Order Domains

John B. Little

Department of Mathematics and Computer Science

College of the Holy Cross

little@mathcs.holycross.edu

Algebra Seminar

University of South Alabama

April 6, 2007

Outline of Talk

- Order domains
- Examples
- History, connections with coding theory
- Generalized Goppa codes from order domains

preprints on this on arXiv: `math.AC/0303299`, `math.AC/0304292`

Weight and Order Functions

Definition. Let R be a commutative k-algebra, and let $(\Gamma, +, \prec)$ be a well-ordered semigroup. An *weight function* on R is a surjective

$$\rho : R \to \{-\infty\} \cup \Gamma$$

satisfying:

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

2. $\rho(cf) = \rho(f)$ for all $f \in R$, all $c \neq 0$ in k

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 k such that $\rho(f - cg) \prec \rho(f)$

5. $\rho(fg) = \rho(f) + \rho(g)$ for all $f, g \in R$,

(If only 1 - 4 hold, then ρ is an order function.)

Order Domains – First Properties

- All examples we consider will have *weight* functions.

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

- Let $K = QF(R)$.

- From one point of view, order functions "really come from" *valuations* on K (see Axiom 3). We'll return to this point.

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

$$r = tr.deg._k(K).$$

First Examples

- $R = k[x]$, $\rho : R \to \mathbf{Z}_{\geq 0} \cup \{-\infty\}$ the degree mapping.

- Note: $K = k(x)$ is the rational function field in one variable $\leftrightarrow$ the projective line, $\mathbf{P}^1$, and $\rho(f) =$ "order of pole at ∞".

- If X/k is an algebraic curve ($k(X)$ is a function field of transcendence degree 1 over k), Q is a smooth k-rational point (place of degree 1) of X, $a \geq 0$, define $L(aQ) = \{f \in k(X) : f$ has a pole of order $\leq a$ at Q and no other poles$\} \cup \{0\}$. Then

$$\begin{aligned} R &= L(\infty Q) \\ &= \cup_{a \geq 0} L(aQ) \end{aligned}$$

  is an order domain, with $\rho(f) = -v_Q(f)$ (v_Q the discrete valuation at Q – the "pole order"). $\Gamma =$ Weierstrass semigroup of X at Q.

Some Questions

Some natural questions at this point:

- How general is the order domain construction?
- Is there anything special about curves?
- Do other algebraic varieties give examples of order domains?
- Why would anyone be especially interested in these rings?

More Examples

- $R = k[X_1, \ldots, X_r]$ is an order domain with $\Gamma = \mathbf{Z}^r_{\geq 0}$, $\succ$ any monomial order (as in my colloquium talk yesterday), $\rho(f) = \alpha$ if $LT_{\succ}(f) = cx^{\alpha}$, $c \neq 0 \in k$.

- Say $r = 2$, $\Gamma = \langle (3,0), (1,1), (0,2) \rangle \subset \mathbf{Z}^2_{\geq 0}$ ordered by graded lex (for example). Say R is an order domain with this Γ as value semigroup.

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

  $$\phi : k[X, Y, Z] \to R,$$

  where if $\phi(X) = x$, $\phi(Y) = y$, $\phi(Z) = z$, $\rho(x) = (3,0)$, $\rho(y) = (1,1)$, $\rho(z) = (0,2)$.

Examples, cont.

- Easy to see that all relations between the generators for Γ are generated by

$$2 \cdot (3,0) + 3 \cdot (0,2) = 6 \cdot (1,1)$$

So $\rho(x^2z^3) = \rho(y^6)$.

- From Axiom 4, must have

$$\rho(y^6 - cx^2z^3) < \rho(y^6)$$

for some $c \neq 0$. So $R \cong k[X,Y,Z]/I$, where $I = \langle F \rangle$ for some F of the form

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

- Can check all such R are order domains, and all are flat deformations of the *semi-group algebra* $k[\Gamma] = k[u^3, uv, v^2]$.

An "Extrinsic" Characterization

Theorem 1 *(Geil-Pellikaan) Let G be a Gröbner basis for*

$$I \subset k[X_1, \ldots, X_s]$$

with respect to a weight order $> = >_{w,\tau}$, w some s-tuple of weight vectors.

1. *Suppose that the monomials in the complement of $LT_>(I)$ have distinct w-weights, and that every element of G has exactly two monomials of highest weight in its support. Then $R = k[X_1, \ldots, X_s]/I$ is an order domain with*

$$\rho(f) = \max_{\prec}\{w(m) : m \in supp(f)\}.$$

2. *Conversely, every order domain with semigroup $\Gamma = \langle w \rangle$ can be obtained this way.*

Connections

A reinterpretation of this result makes some quite interesting connections with recent work on "toric deformations" in combinatorics, theory of singularities, mirror symmetry, ...

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

$$R_\Gamma = k[\Gamma] \cong k[X_1, \ldots, X_s]/I_\Gamma$$

be the semigroup (or toric) algebra associated to Γ. Then R has a flat deformation to R_Γ. Conversely, every flat deformation of R_Γ of the form given in Geil and Pellikaan's theorem is an order domain with value semigroup Γ.

Example – Grassmannians

- The Grassmannian $G(k,n)$ is a projective variety whose points are in one-to-one correspondence with the k-dimensional vector subspaces of an n-dimensional vector space.

- The $\mathbb{F}$-rational points of $G(k,n)$ correspond to linear subspaces defined over $\mathbb{F}$.

- Given any basis $\{v_1, \ldots, v_k\}$ for a k-dimensional vector subspace W of $\overline{\mathbb{F}}^n$, we form the $k \times n$ matrix with rows v_i. The $k \times k$ (maximal) minors of this matrix are components of the *Plücker coordinate vector* of W in $\mathbb{P}^{\binom{n}{k}-1}$.

- The locus of all such points (for all W) forms the Grassmannian $G(k,n)$.

A Toric Deformation of $G(k,n)$

Theorem 3 *(B. Sturmfels) There exists a toric deformation taking $G(k,n)$ to the projective toric variety defined by a semigroup $\Gamma_{k,n}$ defined as follows:*

- *Let $N = (t_{ij})$ be a generic $k \times n$ matrix (t_{ij} independent indeterminates).*

- *$\Gamma_{k,n}$ is the semigroup in $\mathbb{Z}_{\geq 0}^{\binom{n}{k}}$ generated by the columns of the $\binom{n}{k} \times kn$ matrix whose ℓth row has 1's in the positions corresponding to the t_{ij} in the diagonal of the ℓth minor of N and zeroes in all other positions.*

An Example

Let

$$N = \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{15} \\ t_{21} & t_{22} & \cdots & t_{25} \\ t_{31} & t_{32} & \cdots & t_{35} \end{pmatrix}$$

be the generic 3×5 matrix. There are $\binom{5}{3} = 10$ maximal minors of N. The diagonal terms are

$$t_{11}t_{22}t_{33}, t_{11}t_{22}t_{34}, \ldots, t_{13}t_{24}t_{35}.$$

Form a (0,1)-matrix $\mathcal{B}_{3,5}$ recording which variables appear in the diagonal terms of each maximal minor – columns of $\mathcal{B}_{3,5}$ generate the semigroup $\Gamma_{3,5}$.

Example, continued

Write $X_1, \ldots, X_{10}$ for the coordinates in $\mathbb{P}^9$. The toric variety corresponding to $\mathbb{F}[\Gamma_{3,5}]$ is given by the parametrization

$$X_1 = t_{11}t_{22}t_{33}, X_2 = t_{11}t_{22}t_{34}, \ldots, X_{10} = t_{13}t_{24}t_{35}$$

Eliminating the t_{ij}, we find the graded reverse lex Gröbner basis of $I_{\Gamma_{3,5}}$ equals

$$\begin{aligned} G_T = \{ \; & X_8X_6 - X_9X_5, \\ & X_7X_6 - X_4X_9, \\ & X_7X_5 - X_8X_4, \\ & X_7X_3 - X_8X_2, \\ & X_4X_3 - X_5X_2 \; \}. \end{aligned}$$

(the positive term is the leading term in each case). The corresponding projective toric variety has dimension 6 and degree 5 in $\mathbb{P}^9$.

Example, continued

The ideal of the Grassmannian $G(3,5)$ is generated by quadratic polynomials called the *Plücker relations* between the Plücker coordinate vectors of 3-planes W. We have the following Gröbner basis for this ideal with respect to the same graded reverse lex order as before:

$$\begin{aligned} G_G = \{ \; & X_8X_6 - X_9X_5 + X_3X_{10}, \\ & X_7X_6 - X_4X_9 + X_2X_{10}, \\ & X_7X_5 - X_8X_4 + X_1X_{10}, \\ & X_7X_3 - X_8X_2 + X_1X_9, \\ & X_4X_3 - X_5X_2 + X_1X_6 \; \}. \end{aligned}$$

Example, concluded

Note that in each polynomial in G_G, the same two terms as in the corresponding polynomial in G_T appear. These are the terms of maximum weight in each case. So the ideal $\langle G_T \rangle$ defines a toric deformation of (the affine cone over) the Grassmannian.

Can check Geil and Pellikaan's condition on weights of basis monomials for quotient is satisfied.

Therefore, $\mathbb{F}[X_1, \ldots, X_{10}]/\langle G_G \rangle$ has an order domain structure.

Order Domains and Valuations

On the other hand, there is a close connection between order domains and *valuations* on function fields.

- 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 4 *Any valuation on a function field of rational rank equal to the dimension of the variety, with center a point "at infinity" on some projective model yields a corresponding order domain in the function field.*

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

- see (-), `arXiv:math.AC/0304292` (Advances in Mathematics of Communications, v.1) for more details.

Some History and Background

- Order domains were first defined in general by Høholdt, van Lint, Pellikaan for use in *algebraic coding theory* around 1998.

- A code is a set of codewords – our cases, vector subspaces $C \subset \mathbb{F}_q^n$

- Parameters of a code: $[n, k, d]$, $n =$ block-length, $k = \dim(C)$, $d =$ minimum Hamming distance between distinct codewords (measures error-detection/correction capacity).

- A "big story" from mid-1980's through 1990's was the development of AG Goppa codes from algebraic curves over $k = \mathbb{F}_q$.

A Goppa Example

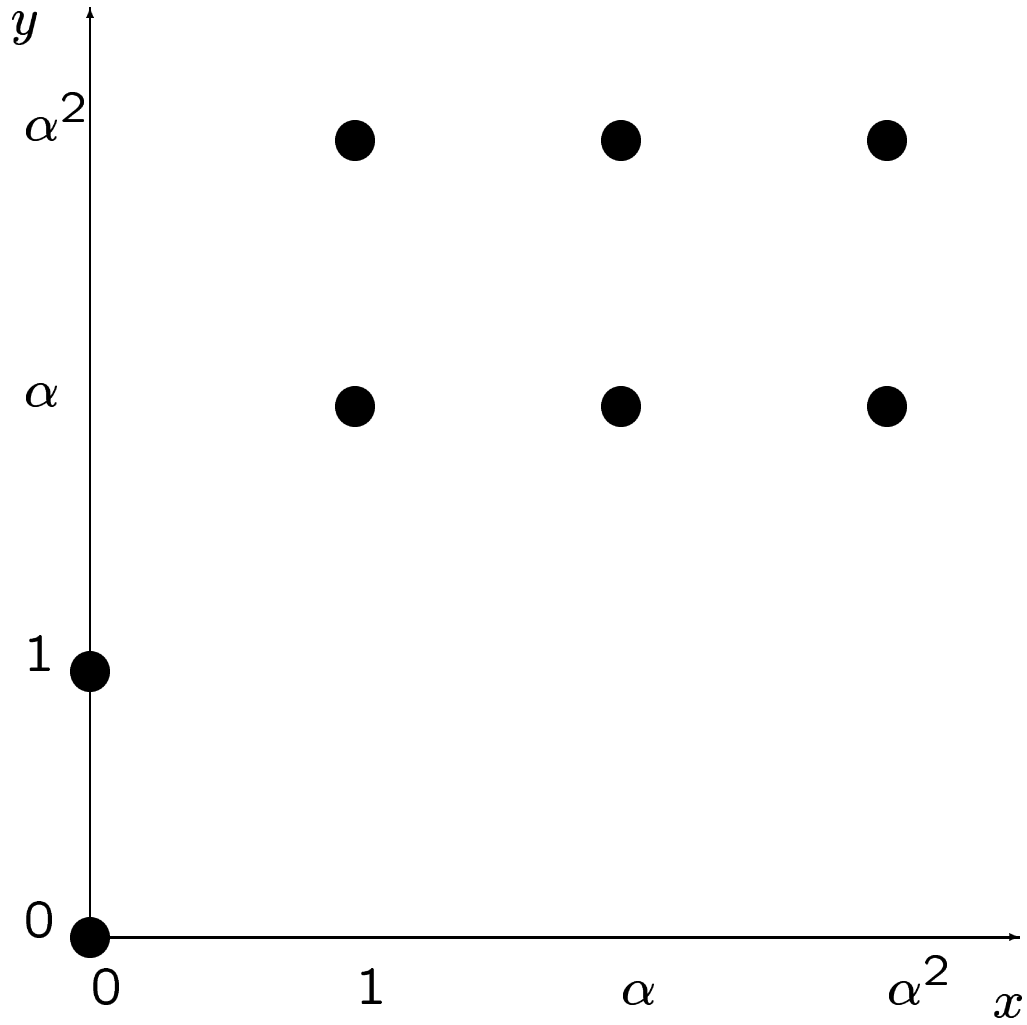
Let $q = 4$, $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/\langle \alpha^2 + \alpha + 1 \rangle$ (α is primitive).

Take $X = V(x^3 + y^2z + yz^2) \subset \mathbf{P}^2$. 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 $L(3Q) = \mathsf{Span}\{1, x, y\}$.

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).

Genesis of Order Domains

- Order domains give a framework to understand many previously constructed families of codes, and good decoding algorithms.

- $R = \mathbf{F}_q[x] \leftrightarrow$ Reed-Solomon codes, Berlekamp-Massey.

- $R = L(aQ) \leftrightarrow$ "one-point" Goppa codes from curves, Berlekamp-Massey-Sakata.

- $R = \mathbf{F}_q[x_1, \ldots, x_r] \leftrightarrow$ Reed-Muller codes.

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 $Ev_\ell = ev(V_\ell)$, $C_\ell = Ev_\ell^\perp$.

Codes From Order Domains, cont.

- Construction of good codes by this method still requires finding X_R with many $\mathbf{F}_q$-rational points (hard arithmetic problems)

- On the other hand, there is the possibility of exploiting known higher-dimensional varieties that do (Hermitian hypersurfaces, Grassmannians, flag varieties, ...), and

- Results of O'Sullivan: Many very nice features of one-point Goppa codes generalize to all codes from order domains:

- Good bounds on minimum distance (Feng-Rao-Duursma) tied to a very efficient decoding algorithm (Berlekamp-Massey-Sakata)

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.