Codes from surfaces with small Picard number

John B. Little/joint work with Hal Schenck
–
College of the Holy Cross/University of Illinois
–
Fq12 – Saratoga Springs

July 17, 2015

Evaluation codes

Evaluation codes

- X an algebraic variety over $\mathbb{F}_q$, $\mathcal{S} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$, $\mathcal{L}$ a vector space of functions on X with all $f(P_i)$ defined.

Evaluation codes

- X an algebraic variety over $\mathbb{F}_q$, $\mathcal{S} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$, $\mathcal{L}$ a vector space of functions on X with all $f(P_i)$ defined.
- The image of the *evaluation map*

$$\begin{array}{rcl} ev : \mathcal{L} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

is a linear code; $k \leq \dim \mathcal{L}$; d depends on X, $\mathcal{S}$, $\mathcal{L}$.

Evaluation codes

- X an algebraic variety over $\mathbb{F}_q$, $\mathcal{S} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$, $\mathcal{L}$ a vector space of functions on X with all $f(P_i)$ defined.
- The image of the *evaluation map*

$$\begin{array}{rcl} ev : \mathcal{L} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

  is a linear code; $k \leq \dim \mathcal{L}$; d depends on X, $\mathcal{S}$, $\mathcal{L}$.
- *Reed-Solomon codes* $RS(k, q)$ are examples with $X = \mathbb{P}^1$, $\mathcal{S} = \mathbb{F}_q^* \subset \mathbb{P}^1$, and $\mathcal{L} = \mathrm{Span}\{1, x, \ldots, x^{k-1}\} = L((k-1)P_\infty)$ $(k < q)$ (meet the Singleton bound).

Evaluation codes

- X an algebraic variety over $\mathbb{F}_q$, $\mathcal{S} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$, $\mathcal{L}$ a vector space of functions on X with all $f(P_i)$ defined.
- The image of the *evaluation map*

$$\begin{array}{rcl} ev : \mathcal{L} & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

  is a linear code; $k \leq \dim \mathcal{L}$; d depends on X, $\mathcal{S}$, $\mathcal{L}$.
- *Reed-Solomon codes* $RS(k, q)$ are examples with $X = \mathbb{P}^1$, $\mathcal{S} = \mathbb{F}_q^* \subset \mathbb{P}^1$, and $\mathcal{L} = \mathrm{Span}\{1, x, \ldots, x^{k-1}\} = L((k-1)P_\infty)$ ($k < q$) (meet the Singleton bound).
- AG Goppa codes: $\mathbb{P}^1 \mapsto$ other curves over $\mathbb{F}_q$.

Goal for this work

- What about higher-dimensional varieties X?
- Some examples have been studied–e.g. *projective Reed-Muller codes* from $X = \mathbb{P}^n$
- Codes from quadrics, Hermitian varieties, Grassmannians, flag varieties, Deligne-Lusztig varieties
- But, still really not much known!
- We'll concentrate on *Reed-Muller-type* codes with $\mathcal{S} = X(\mathbb{F}_q)$, $\mathcal{L} =$ vector space of homogeneous forms of some fixed degree s.

Key issue with these codes; motivating example

Key issue with these codes; motivating example

- One recurrent pattern: Low weight codewords tend to come from f where $X \cap \mathbf{V}(f)$ is *reducible* (possibly if $q >> 0$).

Key issue with these codes; motivating example

- One recurrent pattern: Low weight codewords tend to come from f where $X \cap \mathbf{V}(f)$ is *reducible* (possibly if $q >> 0$).
- Example: X a quadric surface in $\mathbb{P}^3$.

Key issue with these codes; motivating example

- One recurrent pattern: Low weight codewords tend to come from f where $X \cap \mathbf{V}(f)$ is *reducible* (possibly if $q >> 0$).
- Example: X a quadric surface in $\mathbb{P}^3$.
- If X is *hyperbolic*, $|X(\mathbb{F}_q)| = q^2 + 2q + 1$. Tangent planes intersect X in reducible curves with $2q + 1$ $\mathbb{F}_q$-points.
- But if X is *elliptic*, rulings not defined over $\mathbb{F}_q$ so $|X(\mathbb{F}_q)| = q^2 + 1$, and planes meet X in curves with at most $q + 1$ $\mathbb{F}_q$-rational points.

Key issue with these codes; motivating example

- One recurrent pattern: Low weight codewords tend to come from f where $X \cap \mathbf{V}(f)$ is *reducible* (possibly if $q >> 0$).
- Example: X a quadric surface in $\mathbb{P}^3$.
- If X is *hyperbolic*, $|X(\mathbb{F}_q)| = q^2 + 2q + 1$. Tangent planes intersect X in reducible curves with $2q + 1$ $\mathbb{F}_q$-points.
- But if X is *elliptic*, rulings not defined over $\mathbb{F}_q$ so $|X(\mathbb{F}_q)| = q^2 + 1$, and planes meet X in curves with at most $q + 1$ $\mathbb{F}_q$-rational points.
- $s = 1$ codes with $S = X(\mathbb{F}_q)$ have parameters: $[q^2 + 2q + 1, 4, q^2]$ (hyperbolic) and $[q^2 + 1, 4, q^2 - q]$ (elliptic – better – equals best known for $q = 8, 9$).

Ansatz from 2007 thesis of M. Zarzar (UT Austin)

Ansatz from 2007 thesis of M. Zarzar (UT Austin)

- $NS(X)$ = group of $\mathbb{F}_q$-*rational divisor classes modulo algebraic equivalence* (a finitely-generated abelian group)

Ansatz from 2007 thesis of M. Zarzar (UT Austin)

- $NS(X)$ = group of $\mathbb{F}_q$-*rational divisor classes modulo algebraic equivalence* (a finitely-generated abelian group)
- Example: X an elliptic quadric: $NS(X) = \mathbb{Z} \cdot [H]$, H = a smooth conic plane section; X a hyperbolic quadric: $NS(X) = \mathbb{Z}[L_1] \oplus \mathbb{Z}[L_2]$ (lines from the two rulings).

Ansatz from 2007 thesis of M. Zarzar (UT Austin)

- $NS(X)$ = group of $\mathbb{F}_q$-*rational divisor classes modulo algebraic equivalence* (a finitely-generated abelian group)
- Example: X an elliptic quadric: $NS(X) = \mathbb{Z} \cdot [H]$, H = a smooth conic plane section; X a hyperbolic quadric: $NS(X) = \mathbb{Z}[L_1] \oplus \mathbb{Z}[L_2]$ (lines from the two rulings).

Theorem (Zarzar)

If $\deg X = d$ *with* $(d, \mathrm{char}(\mathbb{F}_q)) = 1$, $\mathrm{rank}(NS(X)) = 1$, *and* Y *irreducible over* $\mathbb{F}_q$ *with* $\deg Y < d$, *then* $X \cap Y$ *is irreducible.*

Ansatz from 2007 thesis of M. Zarzar (UT Austin)

- $NS(X)$ = group of $\mathbb{F}_q$*-rational divisor classes modulo algebraic equivalence* (a finitely-generated abelian group)
- Example: X an elliptic quadric: $NS(X) = \mathbb{Z} \cdot [H]$, H = a smooth conic plane section; X a hyperbolic quadric: $NS(X) = \mathbb{Z}[L_1] \oplus \mathbb{Z}[L_2]$ (lines from the two rulings).

Theorem (Zarzar)

If $\deg X = d$ *with* $(d, \mathrm{char}(\mathbb{F}_q)) = 1$, $\mathrm{rank}(NS(X)) = 1$, *and* Y *irreducible over* $\mathbb{F}_q$ *with* $\deg Y < d$, *then* $X \cap Y$ *is irreducible.*

- So (**key idea**) – good codes (might) come from surfaces X with Picard number $= \mathrm{rank}\ NS(X) = 1$ (or small).

A test case – cubic surface codes

A test case – cubic surface codes

- "Fact 1:" Over an algebraically closed field, a smooth cubic surface contains exactly 27 lines, always in a particular highly symmetric configuration.
- Symmetry group of the 27 lines is a group of order 51840 $(= W(E_6))$

A test case – cubic surface codes

- "Fact 1:" Over an algebraically closed field, a smooth cubic surface contains exactly 27 lines, always in a particular highly symmetric configuration.
- Symmetry group of the 27 lines is a group of order 51840 $(= W(E_6))$
- Frobenius acts as a permutation of the lines
- There is a complete classification of the conjugacy classes in $W(E_6)$; the class where Frobenius lies determines the $\mathbb{F}_q$-structure!

A test case – cubic surface codes

- "Fact 1:" Over an algebraically closed field, a smooth cubic surface contains exactly 27 lines, always in a particular highly symmetric configuration.
- Symmetry group of the 27 lines is a group of order 51840 $(= W(E_6))$
- Frobenius acts as a permutation of the lines
- There is a complete classification of the conjugacy classes in $W(E_6)$; the class where Frobenius lies determines the $\mathbb{F}_q$-structure!
- The 25 possibilities summarized in a 1967 paper of Swinnerton-Dyer (and in a related table in Manin's book *Cubic Forms*).

An extract from the Swinnerton-Dyer table

Exactly five types of cubics with Picard number $= 1$ ($\Rightarrow$ *no* $\mathbb{F}_q$-rational lines or conics)

Class	Perm Type of Frob	$\lvert X(\mathbb{F}_q)\rvert$
C_{10}	$\{3, 6^3, 6\}$	$q^2 - q + 1$
C_{11}	$\{3^9\}$	$q^2 - 2q + 1$
C_{12}	$\{3, 6^4\}$	$q^2 + 2q + 1$
C_{13}	$\{3, 12^3\}$	$q^2 + 1$
C_{14}	$\{9^3\}$	$q^2 + q + 1$

Some experimental results

With $q = 7$, the $s = 1$ (and $s = 2$) codes look like this:

- C_{10} – $[43, 4, 30]$ and $[43, 4, 31]$ examples (but best known is $d = 35$)
- C_{11} – $[36, 4, 23]$ and $[36, 4, 24]$ examples (but best possible is $28 \leq d \leq 29$)
- C_{12} – $[64, 4, 51]$ examples (but best possible is $52 \leq d \leq 53$) (also $s = 2$ with $[64, 10, 38]$, but best possible is $41 \leq d \leq 48$)
- C_{13} (very rare) – $[50, 4, 37]$ (but best known is $d = 42$)
- C_{14} (rare) – $[57, 4, 44]$ (but best known is $d = 47$)

What to make of all this?

What to make of all this?

- Among these, C_{12} cubics are the best for this construction, but still not that great
- Plane sections of cubics with Picard number > 1 can have up to $3q + 1$ $\mathbb{F}_q$-points (Eckardt points as in Amanda Knecht's talk!) Largest number of $\mathbb{F}_7$-points here is e.g., $64 - 51 = 13$ ($\Rightarrow$ confirmation of Zarzar's Ansatz)

What to make of all this?

- Among these, C_{12} cubics are the best for this construction, but still not that great
- Plane sections of cubics with Picard number > 1 can have up to $3q + 1$ $\mathbb{F}_q$-points (Eckardt points as in Amanda Knecht's talk!) Largest number of $\mathbb{F}_7$-points here is e.g., $64 - 51 = 13$ ($\Rightarrow$ confirmation of Zarzar's Ansatz)
- *Why 13?* Hasse-Weil-Serre bound: The maximum number of $\mathbb{F}_7$-points on a smooth plane cubic is $1 + 7 + \lfloor 2\sqrt{7} \rfloor = 13$ and attained. Singular (but irreducible) plane sections all have either $q = 7$ ("split" node), $q + 1 = 8$ (cusp), or $q + 2 = 9$ ("non-split" node) $\mathbb{F}_7$-points.
- Note: Some C_{10} and C_{11} surfaces have no plane sections with 13 $\mathbb{F}_7$-points.

A byproduct of this experimentation

Based on lots of additional experimental evidence for prime powers $q \leq 37$,

Conjecture

For all $q \geq 5$, C_{12} cubics always have **optimal** *cubic plane sections, i.e. plane sections with the maximum number of $\mathbb{F}_q$-points for a smooth plane cubic curve.*

Have verified this completely for q up to 13 by "brute force," but is there a deeper reason why it should hold?

Also would show $s = 1$ codes from C_{12} cubics *do not* give any "new bests" for larger q.

Some bounds – *sectional genus* of X also matters!

Notation: $C(X, s, \mathbb{F}_q) =$ degree s code on a projective surface X.

Theorem

Assume $(\deg X, \mathrm{char}(\mathbb{F}_q)) = 1$ *and Picard number of* $X = 1$. *Writing* $d_1 = d(C(X, 1, \mathbb{F}_q))$, $g =$ *sectional genus,*

$$n - d_1 \leq 1 + q + g\lfloor 2\sqrt{q} \rfloor.$$

Corollary

In situation of theorem, if q *is sufficiently large, then writing* $d_s = d(C(X, s, \mathbb{F}_q))$,

$$n - d_s \leq s(n - d_1).$$

Sectional genus $g = 0$

Theorem

If S is a smooth abstract surface and L is an ample line bundle with $g(L) = 0$, then (S, L) is one of the following:

- $(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(r))$, $r = 1, 2$.
- $(Q, \mathcal{O}_Q(1))$
- *a Hirzebruch surface* $(F_r, \mathcal{O}_{F_r}(E + sf))$, $s \geq r + 1$.

In other words, few examples, and those are pretty well understood from coding theory perspective – e.g. codes from scrolls (C. Carvalho's talk), toric surface codes.

Higher sectional genus surfaces not promising

Higher sectional genus surfaces not promising

- Consider the surface X_m in $\mathbb{P}^3$ given by

$$0 = w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}.$$

Shioda: $\mathrm{rank}\ NS(X) = 1$ over $\mathbb{C}$ if $m \geq 5$ (and K3 with $\mathrm{rank}\ NS(X) = 20$ for $m = 4$).

Higher sectional genus surfaces not promising

- Consider the surface X_m in $\mathbb{P}^3$ given by
$$0 = w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}.$$
Shioda: $\mathrm{rank}\ NS(X) = 1$ over $\mathbb{C}$ if $m \geq 5$ (and K3 with $\mathrm{rank}\ NS(X) = 20$ for $m = 4$).
- For $m = 4$, reduction of S_4 may have no $\mathbb{F}_q$-lines or conics $\Rightarrow$ no reducible plane sections.

Higher sectional genus surfaces not promising

- Consider the surface X_m in $\mathbb{P}^3$ given by

$$0 = w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}.$$

  Shioda: $\mathrm{rank}\ NS(X) = 1$ over $\mathbb{C}$ if $m \geq 5$ (and K3 with $\mathrm{rank}\ NS(X) = 20$ for $m = 4$).
- For $m = 4$, reduction of S_4 may have no $\mathbb{F}_q$-lines or conics $\Rightarrow$ no reducible plane sections.
- With $q = 11$ and $s = 1$, $C(S_4, 1, \mathbb{F}_{11})$ is $[144, 4, 120]$.

Higher sectional genus surfaces not promising

- Consider the surface X_m in $\mathbb{P}^3$ given by
$$0 = w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}.$$
Shioda: $\mathrm{rank}\ NS(X) = 1$ over $\mathbb{C}$ if $m \geq 5$ (and K3 with $\mathrm{rank}\ NS(X) = 20$ for $m = 4$).
- For $m = 4$, reduction of S_4 may have no $\mathbb{F}_q$-lines or conics $\Rightarrow$ no reducible plane sections.
- With $q = 11$ and $s = 1$, $C(S_4, 1, \mathbb{F}_{11})$ is $[144, 4, 120]$.
- Min. weight codewords $\leftrightarrow$ smooth plane quartics ($g = 3$) with 24 $\mathbb{F}_{11}$-rational points (optimal for $g = 3$ by `manypoints.org`).

Higher sectional genus surfaces not promising

- Consider the surface X_m in $\mathbb{P}^3$ given by
$$0 = w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}.$$
Shioda: $\mathrm{rank}\ NS(X) = 1$ over $\mathbb{C}$ if $m \geq 5$ (and K3 with $\mathrm{rank}\ NS(X) = 20$ for $m = 4$).
- For $m = 4$, reduction of S_4 may have no $\mathbb{F}_q$-lines or conics $\Rightarrow$ no reducible plane sections.
- With $q = 11$ and $s = 1$, $C(S_4, 1, \mathbb{F}_{11})$ is $[144, 4, 120]$.
- Min. weight codewords $\leftrightarrow$ smooth plane quartics ($g = 3$) with 24 $\mathbb{F}_{11}$-rational points (optimal for $g = 3$ by `manypoints.org`).
- C_{12} cubics over $\mathbb{F}_{11}$: all give $[144, 4, 126]$ codes: $g = 1$ curves over $\mathbb{F}_{11}$ have at most 18 rational points.

Higher sectional genus surfaces not promising

- Consider the surface X_m in $\mathbb{P}^3$ given by
$$0 = w^m + xy^{m-1} + yz^{m-1} + zx^{m-1}.$$
Shioda: $\mathrm{rank}\ NS(X) = 1$ over $\mathbb{C}$ if $m \geq 5$ (and K3 with $\mathrm{rank}\ NS(X) = 20$ for $m = 4$).
- For $m = 4$, reduction of S_4 may have no $\mathbb{F}_q$-lines or conics $\Rightarrow$ no reducible plane sections.
- With $q = 11$ and $s = 1$, $C(S_4, 1, \mathbb{F}_{11})$ is $[144, 4, 120]$.
- Min. weight codewords $\leftrightarrow$ smooth plane quartics ($g = 3$) with 24 $\mathbb{F}_{11}$-rational points (optimal for $g = 3$ by `manypoints.org`).
- C_{12} cubics over $\mathbb{F}_{11}$: all give $[144, 4, 126]$ codes: $g = 1$ curves over $\mathbb{F}_{11}$ have at most 18 rational points.
- Similarly for $m \geq 5$.

A better sectional genus 1 example

A better sectional genus 1 example

- Consider the linear system of cubics in $\mathbb{P}^2$ through a general Frobenius orbit $\mathcal{O}_3 = \{P, F(P), F^2(P)\}$ $(P \in \mathbb{P}^2(\mathbb{F}_{q^3}))$

A better sectional genus 1 example

- Consider the linear system of cubics in $\mathbb{P}^2$ through a general Frobenius orbit $\mathcal{O}_3 = \{P, F(P), F^2(P)\}$ $(P \in \mathbb{P}^2(\mathbb{F}_{q^3}))$
- dim $= 7$, so defines a rational map $\mathbb{P}^2$ into $\mathbb{P}^6$
- Image is a degree 6 del Pezzo surface X over $\mathbb{F}_q$,

A better sectional genus 1 example

- Consider the linear system of cubics in $\mathbb{P}^2$ through a general Frobenius orbit $\mathcal{O}_3 = \{P, F(P), F^2(P)\}$ $(P \in \mathbb{P}^2(\mathbb{F}_{q^3}))$
- $\dim = 7$, so defines a rational map $\mathbb{P}^2$ into $\mathbb{P}^6$
- Image is a degree 6 del Pezzo surface X over $\mathbb{F}_q$,
- Blows up the points in $\mathcal{O}_3$ to lines, but defined over $\mathbb{F}_{q^3}$, not $\mathbb{F}_q$.

A better sectional genus 1 example

- Consider the linear system of cubics in $\mathbb{P}^2$ through a general Frobenius orbit $\mathcal{O}_3 = \{P, F(P), F^2(P)\}$ $(P \in \mathbb{P}^2(\mathbb{F}_{q^3}))$
- $\dim = 7$, so defines a rational map $\mathbb{P}^2$ into $\mathbb{P}^6$
- Image is a degree 6 del Pezzo surface X over $\mathbb{F}_q$,
- Blows up the points in $\mathcal{O}_3$ to lines, but defined over $\mathbb{F}_{q^3}$, not $\mathbb{F}_q$.
- $\Rightarrow$ Picard number equal to 2
- $\mathrm{NS}(X)$ is generated by classes of proper transforms of conics in $\mathbb{P}^2$ through $\mathcal{O}_3$, and lines in $\mathbb{P}^2$.

How to determine the Picard number

- The zeta function of X has the form

$$Z(X,t) = \frac{[deg\ 0][deg\ 0]}{[deg\ 1][deg\ 4][deg\ 1]} = \frac{1}{(1-t)P_2(t)(1-q^2t)},$$

where $P_2(t) = (1-qt)\prod_{j=1}^{3}(1-\alpha_j t)$, with $|\alpha_j| = q$ all j.

- Usual zeta function "yoga":

$$|X(\mathbb{F}_{q^r})| = 1+q^{2r}+q^r+\sum_{j=1}^{3}\alpha_j^r = \begin{cases} 1+q^{2r}+q^r & r \equiv 1,2 \bmod 3 \\ 1+q^{2r}+4q^r & r \equiv 0 \bmod 3 \end{cases}$$

- $\Rightarrow \alpha_j = q, e^{2\pi i/3}q, e^{4\pi i/3}q$. Tate: the Picard number of X equals $1+$ the number of α_j equal to q.

(More) interesting codes!

Theorem (also see Couvreur, [1])

] $C(X, 1, \mathbb{F}_q)$ is a $[q^2 + q + 1, 7, q^2 - q - 1]$ code over $\mathbb{F}_q$.

(Min weight words from reducible cubics: conic through $\mathcal{O}_3$ union a line meeting the conic in a pair of conjugate $\mathbb{F}_{q^2}$-points) For $q = 7, 8, 9$ this equals the best known d for these n, k according to Grassl's tables.

Conjecture

$C(X, 2, \mathbb{F}_q)$ is a $[q^2 + q + 1, 19, q^2 - 3q - 1]$ code over $\mathbb{F}_q$.

Would be new best for $q = 7, 9$ and equal best known for $q = 8$.

Thanks for your attention!

References

(1) A. Couvreur, Construction of rational surfaces yielding good codes, *Finite Fields Appl.* **17** (2011), 424-441.

(2) J. Voloch and M. Zarzar, Algebraic geometric codes on surfaces, in “Arithmetic, geometry, and coding theory", *Sémin. Congr. Soc. Math. France*, **21** (2010), 211-216.

(3) M. Zarzar, Error-correcting codes on low rank surfaces, *Finite Fields Appl.* **13** (2007), 727-737.