Evaluation Codes from Algebraic Surfaces over a Finite Field

John B. Little/joint work with Hal Schenck

–

College of the Holy Cross/University of Illinois

–

AG17 – SIAM Conference on Applied Algebraic Geometry
Georgia Tech

August 2, 2017

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*

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

  is a linear code; $k \leq \dim \mathcal{L}$; d depends on X, $\mathcal{S}$, $\mathcal{L}$.
- Well-known examples: *Reed-Solomon codes* from $\mathcal{S} = \mathbb{F}_q^* \subset X = \mathbb{P}^1$; *AG Goppa codes* with $X =$ other curves over $\mathbb{F}_q$.

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, toric varieties, etc.
- But, is there potential for producing really good codes(?)
- We'll concentrate on X a projective *surface* ($\dim X = 2$) and *Reed-Muller-type* codes with $\mathcal{S} = X(\mathbb{F}_q)$, $\mathcal{L} =$ vector space of homogeneous forms of some fixed degree s.
- Notation: $C(X, s, \mathbb{F}_q)$

Key issue with these codes; a motivating example

- Note: If $f \in \mathcal{L}$, $X \cap \mathbf{V}(f)$ is a curve
- Recurrent pattern: (Hasse-Weil-type bounds $\Rightarrow$) lowest-weight codewords tend to come from $f \in \mathcal{L}$ for which $X \cap \mathbf{V}(f)$ *reducible*, especially reducible with genus 0 components, at least if $q >> 0$;
- For instance, consider the $C(X, 1, \mathbb{F}_q)$ codes from quadric surfaces in $\mathbb{P}^3$:
  1. *X a hyperbolic* $\Rightarrow |X(\mathbb{F}_q)| = q^2 + 2q + 1$, and $|(X \cap \mathbf{V}(f))(\mathbb{F}_q)| = 2q + 1$ if the plane $\mathbf{V}(f)$ is tangent to X.
  2. *X elliptic* $\Rightarrow |X(\mathbb{F}_q)| = q^2 + 1$, $|(X \cap \mathbf{V}(f))(\mathbb{F}_q)| = q + 1$ all f.
- Parameters $[q^2 + 2q + 1, 4, q^2]$ (hyperbolic) and $[q^2 + 1, 4, q^2 - q]$ (elliptic; equals best known for $q = 8, 9$).

Our starting point: *Ansatz* from thesis of M. Zarzar

Definition (Néron-Severi group)

$NS(X)$ = group of $\mathbb{F}_q$-rational divisor classes modulo algebraic equivalence, a finitely-generated abelian group, rank is denoted $\rho(X)$, called the Picard number of X.

(**Key idea**) – look for surfaces X with $\rho(X) = 1$ (or small).

Theorem (Zarzar-Voloch)

If $NS(X)$ is generated by $[H]$, H ample, and $[D] = m[H]$, then for any nonzero $f \in L(D)$, the divisor of zeroes of f has at most m irreducible components.

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

Theorem (Corollary of Zarzar-Voloch and Hasse-Weil-Serre)

Assume $\rho(X) = 1$, $NS(X) = \langle [H] \rangle$. Writing $d_1 = d(C(X, 1, \mathbb{F}_q))$ and g = sectional genus, the max. no. of zeroes in a non-zero codeword is

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

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

- $(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(r))$, $r = 1, 2$.
- $Q \subset \mathbb{P}^3$ *a smooth quadric,* $(Q, \mathcal{O}_Q(1))$
- *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 quadrics, rational scrolls, toric surface codes.

Higher sectional genus not immediately 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: $\rho(X_m) = 1$ over $\mathbb{C}$ if $m \geq 5$.)
- For $m = 4$ and some q, reduction of X_4 has no $\mathbb{F}_q$-lines or conics $\Rightarrow$ no reducible plane sections over $\mathbb{F}_q$.
- With $q = 11$ and $s = 1$, $C(X_4, 1, \mathbb{F}_{11})$ is $[144, 4, 120]$.
- Min. weight codewords $\leftrightarrow$ smooth plane quartics ($g = 3$) with 24 $\mathbb{F}_{11}$-rational points (optimal by `manypoints.org`).
- But there are codes from cubic surfaces ($g = 1$) over $\mathbb{F}_{11}$ with parameters $[144, 4, 126]$

Sectional genus $g = 1$?

- Surfaces with sectional genus 1 essentially come in “two flavors”
- Ruled surfaces (“scrolls”) over elliptic curves – but these don’t ever seem to give good codes: $\rho(X) \geq 2$ and reducible hyperplane sections containing multiple fibers of the ruling are hard to avoid
- Del Pezzo surfaces (and surfaces that “become Del Pezzo” over an algebraic extension of $\mathbb{F}_q$)
- Cubic surfaces in $\mathbb{P}^3$ are the simplest examples – examples considered already by Zarzar and Voloch. (If time, some experimental results on those at end.)

Our best $g = 1$ examples

- 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 surface X over $\mathbb{F}_q$, "becomes Del Pezzo" over $\mathbb{F}_{q^3}$
- Blows up the points in $\mathcal{O}_3$ to lines defined over $\mathbb{F}_{q^3}$, not $\mathbb{F}_q$.
- **Claim:** $\rho(X) = 2$; $\mathrm{NS}(X)$ is generated by classes of proper transforms of conics in $\mathbb{P}^2$ through $\mathcal{O}_3$, and lines in $\mathbb{P}^2$.

Zeta function and Picard number

- The zeta function of this 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":

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

- $\Rightarrow \alpha_j = q, e^{2\pi i/3}q, e^{4\pi i/3}q$. A result of Tate: $\rho(X) \leq 1+$ the number of α_j equal to q, *hence equal to 2*

(More) interesting codes!

Theorem (also see Couvreur (1))

For $q \geq 5$, $C(X, 1, \mathbb{F}_q)$ is a $[q^2 + q + 1, 7, q^2 - q - 1]$ code over $\mathbb{F}_q$.

For $q = 7, 8, 9$ this equals the best known d for these n, k according to Grassl's tables.

Theorem (L-Schenck)

For $q \geq 5$, $C(X, 2, \mathbb{F}_q)$ is a $[q^2 + q + 1, 19, \leq q^2 - 3q - 1]$ code over $\mathbb{F}_q$, with equality for all $q >> 0$.

Experimental results

- $d(C(X,2,\mathbb{F}_7)) = 7^2 - 3 \cdot 7 - 1 = 27$, and a "new best" for $q = 7$ (Magma),
- (Magma) d also equals $q^2 - 3q - 1$ for $q = 9$ (this improves best known d *by* 2 *in Grassl's tables*)
- But $d = 37 < 8^2 - 3 \cdot 8 - 1$ for $q = 8$ – minimum weight words come from irreducible curves of degree 6 with nodes at the points of the Frobenius orbit, some have 36 $\mathbb{F}_8$-rational points (new best there for curves of genus 7(!))

A few details

- The minimum-weight words for the $C(X, 1, \mathbb{F}_q)$ code come from hyperplane sections $\leftrightarrow$ reducible cubics of the form $C \cup L$ where C is a conic containing $\mathcal{O}_3$ and $C \cap L$ is defined over $\mathbb{F}_{q^2} \Rightarrow 2q + 2$ points over $\mathbb{F}_q$
- $\dim C(X, 2, \mathbb{F}_q) = 19 = \binom{6+2}{2} - 9$ because the ideal of X is generated by 9 quadrics in $\mathbb{P}^6$
- For $q >> 0$, the minimum-weight words for $C(X, 2, \mathbb{F}_q) \leftrightarrow$ reducible sextics $(C_1 \cup L_1) \cup (C_2 \cup L_2)$ with $C_i \cup L_i$ as above and $L_i \cap C_j$ defined over $\mathbb{F}_{q^2}$; can see exactly $(2q + 2) + (2q + 2) - 2 = 4q + 2$ points over $\mathbb{F}_q$.
- Thanks for your attention!

Cubic surfaces with $\rho = 1$ – experimental results

Over the alg. closure, a smooth cubic surface contains exactly 27 lines with symmetry group $W(E_6)$. Frob acts as a permutation of the lines; the conjugacy class of Frob in $W(E_6)$ determines the $\mathbb{F}_q$-structure – Swinnerton-Dyer/Manin:

Class	$\lvert X(\mathbb{F}_q)\rvert$	$C(X, 1, \mathbb{F}_7)$	best d
C_{10}	$q^2 - q + 1$	$[43, 4, 30/31]$	35
C_{11}	$q^2 - 2q + 1$	$[36, 4, 23/24]$	29
C_{12}	$q^2 + 2q + 1$	$[64, 4, 51]$	52
C_{13}	$q^2 + 1$	$[50, 4, 37]$	42
C_{14}	$q^2 + q + 1$	$[57, 4, 44]$	47

$C(X, 2, \mathbb{F}_7)$ from C_{12} cubics: $[64, 10, 38]$ (best known $d = 41$).

What to make of all this?

- $\rho(X) = 1 \Rightarrow$ *all $\mathbb{F}_q$-rational plane sections are irreducible*; these surfaces contain no $\mathbb{F}_q$-rational lines or conics
- Note often (but not always!) $n - d = 13$. *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.

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.*

References

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

(2) H.P.F. Swinnerton-Dyer, The zeta function of a cubic surface over a finite field, Proc. Cambridge Phil. Soc. **63** (1967), 55-71.

(3) 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.

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