Gröbner Bases for Encoding of Certain Codes from Order Domains

John B. Little

Department of Mathematics and Computer Science, College of the Holy Cross

little@mathcs.holycross.edu

RISC Workshop

Linz, Austria

May 1, 2006

utline of talk

- Motivation; polynomial division encoding for cyclic codes
- Automorphisms $\Rightarrow$ module (quasi-cyclic) structures
- Gröbner bases for modules
- Evaluation codes from order domains (including AG Goppa codes)
- Examples

§1. Some motivation

- To use a code in practice, must have efficient encoding and decoding algorithms.

- For encoding a linear block code, knowing a generator matrix suffices.

- *But* for "large" codes (large n and k, over large fields), a full generator matrix G can require a large amount of storage space.

- Can we do better?

Cyclic codes

- When our code has some additional structure, often, *yes*.

- Say C is cyclic of block-length n over $\mathbb{F}_q$ (key example – the Reed-Solomon codes $RS(k,q)$ with $n = q-1$).

- Standard fact: Representing code words as polynomials modulo x^n-1, C can be viewed as an ideal $C \subset \mathbb{F}_q[x]/\langle x^n-1\rangle$.

- PID property of $\mathbb{F}_q[x] \Rightarrow C$ is generated by some $g(x)$ of degree $\leq n-1$.

- $\Leftrightarrow C$ has a generator matrix G whose rows are all cyclic shifts of the vector of coefficients of $g(x)$, so we can replace full G by one of its rows without loss of information.

Cyclic codes, continued

- To encode in this setting, we can use the following procedure: *Information positions* are the coefficients of $t^{n-k}, \ldots, x^{n-1}$, and the *parity checks* are the coefficients of $1, x, \ldots, x^{n-k-1}$.

  Input: $g(x)$, generator poly for C
  information symbols $c_{n-k}, \ldots, c_{n-1}$
  Output: y, a codeword

  $p := c_{n-k}x^{n-k} + \cdots + c_{n-1}x^{n-1}$;
  $y := p - Rem(p, g, x)$;

- As usual, $p - Rem(p, g, x)$ is divisible by $g(x)$, hence an element of the ideal C.

- Since g has degree $n - k$, $Rem(p, g, x)$ contains only terms in $1, x, \ldots, x^{n-k-1}$. The other terms will be the same as in $p \Rightarrow$ this is a "systematic" encoding method.

§2. Automorphisms and module structures

Generalizing the cyclic case, consider any linear block code C with a cyclic group $G = \langle \sigma \rangle$ of automorphisms (C is "quasicyclic").

- Let O_i, $i = 1, \ldots, r$ be the *orbits* of the components of codewords under σ.

- For example, if $n = 8$, and $\sigma =$ right cyclic shift by *two* positions:

  $$\sigma : (x_1, x_2, x_3 \ldots, x_8) \mapsto (x_7, x_8, x_1, \ldots, x_6)$$

  is an automorphism of a code, then there are *two orbits*: $O_1 =$ the odd-numbered positions and $O_2 =$ the even-numbered positions.

- By general facts on group actions, $|O_i| \mid |G|$ all i.

The module structure

- Pick any $x_{i,0}$ in ith orbit and relabel the orbit as $x_{i,j}$, $j = 0, \ldots, |O_i|-1$, where $\sigma(x_{i,j}) = x_{i,j+1 \bmod |O_i|}$.

- Construct $\varphi : C \to \mathbb{F}_q[t]^r$ by

$$(x_{i,j}) \mapsto \sum_{i=1}^{r} \Big(\sum_{j=0}^{|O_i|-1} x_{i,j} t^j \Big) \mathbf{e}_i$$

- For example if $x \in C$, $n = 8$ which has $\sigma =$ double right cyclic shift as an automorphism, taking $x_{1,0} = x_1$ and $x_{2,0} = x_2$, we have

$$\begin{aligned} \phi(x) &= (x_1 + x_3 t + x_5 t^2 + x_7 t^3, \\ &\qquad x_2 + x_4 t + x_6 t^2 + x_8 t^3) \end{aligned}$$

The module structure, continued

- $\varphi(C)$ is closed under sums if C is linear.

- $t \cdot \varphi(x)$, followed by "division by $t^{|O_i|} - 1$ in the ith component," gives $\varphi(\sigma(x))$.

- In example,

$$\begin{aligned} t \cdot \varphi(x) &= (x_1 t + \cdots + x_7 t^4, x_2 t + \cdots + x_8 t^4) \\ &\equiv (x_7 + \cdots + x_5 t^3, x_8 + \cdots + x_6 t^3) \\ &= \varphi(\sigma(x)) \end{aligned}$$

- Let $\pi : \mathbb{F}_q[t]^r \to \mathbb{F}_q[t]^r/O$, where $O = \langle (t^{|O_i|} - 1)\mathbf{e}_i : i = 1, \ldots, r \rangle$. Then $\pi(\varphi(C))$ is closed under multiplication by t, hence by any polynomial.

Formal statement

We have sketched the proof of:

Theorem 1 *Any linear block code C over $\mathbb{F}_q$ with a cyclic group G of automorphisms has the structure of a module over the ring $\mathbb{F}_q[t]$ (a submodule of*

$$\mathbb{F}_q[t]^r / \langle (t^{|O_i|} - 1)\mathbf{e}_i : i = 1, \ldots, r \rangle,$$

where r, O_i as above).

(Can also be generalized to non-cyclic groups G; the corresponding statement is that the code can be viewed as a submodule of a free module over the *group algebra* $\mathbb{F}_q[G]$.)

We'll see some interesting examples later.

§3. Gröbner bases for modules

- A useful tool for studying these module structures on codes is provided by the theory of Gröbner bases for modules over polynomial rings S – theory for ideals can be seen as a special case.

- We will only use the case of $S = \mathbb{F}_q[t]$ which is somewhat simpler; consult references for general theory.

- A *monomial* m in $M = \mathbb{F}_q[t]^r$ is an element of the form $m = t^i \mathbf{e}_j$, where $\mathbf{e}_j$ is the jth standard basis vector in M.

- A *monomial ordering* is a total ordering $>$ on the collection of monomials that satisfies $t^i \mathbf{e}_j > \mathbf{e}_j$ for all j and all $i > 0$, and is compatible with the module structure: $m_1 > m_2 \Rightarrow t^i m_1 > t^i m_2$, all i.

Some examples of monomial orders

- First order the $\mathbf{e}_j$ themselves; we'll use

$$\mathbf{e}_1 > \mathbf{e}_2 > \cdots > \mathbf{e}_r$$

(opposite is also possible and is used too).

- The *position over term* (or POT) ordering on $\mathbb{F}_q[t]^r$:

$$t^i \mathbf{e}_j >_{POT} t^k \mathbf{e}_\ell$$

if $j < \ell$, or $j = \ell$ and $i > k$.

- The *term over position* (or TOP) ordering on $\mathbb{F}_q[t]^r$:

$$t^i \mathbf{e}_j >_{TOP} t^k \mathbf{e}_\ell$$

if $i > k$, or $i = k$ and $j < \ell$.

Another example

In his Gröbner basis description of Reed-Solomon decoding algorithms, Fitzpatrick uses another order $>_s$ on $\mathbb{F}_q[t]^2$. Pick $s \in \mathbb{Z}$. Then $>_s$ is defined by $t^i \mathbf{e}_j >_s t^k \mathbf{e}_\ell$ if $j = \ell$ and $i > k$ and $t^i \mathbf{e}_2 >_3 t^k \mathbf{e}_1$ if $i + s \geq k$ (and opposite order if not).

For instance, with $s = 3$:

$$\mathbf{e}_1 <_3 t\mathbf{e}_1 <_3 t^2\mathbf{e}_1 < t^3\mathbf{e}_1 <_3 \mathbf{e}_2 <_3 t^4\mathbf{e}_1 <_3 \dots$$

(Whether $\mathbf{e}_1 >_s \mathbf{e}_2$ or $\mathbf{e}_1 <_s \mathbf{e}_2$ depends on sign of $s \in \mathbb{Z}$ here.)

"Gröbner basics"

- Given a monomial order $>$, every $f \in \mathbb{F}_q[t]^r$ has a unique leading term $LT_>(f)$.

- There is a division, or normal form algorithm generalizing the algorithm for polynomials.

- For any nonzero submodule $M \subset \mathbb{F}_q[t]^r$, have $LT_>(M)$, the submodule generated by all leading terms of elements of M.

- A Gröbner basis $\mathcal{G}$ for M w.r.t. $>$ is a set $\mathcal{G} \subset M$ such that the $LT_>(g)$ for $g \in \mathcal{G}$ generate the leading term submodule $LT_>(M)$.

- Have general Buchberger algorithm for computing Gröbner bases in this setting.

Gröbner basis of a code

Given a code C as in Prop 1, we consider the corresponding submodule of $\mathbb{F}_q[t]^r$, that is the submodule

$$M(C) = \langle \varphi(C) \rangle + \langle (t^{|O_i|} - 1)\mathbf{e}_i : i = 1, \ldots, r \rangle$$

A Gröbner basis for $M(C)$ will be called a *Gröbner basis for the code*.

"Toy example": Consider the code C over $\mathbb{F}_2$ with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Note C is closed under $\sigma =$ right double cyclic shift.

"Toy example," continued

- With orbits O_1, O_2 as before, the rows of G correspond to module elements

$$\begin{aligned} g_1 &= (1+t^2)\mathbf{e}_1, \\ g_2 &= (t+t^3)\mathbf{e}_1 = tg_1, \\ g_3 &= (1+t+t^2+t^3)\mathbf{e}_2. \end{aligned}$$

- $M(C) = \langle g_1, g_2, g_3 \rangle + \langle (t^4+1)\mathbf{e}_1, (t^4+1)\mathbf{e}_2 \rangle$.

- With respect to POT order, $\mathcal{G} = \{g_1, g_3\}$ is a Gröbner basis of C, since $(t^4+1)\mathbf{e}_1 = (t^2+1)g_1$ and $(t^4+1)\mathbf{e}_2 = (t+1)g_3$.

Gröbner basis encoding

When Proposition 1 holds, can use a Gröbner basis $\mathcal{G}$ for C (any monomial order) to encode:

- Information positions are the coefficients of the *non-standard* monomials (i.e. elements of $LT_>(M(C))$ of form $t^j \mathbf{e}_i$ with $j \leq |O_i| - 1$)

- Parity check positions are the *standard monomials* (i.e. in complement of $LT_>(M(C))$)

- To encode a word c, form the linear combination $f = \sum c_i m_i$ (m_i the non-standard monomials), then

- Compute $x = f - \overline{f}^{\mathcal{G}}$ (where $\overline{f}^{\mathcal{G}}$ is the remainder on division by $\mathcal{G}$.

- $\Rightarrow x \in M(C)$.

§4. AG Goppa codes and codes from order domains

Our general constructions apply to many interesting codes, e.g. some AG Goppa codes.

- Start with a smooth projective algebraic curve $X \subset \mathbb{P}^n$ defined over $\mathbb{F}_q$ (preferably with "many" $\mathbb{F}_q$-rational points).

- Let G and $D = P_1 + \ldots + P_n$ be effective divisors on X, sums of $\mathbb{F}_q$-rational points, w/ disjoint supports. Take $L(G) = \{f \in \mathbb{F}_q(X) : (f) + G \geq 0\} \cup \{0\}$.

- Define

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

  Let $C = C_L(D, G) = im(ev) \subset \mathbb{F}_q^n$.

bservations

- Can take $G = mQ$ and $D =$ sum of all other $\mathbb{F}_q$-rational points to maximize $|G|$ (gives the class of "one-point Goppa codes")

- Many interesting curves that have lots of $\mathbb{F}_q$-rational points *also* have many automorphisms fixing $G = mQ$ and D.

- Any such automorphism induces an automorphism of the code $C_L(D, mQ)$.

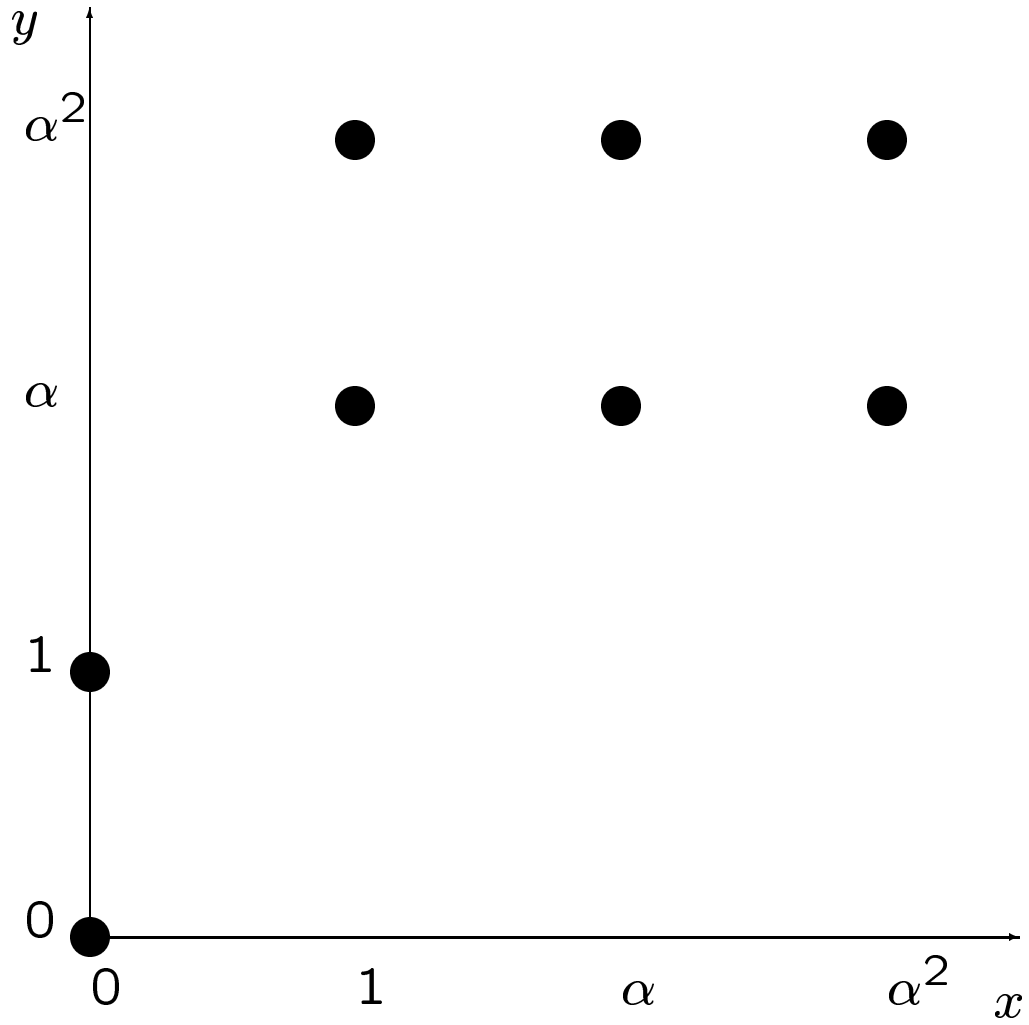
- We can take $\sigma =$ any such automorphism and use $G = \langle \sigma \rangle$.

- $\Rightarrow$ such codes have $\mathbb{F}_q[t]$-module structures, and Gröbner basis encoding.

Hermitian curve codes

- Let α be a primitive element of $\mathbb{F}_{q^2}$.
- Consider the Hermitian curve over $\mathbb{F}_{q^2}$ – $H = V(X^{q+1} - Y^q Z - Y Z^q) \subset \mathbb{P}^2$.
- H has $q^3 + 1$ $\mathbb{F}_q$-rational points: q^3 affine points: q on each line $X = cZ$ and $Q = (0 : 1 : 0)$ at infinity.
- This is the maximum possible for a curve of genus $g = q(q-1)/2$ over $\mathbb{F}_{q^2}$, by the Hasse-Weil bound: $|C(\mathbb{F}_{q^2})| \leq 1 + q^2 + 2gq$.
- Let $\sigma : (X : Y : Z) \mapsto (\alpha X : \alpha^{q+1} Y : Z)$, then σ is an auto. of H fixing Q and permuting the q^3 affine $\mathbb{F}_{q^2}$-rational points. $\Rightarrow$ Can apply the construction above.

The Hermitian curve over $\mathbb{F}_4$



$C_L(D, mQ)$'s module structure

$\sigma : (X : Y : Z) \mapsto (\alpha X : Y : Z)$ permutes the affine $\mathbb{F}_4$-rational points in 4 orbits, two of length 3, and two of length 1:

$$\begin{aligned} O_1 &= \{(1 : \alpha : 1), (\alpha : \alpha : 1), (\alpha^2 : \alpha : 1)\} \\ O_2 &= \{(1 : \alpha^2 : 1), (\alpha : \alpha^2 : 1), (\alpha^2 : \alpha^2 : 1)\} \\ O_3 &= \{(0 : 0 : 1)\} \\ O_4 &= \{(0 : \alpha : 1)\} \end{aligned}$$

Similar patterns for any $\mathbb{F}_{q^2}$: Under σ there are q orbits of length $q^2 - 1$ (all coordinates nonzero), one of length $q - 1$ ($X = 0$, $Y \neq 0$), and one of length 1 ($\{(0 : 0 : 1)\}$)

The code $C_L(D, 3\ \ )$

The affine coordinate functions $x = X/Z$ and $y = Y/Z$ are elements of $L(3Q)$, as is $1 = Z/Z$. Hence, if we order the $\mathbb{F}_4$-rational points on H in one particular way, the code $C_L(D, 3Q)$ is the span of the rows of the matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \end{pmatrix}$$

Can be seen that this code has parameters $[n, k, d] = [8, 3, 5]$ over $\mathbb{F}_4$ (best possible for this n, k).

Gröbner basis

The reduced POT Gröbner basis for the corresponding submodule of $\mathbb{F}_4[t]^4$ is:

$$\begin{aligned} g_1 &= (t+\alpha, t+\alpha, \alpha^2, \alpha^2) \\ g_2 &= (0, t^2+t+1, \alpha, \alpha^2) \\ g_3 &= (0, 0, t-1, 0) \\ g_4 &= (0, 0, 0, t-1) \end{aligned}$$

- Information positions: $t^2\mathbf{e}_1$, $t\mathbf{e}_1$, $t^2\mathbf{e}_2$.

- Parity checks: $\mathbf{e}_1$,$t\mathbf{e}_2$, $\mathbf{e}_2$, $\mathbf{e}_3$, $\mathbf{e}_4$.

rder functions

Høholdt, van Lint, and Pellikaan (building on *a lot* of previous work) introduced the following idea:

Def. Let R be a $\mathbb{F}_q$-algebra. Let $(\Gamma, +, \prec)$ be a well-ordered semigroup. An *order, or weight, function* is a surjective mapping $\rho : R \to \{-\infty\} \cup \Gamma$ satisfying:

1. $\rho(f) = -\infty \Leftrightarrow f = 0$

2. $\rho(cf) = \rho(f)$ for all $f \in R$, all $c \neq 0$ in $\mathbb{F}_q$

3. $\rho(f + g) \preceq \max_{\prec}\{\rho(f), \rho(g)\}$

4. if $\rho(f) = \rho(g) \neq -\infty$, then $\exists\ c \neq 0$ in $\mathbb{F}_q$ such that $\rho(f - cg) \prec \rho(f)$

5. $\rho(fg) = \rho(f) + \rho(g)$

First properties

- Axioms 1 and 5 imply that R must be a domain; a ring with an order function is called an *order domain*.

- Let $K = QF(R)$.

- From now on, restrict to case Γ a sub-semigroup of $\mathbf{Z}^r_{\geq 0}$, some $r \geq 1$, so *finitely generated*.

- Then WLOG, may assume $r = tr.deg._{\mathbb{F}_q}(K)$.

- "order" refers to the ordered $\mathbb{F}_q$ basis of R with distinct ρ-values guaranteed by axiom 4

Examples

- Let X be a smooth curve, $Q \in X$. $R = L(\infty Q)$ is an order domain with $\Gamma =$ Weierstrass semigroup of X at Q, $\rho(f) = -v_Q(f)$, i.e. the pole order at Q. (Goppa)

- $R = \mathbb{F}_q[X_1, \ldots, X_r]$ is an order domain taking $\Gamma = \mathbf{Z}^r_{\geq 0}$, $\prec$ a monomial order, $\rho(f) = \alpha$ if $LT_\prec(f) = X^\alpha$ for $f \neq 0$. (Reed-Muller)

- Many other ways to produce order domains from virtually any algebraic variety (of dim ≥ 1), connections with theory of valuations on function fields.

- Can also construct order domains with a given Γ.

Examples, continued

- Consider $\Gamma = \langle (0,2), (1,1), (3,0) \rangle \subset \mathbb{Z}^2_{\geq 0}$

- 3 generators for $\Gamma \Rightarrow$ a surjective ring homomorphism:

  $$\phi : \mathbb{F}_q[X, Y, Z] \to R,$$

  where $\phi(X) = x$, etc. and $\rho(x) = (0,2)$, $\rho(y) = (1,1)$, $\rho(z) = (3,0)$.

- All relations between $\rho(x)$, $\rho(y)$,$\rho(z)$ generated by $\rho(x^3z^2) = \rho(y^6)$

- Must have $\rho(y^6 - cx^3z^2) < \rho(y^6)$ for some $c \neq 0$. $\Rightarrow R \cong \mathbb{F}_q[X, Y, Z]/I$, where $I = \langle F \rangle$,

  $$F = Y^6 - cX^3Z^2 + \text{lower order terms}$$

An extrinsic characterization

Can check all such R are order domains (and all deformations of the *monomial algebra* $\mathbb{F}_q[\Gamma] = \mathbb{F}_q[v^2, uv, u^3] \cong \mathbb{F}_q[X, Y, Z]/\langle Y^6 - X^3Z^2 \rangle$). In general,

Theorem 2 *(Geil-Pellikaan) Let R be an order domain with a given finitely-generated value semigroup $\Gamma \subset \mathbf{Z}^r_{\geq 0}$. Let*

$$R_\Gamma = \mathbb{F}_q[\Gamma] \cong \mathbb{F}_q[X_1, \ldots, X_s]/I_\Gamma$$

be the "toric" algebra associated to Γ (I_Γ is a toric ideal – generated by differences of monomials). Then R has a flat deformation to R_Γ coming from a presentation of R similar to our last example above.

Codes from order domains

To construct codes from an order domain $R = \mathbb{F}_q[X_1, \ldots, X_s]/I$, generalize Goppa's construction:

- Let Δ be the ordered basis of R (ordered by ρ value) given by the monomials in complement of $LT_>(I)$
- Let $X_R = V(I)$, and $X_R(\mathbb{F}_q) = \{P_1, \ldots, P_n\}$ be the set of $\mathbb{F}_q$-rational points on X_R
- Let V_ℓ be the span of the first ℓ elements of Δ
- Let $ev : R \to \mathbb{F}_q^n$: $ev(f) = (f(P_1), \ldots, f(P_n))$
- Get codes $E_\ell = ev(V_\ell)$, $C_\ell = Ev_\ell^\perp$.

Final example – Hermitian surface codes

- Consider the Hermitian surface:

  $$\mathcal{H} = V(X_0^{q+1} + X_1^{q+1} + X_2^{q+1} - X_3^{q+1})$$

  in $\mathbb{P}^3$ over the field $\mathbb{F}_{q^2}$.

- $\mathcal{H}$ has $(q^2+1)(q^3+1)$ $\mathbb{F}_{q^2}$-rational points.

- Can introduce a linear change of coordinates to put a tangent plane to the surface as the plane at infinity.

- A tangent plane meets $\mathcal{H}$ in reducible curve made up of $q+1$ concurrent lines.

- $\Rightarrow$ affine surface is $\mathcal{H}' = V(X^{q+1} + Y^{q+1} - Z^q - Z)$, and has q^5 $\mathbb{F}_{q^2}$-rational points.

Hermitian surface codes

- Can check the affine coordinate ring also has an order domain structure.

- Have many automorphisms, e.g.

$$\sigma : (X, Y, Z) \mapsto (\alpha X, \alpha Y, \alpha^{q+1} Z)$$

(order $= q^2 - 1$)

- σ fixes plane at infinity and permutes the q^5 affine $\mathbb{F}_{q^2}$-rational points on the surface in $q^3 + q$ orbits of size $q^2 - 1$, one of size $q - 1$, and one of size 1.

- Could also use

$$\tau : (X, Y, Z) \mapsto (\alpha Y, \alpha X, \alpha^{q+1} Z)$$

(higher order if q even).

Hermitian surface codes, continued

- For instance, the code from the Hermitian surface over $\mathbb{F}_4$ constructed by evaluating $1, X, Y, Z$ has $[n, k, d] = [32, 4, 22]$

- Minimum weight codeword comes by evaluating a linear polynomial which defines the tangent plane at one of the $\mathbb{F}_{q^2}$-rational points on the surface.

- Equals best possible $n = 32$, $k = 4$ code over $\mathbb{F}_4$ (Brouwer's table).

- But also have Gröbner basis encoding, good decoding, etc. for this code because of the extra structure(!)

Comment

- Ironically, when order domains were introduced by Høholdt, van Lint, and Pellikaan, their goal was to "take the (hard) algebraic geometry out of the theory of Goppa codes" (!)

- As it turns out, their synthesis of that theory has made it possible to use even more commutative algebra and algebraic geometry to construct new examples of error control codes, generalize the existing decoding algorithms, etc.