with cycle decomposition of shape λ.

Cohen's Theorem

Then S. Cohen proved the following statement in 1972:

Theorem 2

Let $\mathcal{F}$ satisfy the conditions above, and let $\mathcal{F}_\lambda$ be the subset of $\mathcal{F}$ consisting of polynomials with factorization pattern λ in $\mathbb{F}_q[u]$. Then for all q sufficiently large,

$$|\mathcal{F}_\lambda| = T(\lambda)q^m + O\left(q^{m-\frac{1}{2}}\right)$$

where the implied constant depends only on ℓ.

Usually applied to produce *irreducibles* of given shapes; we want to apply it to get *"completely reducibles"*.

Distinct Roots

- We want to study factorizations of shape $\lambda = \lambda_0 := 1^\ell$ where, in addition,

$$f(u) = \prod_{i=1}^{\ell} (u - \beta_i)$$

with β_i distinct in $\mathbb{F}_q^*$.

Distinct Roots

- We want to study factorizations of shape $\lambda = \lambda_0 := 1^\ell$ where, in addition,

$$f(u) = \prod_{i=1}^{\ell} (u - \beta_i)$$

with β_i distinct in $\mathbb{F}_q^*$.

- Elements of $\mathcal{F}$ with repeated roots (possibly in some extension of $\mathbb{F}_q$) correspond to $\mathbb{F}_q$-rational points

$$(t_1, \ldots, t_m) \subset \mathcal{D}_{\mathcal{F}},$$

where $\mathcal{D}_{\mathcal{F}} = V(\Delta_{\mathcal{F}})$ and

$$\Delta_{\mathcal{F}} = \text{resultant}(f(u), f'(u), u)$$

is the *discriminant* of the family.

The Discriminant Variety

- Note that $\mathcal{D}_{\mathcal{F}}$ is an $(m-1)$-dimensional affine hypersurface, singular and possible reducible.

The Discriminant Variety

- Note that $\mathcal{D}_{\mathcal{F}}$ is an $(m-1)$-dimensional affine hypersurface, singular and possible reducible.
- However, when the characteristic p is large enough, it is known that when the conditions above hold on $\mathcal{F}$, $\mathcal{D}_{\mathcal{F}}$ can have at most one irreducible component other than the hyperplane $V(t_m)$.

The Discriminant Variety

- Note that $\mathcal{D}_{\mathcal{F}}$ is an $(m-1)$-dimensional affine hypersurface, singular and possible reducible.
- However, when the characteristic p is large enough, it is known that when the conditions above hold on $\mathcal{F}$, $\mathcal{D}_{\mathcal{F}}$ can have at most one irreducible component other than the hyperplane $V(t_m)$.
- By a general bound of Ghorpade-Lachaud, it follows that

$$|D_{\mathcal{F}}(\mathbb{F}_q)| \leq \delta \pi_{m-1},$$

where $\pi_{m-1} = |\mathbb{P}^{m-1}(\mathbb{F}_q)| = q^{m-1} + q^{m-2} + \cdots + q + 1$, and $\delta = \deg \Delta_{\mathcal{F}} \leq 2\ell - 2$.

Existence of Completely Reducibles

Corollary 3

If $p > \ell$ and $q = p^h$ is sufficiently large, there exist elements of the family $\mathcal{F} \subset \mathbb{F}_q[u]$ with factorization pattern $\lambda_0 = 1^\ell$ in which the irreducible factors are distinct, and for which all the roots are nonzero.

Proof.

The first part of this comes from comparing the orders of growth of the various terms in Cohen and Ghorpade-Lachaud. The last part of this is clear since if any of the roots is zero, then the coefficient $t_m = 0$, and the locus where that is true has dimension $m - 1$. □

First Main Theorem

Theorem 4

Let P have full Minkowski length $L(P) = \ell$ from a unique $Q \subset P$ lattice equivalent to ℓI for a primitive lattice segment. Let $S \subset Q \cap \mathbb{Z}^2$ correspond to a family $\mathcal{F}$ such that

1. *S contains the endpoints of Q, and*
2. *The k_i and ℓ are not all multiples of any fixed integer $j > 1$.*

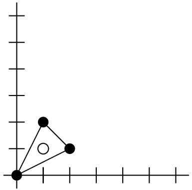
Then for all primes p sufficiently large and all $h \geq 1$, letting $q = p^h$, we have

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

Moreover, for all q, there exists $h \geq 1$ such that the same statement is true if we replace q by q^h.

The Exceptional Triangle

The first main theorem only applies in case there is a unique maximally decomposable Q *not* containing T_0:



Let S consist of the three boundary lattice points. Question: How do $d(C_{T_0}(\mathbb{F}_q))$ and $d(C_S(\mathbb{F}_q))$ compare?

Some Experimental Results

$$
\begin{aligned}
d(C_S(\mathbb{F}_7)) &= 27 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_7)) = 27\\
d(C_S(\mathbb{F}_8)) &= 42 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_8)) = 40\\
d(C_S(\mathbb{F}_9)) &= 56 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_9)) = 52\\
d(C_S(\mathbb{F}_{11})) &= 90 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_{11})) = 85\\
d(C_S(\mathbb{F}_{13})) &= 126 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_{13})) = 126\\
d(C_S(\mathbb{F}_{16})) &= 207 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_{16})) = 204\\
d(C_S(\mathbb{F}_{17})) &= 240 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_{17})) = 235\\
d(C_S(\mathbb{F}_{19})) &= 300 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_{19})) = 300\\
d(C_S(\mathbb{F}_{23})) &= 462 \quad \text{vs.} \quad d(C_{T_0}(\mathbb{F}_{23})) = 454.
\end{aligned}
$$

Are there arbitrarily large q with $d(C_S) > d(C_{T_0})$ and also with $d(C_S) = d(C_{T_0})$?

The Corresponding Curves

- The span of the monomials corresponding to all lattice points in T_0 is the family of polynomials

$$Ax^2y + Bxy^2 + Cxy + D$$

The Corresponding Curves

- The span of the monomials corresponding to all lattice points in T_0 is the family of polynomials

$$Ax^2y + Bxy^2 + Cxy + D$$

- The ones from S all have $C = 0$.

The Corresponding Curves

- The span of the monomials corresponding to all lattice points in T_0 is the family of polynomials

$$Ax^2y + Bxy^2 + Cxy + D$$

- The ones from S all have $C = 0$.
- Note total degree is ≤ 3 – if $ABD \neq 0$, the variety is irreducible, hence a curve of (arithmetic) genus 1. The family contains nodal cubics; smooth ones are *elliptic curves*.

The Corresponding Curves

- The span of the monomials corresponding to all lattice points in T_0 is the family of polynomials

$$Ax^2y + Bxy^2 + Cxy + D$$

- The ones from S all have $C = 0$.
- Note total degree is ≤ 3 – if $ABD \neq 0$, the variety is irreducible, hence a curve of (arithmetic) genus 1. The family contains nodal cubics; smooth ones are *elliptic curves*.
- To understand d for corresponding codes, need to know how many $\mathbb{F}_q$-rational points they can have

More Properties

- The cubic curves from T_0 with $AB \neq 0$ have *three flexes* on the line at infinity. How can we see this?

More Properties

- The cubic curves from T_0 with $AB \neq 0$ have *three flexes* on the line at infinity. How can we see this?
- Homogenized, equation is:
$AX^2Y + BXY^2 + CXYZ + DZ^3 = 0.$

More Properties

- The cubic curves from T_0 with $AB \neq 0$ have *three flexes* on the line at infinity. How can we see this?
- Homogenized, equation is: $AX^2Y + BXY^2 + CXYZ + DZ^3 = 0$.
- For instance, at $[X : Y : Z] = [1 : 0 : 0]$, the tangent line is $Y = 0$, and this meets curve with multiplicity 3 – a "flex tangent."

More Properties

- The cubic curves from T_0 with $AB \neq 0$ have *three flexes* on the line at infinity. How can we see this?
- Homogenized, equation is: $AX^2Y + BXY^2 + CXYZ + DZ^3 = 0$.
- For instance, at $[X : Y : Z] = [1 : 0 : 0]$, the tangent line is $Y = 0$, and this meets curve with multiplicity 3 – a "flex tangent."
- Flexes $\Leftrightarrow$ *points of order 3* in the group law, and *the three points at infinity form a subgroup of order 3*

A “Universal Family”

- In fact, this is the so-called “Hessian family,” a well-known sort of universal family for elliptic curves over $\mathbb{F}_q$ with nontrivial 3-torsion subgroups

A “Universal Family”

- In fact, this is the so-called “Hessian family,” a well-known sort of universal family for elliptic curves over $\mathbb{F}_q$ with nontrivial 3-torsion subgroups
- For simplicity, we’ll stick to cases $p \geq 5$.

A “Universal Family”

- In fact, this is the so-called “Hessian family,” a well-known sort of universal family for elliptic curves over $\mathbb{F}_q$ with nontrivial 3-torsion subgroups
- For simplicity, we'll stick to cases $p \geq 5$.
- Can easily convert to Weierstrass form, to look at j-invariant

A "Universal Family"

- In fact, this is the so-called "Hessian family," a well-known sort of universal family for elliptic curves over $\mathbb{F}_q$ with nontrivial 3-torsion subgroups
- For simplicity, we'll stick to cases $p \geq 5$.
- Can easily convert to Weierstrass form, to look at j-invariant
- For a Weierstrass cubic $u^2 = v^3 + \alpha v + \beta$,

$$j = 1728 \frac{4\alpha^3}{4\alpha^3 + 27\beta^2}.$$

A “Universal Family”

- In fact, this is the so-called “Hessian family,” a well-known sort of universal family for elliptic curves over $\mathbb{F}_q$ with nontrivial 3-torsion subgroups
- For simplicity, we'll stick to cases $p \geq 5$.
- Can easily convert to Weierstrass form, to look at j-invariant
- For a Weierstrass cubic $u^2 = v^3 + \alpha v + \beta$,

$$j = 1728 \frac{4\alpha^3}{4\alpha^3 + 27\beta^2}.$$

- Curves from S with $ABD \neq 0$ always correspond to smooth elliptic curves with $j = 0$

Supersingular Curves

- When $p \equiv 2 \bmod 3$ for an odd prime p, elliptic curves with $j = 0$ are *supersingular*

Supersingular Curves

- When $p \equiv 2 \bmod 3$ for an odd prime p, elliptic curves with $j = 0$ are *supersingular*
- Terminological quirk here: supersingular $\not\Rightarrow$ singular – these are smooth elliptic curves, but “special” in several ways

Supersingular Curves

- When $p \equiv 2 \bmod 3$ for an odd prime p, elliptic curves with $j = 0$ are *supersingular*
- Terminological quirk here: supersingular $\not\Rightarrow$ singular – these are smooth elliptic curves, but “special” in several ways
- There are many equivalent characterizations of this property

Supersingular Curves

- When $p \equiv 2 \bmod 3$ for an odd prime p, elliptic curves with $j = 0$ are *supersingular*
- Terminological quirk here: supersingular $\not\Rightarrow$ singular – these are smooth elliptic curves, but "special" in several ways
- There are many equivalent characterizations of this property
- For us, the one that is most relevant (because it directly says someting about numbers of $\mathbb{F}_{p^h}$-rational points) is that the *trace of Frobenius* is zero.

Supersingular Curves

This implies that for E a supersingular curve,

$$|E(\mathbb{F}_{p^h})| = \begin{cases} p^h + 1 & h \text{ odd} \\ p^h + 1 + 2p^{h/2} & \text{if } h \equiv 2 \bmod 4 \\ p^h + 1 - 2p^{h/2} & \text{if } h \equiv 0 \bmod 4. \end{cases}$$

In other words, supersingular elliptic curves defined over $\mathbb{F}_p$ achieve the Hasse-Weil *upper* bound over $\mathbb{F}_{p^h}$ when $h \equiv 2 \bmod 4$. On the other hand, they achieve the Hasse-Weil *lower* bound over $\mathbb{F}_{p^h}$ when $h \equiv 0 \bmod 4$.

Second Main Theorem

Theorem 5

Let p be odd and $p \equiv 2 \bmod 3$. Then

$$d(C_S(\mathbb{F}_p)) = (p-1)^2 - (p-1) > d(C_{T_0}(\mathbb{F}_p)).$$

Proof. The elliptic curves from S are supersingular, so all of the codewords of $C_S(\mathbb{F}_p)$ obtained from evaluation of $Axy^2 + Bxy^2 + D$ with $ABD \neq 0$ will have weight

$$(p-1)^2 - (p+1-3) > (p-1)^2 - (p-1).$$

On the other hand, there are also codewords of weight $(p-1)^2 - (p-1)$ from polynomials with one coefficient equal to zero. Those give the minimum weight words in this case.

Proof, Concluded

By a theorem of Waterhouse, there are elliptic curves over $\mathbb{F}_p$ with

$$|E(\mathbb{F}_p)| = p + 1 + t$$

for all integers t with $t \leq \lfloor 2\sqrt{p} \rfloor$ and $\gcd(t, p) = 1$ (as well as some other possibilities). By the universality of our family for curves with nontrivial 3-torsion, there will be curves here with $p + 1 + t$ points rational over $\mathbb{F}_p$ if t is the *largest* integer satisfying $t \leq \lfloor 2\sqrt{p} \rfloor$, t prime to p, and such that $3|(p + 1 + t)$. These give codewords of considerably smaller weight, close to

$$(p-1)^2 - (p + 1 + 2\sqrt{p} - 3).$$

So d for the code from S will be strictly larger than d for the code from T_0 for all such p. $\square$

"Reality Check"

- Go back and look at the experimental data from before! For instance $p = 23$ vs. $p = 19$.

"Reality Check"

- Go back and look at the experimental data from before! For instance $p = 23$ vs. $p = 19$.
- There are similar patterns for the C_P and C_S codes from all polygons where the Minkowski-decomposable $Q \subset P$ of maximal length contains a term lattice equivalent to T_0.

Conclusion

There are contributions both from

1. geometry of P, S, Minkowski decompositions, etc., *and*
2. arithmetic of rational points of curves over $\mathbb{F}_q$

to the minimum distance of generalized toric surface codes.
Very subtle and interesting phenomena!