Cubic Surfaces and Codes

John B. Little

Department of Mathematics and Computer Science
Faculty Seminar

November 12, 2014

Outline

A disclaimer

As you will see, this is very much work in progress and I don't quite have the "punchline" yet. *Thanks for the opportunity to speak on this though*. The process of preparing this talk has been a good way to take stock of where I am in this project!

"A Mathematical Theory of Communication," Claude Shannon (1948)

$$
\begin{tikzcd}
\text{message} \arrow[d] & & \boxed{\text{noise}} \arrow[d] & & \\
\boxed{\text{encoder}} \arrow[r] & \boxed{\text{trans.}} \arrow[r] & \boxed{\text{channel}} \arrow[r] & \boxed{\text{rec.}} \arrow[r] & \boxed{\text{decoder}} \arrow[d] \\
 & & & & \text{message}
\end{tikzcd}
$$

Examples

This is a *very general* framework, incorporating examples such as

- communication with deep space exploration craft (Mariner, Voyager, etc. – the most important early application)
- storing/retrieving information in computer memory
- storing/retrieving audio information (CDs)
- storing/rerieving video information (DVD and Blu-Ray disks)
- wireless communication

A main goal of coding theory is the design of coding schemes that achieve *error control*: ability to detect and correct errors in received messages.

The case we will look at

- We'll consider "linear block codes" – vector subspaces C of $\mathbb{F}_q^n$ for some n.
- Parameters $[n, k, d]$: the *blocklength* n, the *dimension* $k = \dim_{\mathbb{F}_q}(C)$, and the *Hamming minimum weight/distance*

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

- $t = \lfloor \frac{d-1}{2} \rfloor \Rightarrow$ 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.

Evaluation code basics

Idea (in this form) goes back to work of Goppa from the late 1970's - early 1980's

- Let X be an algebraic variety defined over $\mathbb{F}_q$, with $\mathcal{S} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$.
- Let $\mathcal{L}$ be some vector subspace of the field of rational functions on X with $f(P_i)$ defined for all $f \in L$ and P_i.
- Then consider the *evaluation map*

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

- Image is a linear code of blocklength n, dimension $k \leq \dim \mathcal{L}$, d depends on properties of X, $\mathcal{S}$, $\mathcal{L}$

The "ur-examples"

- The well-known (and extensively used) *Reed-Solomon codes* $RS(k, q)$ are obtained with this construction by taking $X = \mathbb{P}^1$, $n = q - 1$, and $\mathcal{S}$ the set of nonzero affine $\mathbb{F}_q$-rational points of $\mathbb{P}_1$.
  $\mathcal{L} = \mathrm{Span}\{1, x, \ldots, x^{k-1}\} = L((k-1)P_\infty)$ $(k < q)$.
- This evaluation code has $d = (q - 1) - (k - 1) = n - k + 1$, since some polynomials of degree $\leq k - 1$ have $k - 1$ roots in $\mathbb{F}_q$, but no more
- A general bound says this is the *biggest possible d* for a given n, k(!)
- Goppa codes replace $\mathbb{P}^1$ with other algebraic curves over $\mathbb{F}_q$. Known: can get some *very good* codes with this construction for $q > 49$, q a square.

What about higher-dimensional varieties X?

- Codes from some special varieties (quadrics, Hermitian varieties, Grassmannians, flag varieties, toric varieties, types of algebraic surfaces ...) have been investigated, but this subject is still really in its infancy
- One recurrent pattern: If $X \subset \mathbb{P}^n$ for some $n > \dim X$, and $\mathcal{L}$ has the form $\{f/g \mid f \in \mathbb{F}_q[x_0, \ldots, x_n]_s\}$ for some *degree* s, then d can be (much) smaller than we hope because some $X \cap \mathbf{V}(f)$ can be *reducible* and contain lots of $\mathbb{F}_q$-rational points $\Rightarrow ev(f)$ are codewords of low weight.

Example – $s = 1$ codes from quadric surfaces

- Say q is odd to rule out characteristic 2 "weirdness"
- Smooth quadrics in $\mathbb{P}^3$ come in two "flavors"
- *hyperbolic*: ruled surfaces like hyperbolic paraboloids (e.g. $\mathbf{V}(xy - zw)$). Have $X \simeq \mathbb{P}^1 \times \mathbb{P}^1$ in Segre embedding so $|X(\mathbb{F}_q)| = q^2 + 2q + 1$.
- *elliptic*: non-ruled – analogous to real ellipsoids. Have $|X(\mathbb{F}_q)| = q^2 + 1$ in this case.

Example, continued

- Fix a linear form g so $Y = \mathbf{V}(g) \cap X$ a smooth conic ($q + 1$ $\mathbb{F}_q$-points), take $\mathcal{S} = X(\mathbb{F}_q) - Y(\mathbb{F}_q)$, so $n = q^2 + q$ in hyperbolic case and $n = q^2 - q$ in elliptic case.
- Take $\mathcal{L} = \mathbb{F}_q[x, y, z, w]_1/g$.
- In the elliptic case, every plane $\mathbf{V}(f)$ for $f \in \mathbb{F}_q[x, y, z, w]_1$ meets X in either a single point or in a smooth conic ($q + 1$ $\mathbb{F}_q$-points). Therefore, $d = q^2 - q - 1$.
- In the hyperbolic case, the tangent planes to X at $\mathbb{F}_q$-points intersect X in reducible conics consisting of two lines, so $2q + 1$ $\mathbb{F}_q$-points and $d = q^2 - q - 1$ again.
- *But* codes from elliptic quadrics are *much better* – the same d for a smaller n.

Zarzar's *ansatz*

In his 2007 U. Texas PhD thesis, Marcos Zarzar discussed the following idea.

- Take $\dim X = 2$. Zeroes in codewords of an evaluation code come from $\mathbb{F}_q$-points in $\mathbf{V}(f) \cap X$ for $f/g \in \mathcal{L}$. But as above for quadrics, if $\mathbf{V}(f) \cap X$ is reducible (and $q >> 0$) it can contain many more $\mathbb{F}_q$-rational points than corresponding smooth $\mathbf{V}(f) \cap X$ (can quantify this).
- So good codes should come from surfaces X containing few (or no) reducible curves of small degree relative to the degree of the f from $\mathcal{L}$.

The Neron-Severi group

Precise statement uses an important invariant of algebraic varieties–the *Neron-Severi* group of *divisors classes modulo algebraic equivalence*.

This refers to divisors rational over the field of definition of X.

- For elliptic quadrics, $NS(X) = \mathbb{Z} \cdot [H]$, H = any smooth conic plane section
- For hyperbolic quadrics, $NS(X) = \mathbb{Z} \cdot [L_1] \oplus \mathbb{Z} \cdot [L_2]$, where L_i are lines in the two rulings

Fact noted by 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.

Counting $\mathbb{F}_q$-points on varieties – the zeta function

- For any given X and q, it is, of course, a finite problem to determine all $\mathbb{F}_q$-points on X by "brute force."
- But there is also an extremely elegant and beatiful theory based on the generating function known as the *zeta function* of X.
- Let X be defined over $\mathbb{F}_q$ and let $N_r = |X(\mathbb{F}_{q^r})|$.
- Then

$$Z(X, t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right)$$

The Weil Conjectures (Dwork, Deligne, ...)

- Say X can be viewed as reduction of a scheme over $\mathbb{Z}$
- $Z(X,t)$ is a *rational function* of t whose numerator and denominator factor into polynomials
  - reflecting shape of cohomology of the complex variety $X(\mathbb{C})$, and
  - and whose roots have special algebraic properties.
- Best way to explain this is by giving the examples most relevant to our story ...

The zeta function of a smooth plane cubic curve

- $Z(X,t) = \frac{[deg\ 2]}{[deg\ 1][deg\ 1]} = \frac{(1-\alpha_1 t)(1-\alpha_2 t)}{(1-t)(1-qt)}$, where $|\alpha_i| = \sqrt{q}$ and $\alpha_1\alpha_2 = q$
- Taking log of both sides of the equation

$$\exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right) = \frac{(1-\alpha_1 t)(1-\alpha_2 t)}{(1-t)(1-qt)}$$

and equating coefficients gives for all $r \geq 1$:

$$N_r = 1 + q^r - (\alpha_1^r + \alpha_2^r)$$

- With $r = 1$ (and a bit more work), Hasse-Weil-Serre:

$$1 + q - \lfloor 2\sqrt{q} \rfloor \leq N_1 \leq 1 + q + \lfloor 2\sqrt{q} \rfloor$$

The zeta function of a smooth cubic surface

- $Z(X,t) = \frac{[deg\ 0][deg\ 0]}{[deg\ 1][deg\ 7][deg\ 1]} = \frac{1}{(1-t)P_2(t)(1-q^2t)}$, where $P_2(t) = (1-qt)\prod_{j=1}^{6}(1-\alpha_j t)$, with $|\alpha_j| = q$ all j.
- Taking log of both sides of the equation and equating coefficients gives for all $r \geq 1$:

$$N_r = 1 + q^{2r} + q^r + \sum_{j=1}^{6} \alpha_j^r$$

- Tate conjecture (known to hold in this case, I think): the rank of $NS(X)$ equals $1+$ the number of α_j equal to q.

A test case – cubic surface codes

- Construct codes from X a smooth cubic surface in $\mathbb{P}^3$.
- A first observation: there are *many more* differences between cubics than between quadrics – different numbers of $\mathbb{F}_q$-points, different ranks of $NS(X)$, etc.
- Fortunately, this is a well-studied area, starting with work of Cayley and Salmon from the 1850's (over $\mathbb{C}$).
- "Fact 1:" Over an algebraically closed field, a smooth cubic surface contains exactly 27 straight lines, always in a particular highly symmetric and intricate configuration.
- Symmetry group of the 27 lines is a group of order 51840 $(= W(E_6))$
- For some X, some lines may only be defined over an algebraic extension of $\mathbb{F}_q$

The Clebsch cubic

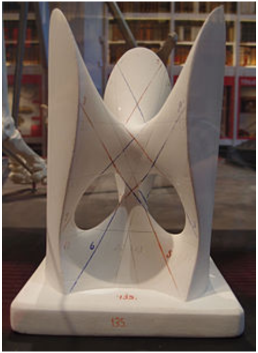

Figure: A cubic surface with 27 real lines

The Frobenius action on the 27 lines

- Because we assume X is defined over $\mathbb{F}_q$ (where all $a \in \mathbb{F}_q$ satisfy $a^q = a$), the Frobenius mapping $F : (x, y, z, w) \to (x^q, y^q, z^q, w^q)$ takes X to itself
- $\Rightarrow F$ also acts as a permutation of the lines on the cubic over the algebraic closure $\overline{\mathbb{F}_q}$
- There is a complete classification of the conjugacy classes in $W(E_6)$.
- Which class F (acting on the 27 lines) belongs to determines the structure of the cubic!
- 25 possibilities summarized in two tables from a 1967 paper of Swinnerton-Dyer (and in a related table in Manin's *Cubic Forms*).

An extract from the Swinnerton-Dyer table

Exactly five types of cubics with $\mathrm{rank}\, NS(X) = 1$ ($\Rightarrow$ *no* $\mathbb{F}_q$-rational lines)

Class	PermType	$N_1 = \lvert X(\mathbb{F}_q)\rvert$	$\mathrm{ord}(\eta_j)$
C_{10}	$\{3, 6^3, 6\}$	$q^2 - q + 1$	$2, 2, 3, 3, 6, 6$
C_{11}	$\{3^9\}$	$q^2 - 2q + 1$	$3, 3, 3, 3, 3, 3$
C_{12}	$\{3, 6^4\}$	$q^2 + 2q + 1$	$3, 3, 6, 6, 6, 6$
C_{13}	$\{3, 12^3\}$	$q^2 + 1$	$3, 3, 12, 12, 12, 12$
C_{14}	$\{9^3\}$	$q^2 + q + 1$	$9, 9, 9, 9, 9, 9$

Notes: η_j is a primitive $\mathrm{ord}(\eta_j)$th root of unity with $\alpha_j = \eta_j q$. Knowing the η_j allows us to compute N_r for all $r \geq 1$ as before.

Some experimental results for $s = 1$ codes

Generated cubic surfaces randomly, classified them by looking at the numbers of $\mathbb{F}_{q^r}$-points for $r = 1, 2, 3$, whether they contained lines defined over $\mathbb{F}_q$, etc. With $q = 7$, for instance:

- C_{10} – found $[43, 4, 30]$ and $[43, 4, 31]$ examples (best possible $d = 35$)
- C_{11} – found $[36, 4, 23]$ and $[36, 4, 24]$ examples (best possible $28 \le d \le 29$)
- C_{12} – *all* $[64, 4, 51]$ (several hundred of them) (best possible $52 \le d \le 53$)
- C_{13} (very rare) – found $[50, 4, 37]$ (best possible $d = 42$)
- C_{14} (rare) – found $[57, 4, 44]$ (best possible $d = 47$)

What to make of all this?

- C_{12} cubics are clearly the best for this construction.
- Also, confirmation of Zarzar's *ansatz*. Cubics with $\mathrm{rank}\, NS(X) > 1$ can have reducible plane sections with as many as $3q + 1 = 22$ points with $q = 7$. The largest number of $\mathbb{F}_7$-points we were seeing in plane sections here for $q = 7$ is, e.g., $64 - 51 = 13$.
- *Why 13?* Recall the Hasse-Weil-Serre bound: The maximum number of $\mathbb{F}_7$-points on a smooth plane cubic is $1 + 7 + \lfloor 2\sqrt{7} \rfloor = 13$. Moreover, singular (but irreducible) plane sections all have either $q = 7$ ("split" node), $q + 1 = 8$ (cusp), or $q + 2 = 9$ ("non-split" node) $\mathbb{F}_q$-points.
- Note: Some of the C_{10} and C_{11} surfaces don't have any plane sections with 13 $\mathbb{F}_7$-points.

A conjecture

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

Conjecture

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

C_{12} cubics – a closer look

For C_{12} surfaces, can extract the following additional information from Swinnerton-Dyer:

- All the lines on a C_{12} are defined over $\mathbb{F}_{q^6}$ (the degree 6 extension field of $\mathbb{F}_q$).
- The Frobenius orbits on the lines consist of:
  - one coplanar 3-cycle ($\Rightarrow$ those lines are defined over $\mathbb{F}_{q^3}$), and
  - four 6-cycles, each consisting of two coplanar triangles, where F takes a line in one triangle to a line in the other triangle ($\Rightarrow$ those triangles and the planes containing them are defined over $\mathbb{F}_{q^2}$)

Well, so what?

The information about the Frobenius orbits of the lines implies:

Theorem

The equation of a C_{12} cubic surface can be written (in four different ways) as

$$\ell \cdot F(\ell) \cdot F^2(\ell) = m \cdot n \cdot F(n) \tag{1}$$

where $\ell = 0$ is a plane defined over $\mathbb{F}_{q^3}$, $m = 0$ is a plane defined over $\mathbb{F}_q$, and $n = 0$ is a plane defined over $\mathbb{F}_{q^2}$.

The idea: $m = 0$ defines the plane of the 3-cycle orbit, which consists of $m = F^i(\ell) = 0$, $i = 0, 1, 2$. A 6-cycle orbit consists of the other 6 "obvious lines" from (1).

More details

The "obvious lines" mentioned before are the

$$\begin{array}{ccc} n = \ell = 0, & F(n) = F(\ell) = 0, & n = F^2(\ell) = 0 \\ F(n) = \ell = 0, & n = F(\ell) = 0, & F(n) = F^2(\ell) = 0 \end{array}$$

coming from the form of the equation (1).

It is *not* the case that *every* cubic with an equation of the form (1) is a C_{12}, though. There are also C_{10}'s and C_{23}'s of this form.

Two final (vague) observations

- The form (1)

$$\ell \cdot F(\ell) \cdot F^2(\ell) = m \cdot n \cdot F(n)$$

is quite reminiscent of the *Weierstrass form* of an elliptic curve when you look at it the right way over $\mathbb{F}_q$:

$$(\text{irreducible cubic in } x) = wy^2$$

By taking plane sections of (1), might be possible to use known facts about Weierstrass equations(!)

- But there's got to be a *pigeonhole principle* component too because the ultimate idea (if the conjecture is true!) has to be: X has lots of $\mathbb{F}_q$-points $\Rightarrow$ some plane section has lots of $\mathbb{F}_q$-points.