Order Domains and Generalized Goppa Codes

John B. Little

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

little@mathcs.holycross.edu

AMS Special Session on Coding Design-Theoretic Applications of Polynomials

Phoenix, AZ

January 7, 2004

Outline of Talk

- Geometric Goppa codes
- Order domains
- Generalized Goppa codes from order domains

arXiv: `math.AC/0303299`, `math.AC/0304292`

§1. Geometric Goppa codes

- Start with a smooth projective algebraic curve X defined over $\mathbf{F}_q$, with "many" $\mathbf{F}_q$-rational points.

- Let G and D be effective divisors on X, sums of $\mathbf{F}_q$-rational points, w/ disjoint supports.

- Take $L(G) = \{f \in \mathbf{F}_q(X) : (f) + G \geq 0\} \cup \{0\}$, an $\mathbf{F}_q$-vector subspace of $\mathbf{F}_q(X)$.

- Define for $D = P_1 + \cdots + P_n$,

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

- Let $C = C_L(D, G) = im(ev) \subset \mathbf{F}_q^n$. (Note: ev is linear so C is a linear code.)

An Example

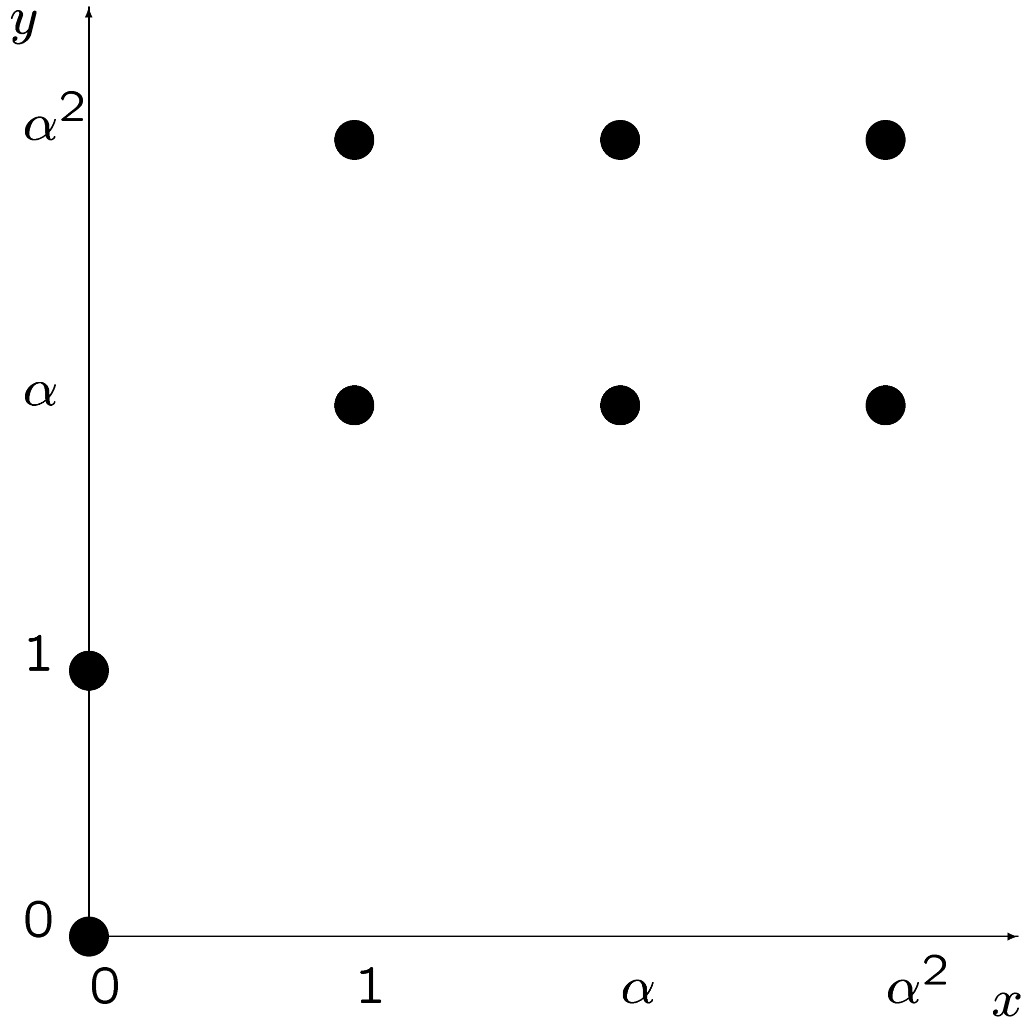
Let $q = 4$, $\mathbf{F}_4 = \mathbf{F}_2[\alpha]/\langle \alpha^2 + \alpha + 1 \rangle$ (α is primitive).

Take X to be the Hermitian curve over $\mathbf{F}_4$: $X = V(x^3 + y^2 z + y z^2) \subset \mathbf{P}^2$. X is smooth, genus $g = 1$. There are 9 $\mathbf{F}_4$-rational points on X: $Q = (0 : 1 : 0)$, and 8 affine points.

(Note: This is the maximum possible for a curve of genus 1 over $\mathbf{F}_4$, by the Hasse-Weil bound:

$$|X(\mathbf{F}_q)| \leq 1 + q + 2g\sqrt{q}.)$$

$$X(\mathbf{F}_4),\ X = V(x^3 + y^2 + y)$$



A Goppa Code from X

Take $G = mQ$, $D = \sum_{i=1}^{8} P_i$.

It can be seen easily that $x \in L(2Q)$ and $y \in L(3Q)$. In fact $L(3Q) = \text{Span}\{1, x, y\}$.

The Goppa code $C_L(D, 3Q)$ is the span of the rows of the matrix:

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

By Bézout's theorem, this code has parameters $[8, 3, 5]$ over $\mathbf{F}_4$ (any ≤ 2 errors in a received word can be corrected by nearest neighbor decoding).

§2. To "Order Domains"

- We took $G = mQ$ and $D =$ sum of all other $\mathbf{F}_q$-rational points to maximize n (gives the class of "one-point Goppa codes")

- Also, X in a "special position" (only one point at infinity) $\Rightarrow$ polynomials in affine coords give elements of $L(mQ)$, $m \geq 1$. The pole orders of the affine coord funs generate the Weierstrass semigroup of X at Q. (Can always achieve this by reembedding X by $|kQ|$, $k \geq 2g-1$ if we want.)

- Can completely describe construction of codes and a good decoding algorithm (Berlekamp-Massey-Sakata) via algebra of the ring $R = L(\infty Q) = \cup_{m=0}^{\infty} L(mQ)$, and the discrete valuation v_Q on $\mathbf{F}_q(X)$.

A Generalization

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

Def. Let R be a $\mathbf{F}_q$-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 $\mathbf{F}_q$

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 $\mathbf{F}_q$ 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 $r = tr.deg._{\mathbf{F}_q}(K)$.

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

Some Examples

- As above, $R = L(\infty Q)$ is an order domain for any point $Q \in X$, a smooth curve. $\Gamma =$ Weierstrass semigroup of X at Q, $\rho(f) = -v_Q(f)$. (Goppa)

- $R = \mathbf{F}_q[X_1, \ldots, X_r]$ 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)

- Can construct all order domains with a given Γ, as in following example. Take $r = 2$, $\Gamma = \langle (0,2), (1,1), (3,0) \rangle \subset \mathbf{Z}^2_{\geq 0}$ ordered by graded lex (for example).

Examples, cont.

- 3 generators for $\Gamma \Rightarrow$ there is a surjective ring homomorphism:
$$\phi : \mathbf{F}_q[X, Y, Z] \to R,$$
where if $\phi(X) = x$, $\phi(Y) = y$, etc. $\rho(x) = (0, 2)$, $\rho(y) = (1, 1)$, $\rho(z) = (3, 0)$.

- Easy to see that all relations between $\rho(x)$, $\rho(y)$,$\rho(z)$ are generated by $\rho(x^3z^2) = \rho(y^6)$

- For axioms to hold, must have $\rho(y^6 - cx^2z^3) < \rho(y^6)$ for some $c \neq 0$. $\Rightarrow R \cong \mathbf{F}_q[X, Y, Z]/I$, where $I = \langle F \rangle$,
$$F = Y^6 - cX^2Z^3 + \text{lower order terms}$$

- Can check all such R are order domains (and all deformations of the *monomial algebra* $\mathbf{F}_q[\Gamma] = \mathbf{F}_q[v^2, uv, u^3]$).

An "Extrinsic" Characterization

Theorem 1 *(Geil-Pellikaan, -) Let R be an order domain with a given finitely-generated value semigroup $\Gamma \subset \mathbf{Z}^r_{\geq 0}$. Let*

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

be the monomial (or toric) algebra associated to Γ. Then R has a flat deformation to R_Γ (coming from a presentation of R similar to our last example above).

Order Domains and Valuations

On the other hand, there is a close connection between order domains and *valuations* on function fields (recall the Goppa code case!)

- If R is an order domain with field of fractions K, then

  $$S_\rho = \{f/g \in K : \rho(g) \geq \rho(f)\}$$

  is a *valuation ring* in K (that is, for all $h \neq 0$ in K, either $h \in S_\rho$, or $1/h \in S_\rho$).

- S_ρ is a local ring with maximal ideal $M_\rho = \{f/g \in K : \rho(g) > \rho(f)\}$.

- R is in a special "$\mathbf{F}_q$-complementary position to S_ρ" in K: $S_\rho \cap R = \mathbf{F}_q$ and $S_\rho = S_\rho \cap R + M_\rho$.

Order Domains and Valuations, cont.

- Conversely, using results of Mosteig and Sweedler, can show

  Theorem 2 *(-) Any valuation on a function field, with rational rank equal to the transcendence degree, with center a point "at infinity" on a projective model yields a corresponding order domain in the function field.*

- see (-), `arXiv:math.AC/0304292` for more details.

- In particular, applies to varieties of interest in coding theory (Hermitian hypersurfaces, Grassmannians, flag varieties, ...)

Codes From Order Domains

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

- Let Δ be the ordered basis of R (ordered by ρ value, or equiv. w-weight) given by the monomials in complement of $LT_>(I)$

- Let $X_R = V(I)$, and $X_R(\mathbf{F}_q) = \{P_1, \ldots, P_n\}$ be the set of $\mathbf{F}_q$-rational points on X_R

- Let V_ℓ be the span of the first ℓ elements of Δ

- Let $ev : R \to \mathbf{F}_q^n$: $ev(f) = (f(P_1), \ldots, f(P_n))$

- Get codes $E_\ell = ev(V_\ell)$, $C_\ell = Ev_\ell^\perp$.

Codes From Order Domains, cont.

- Results of O'Sullivan $\Rightarrow$ many features of one-point Goppa codes generalize to these codes from *all* order domains: Good bounds on minimum distance of C_ℓ codes (Feng-Rao-Duursma) tied to an efficient decoding algorithm (B-M-S)

- Construction of good codes by this method still requires finding X_R with many $\mathbf{F}_q$-rational points, good minimum distance properties, ...

- On the other hand, there is the possibility of exploiting known higher-dimensional varieties of interest.

Final Example

Consider the Hermitian surface:

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

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

- $V_1 = V(X_0)$ is a smooth Hermitian curve on $\mathcal{H}$

- $V_2 = \{(0 : 1 : \delta : 0)\}$ is a point on V_1 if $\delta^{q+1} = -1$.

- From standard construction of *composite divisorial valuations* corresponding to flags of subvarieties, we get an order domain structure on the ring $L(\infty V_1)$ on $\mathcal{H}$ (the subring of the function field consisting of functions with poles only along V_1 (arbitrary order).

Hermitian Surface Codes

- Can also derive explicit presentation as deformation of the toric algebra for

$$\Gamma = \langle (1,q),(1,q+1),(1,0)\rangle$$

- $\mathcal{H}$ has $(q^2+1)(q^3+1)$ $\mathbf{F}_{q^2}$-rational points, of which q^3+1 lie on the plane section V_1. $\Rightarrow$ we get generalized Goppa codes from $\mathcal{H}$ with $n = q^2(q^3+1) = q^5+q^2$.

- With $\ell = 4$, for instance, we evaluating $1, X_1, X_2, X_3$ yields E_4 code with $k = 4$ and $d = q^5 - q^3$ (maximum number of zeroes is $(q+1)q^2 = q^3+q^2$).

- With $q = 2$, for example $d = 2^5 - 2^3 = 24$ (best known code with $n = 36, k = 4$ over $\mathbf{F}_4$ has $d = 25$)

Conclusion

- 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.

Some Questions

Some natural questions at this point:

- How general is the order domain construction? i.e. What algebraic varieties give examples of order domains? Is there anything special about curves (as in Goppa's construction)?

- What is the construction of corresponding codes?

- What other properties do those codes have, such as existence of good decoding algorithms?