

# On the structure of order domains

Ruud Pellikaan

(Technical University of Eindhoven)

joint work with

Olav Geil (Aalborg University)

Euroconference on Crete, August 2000

## Abstract

- Definition of an order domain.
- Value semigroup.
- The theory of Gröbner bases for order domains.
- Factor ring theorem.
- Presentation theorem.
- Dimension (order domain) = rank (value semigroup).

- Algebraic geometry codes on a more elementary foundation.
  - Parameters  $[n, k, d]$  of these codes
  - Order bound for the minimum distance
  - Generalized Hamming weights
- References:
  - Feng-Rao
  - Høholdt-Van Lint-Pellikaan
  - Heijnen-Pellikaan

- Efficient decoding algorithm
  - Basic algorithm
  - Majority voting of unknown syndromes
  - Algorithm of Berlekamp-Massey-Sakata.
  
- References:
  - Justesen-Larsen-Jensen-Havemose-Hoeholdt
  - Skorobogatov-Vladut
  - Feng-Rao, Duursma
  - Sakata
  - O'Sullivan
  - Høholdt-Van Lint-Pellikaan

- Theory of Gröbner bases
- Construction of new order domains,  
Factor ring theorem
- Converse: Presentation theorem
- References:
  - Heegard-Little-Saints
  - O'Sullivan
  - Matsumoto-Miura
  - Geil-Pellikaan

- Value semigroup
- Valuation theory
- Dimension (order domain) = rank (value semigroup)
- Surprising example:
  - order domain in  $\mathbb{F}[X, Y]$
  - value semigroup in  $\mathbb{Q}$
- References:
  - O'Sullivan
  - Geil-Pellikaan

Notation:

- Let  $(\Gamma, <)$  be a well-order.
- The minimal element is denoted by  $0$ .
- $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$  is the order with  $-\infty$  as minimal element.
- Let  $\mathbb{F}$  be a field.
- Let  $R$  be an  $\mathbb{F}$ -algebra.

An *order function* on  $R$  is a surjective map

$$\rho : R \longrightarrow \Gamma_{-\infty},$$

such that for all  $f, g, h \in R$ :

- $\rho(f) = -\infty$  if and only if  $f = 0$ ,
- $\rho(af) = \rho(f)$  for all nonzero  $a \in \mathbb{F}$ ,
- $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$ ,
- and equality holds if  $\rho(f) \neq \rho(g)$ ,
- If  $\rho(f) \leq \rho(g)$ , then  $\rho(fh) \leq \rho(gh)$ ,
- If  $f$  and  $g$  are nonzero and  $\rho(f) = \rho(g)$ , then there exists a nonzero  $a \in \mathbb{F}$  such that

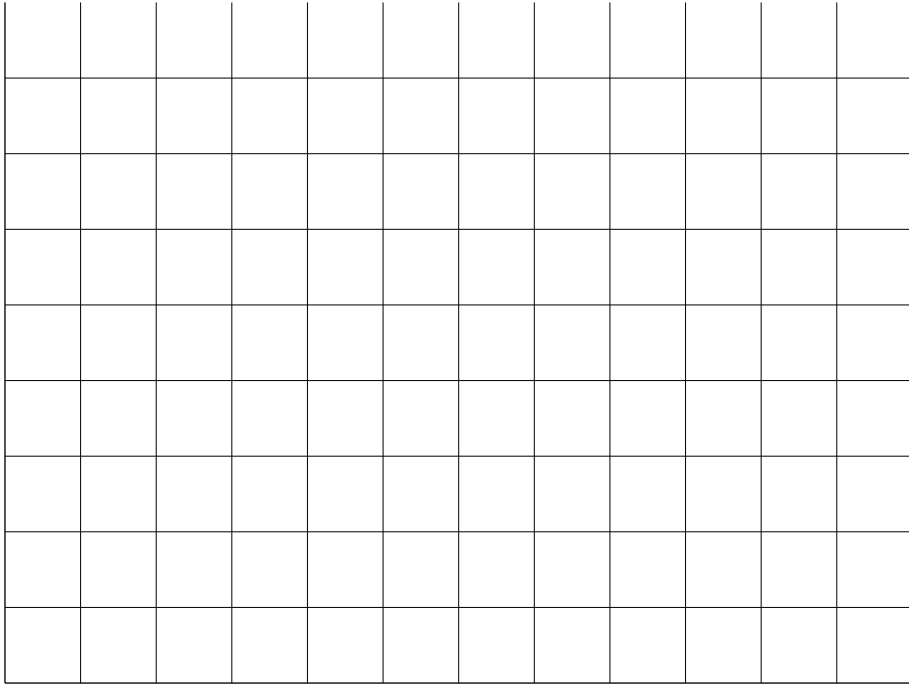
$$\rho(f - ag) < \rho(g).$$



## Examples

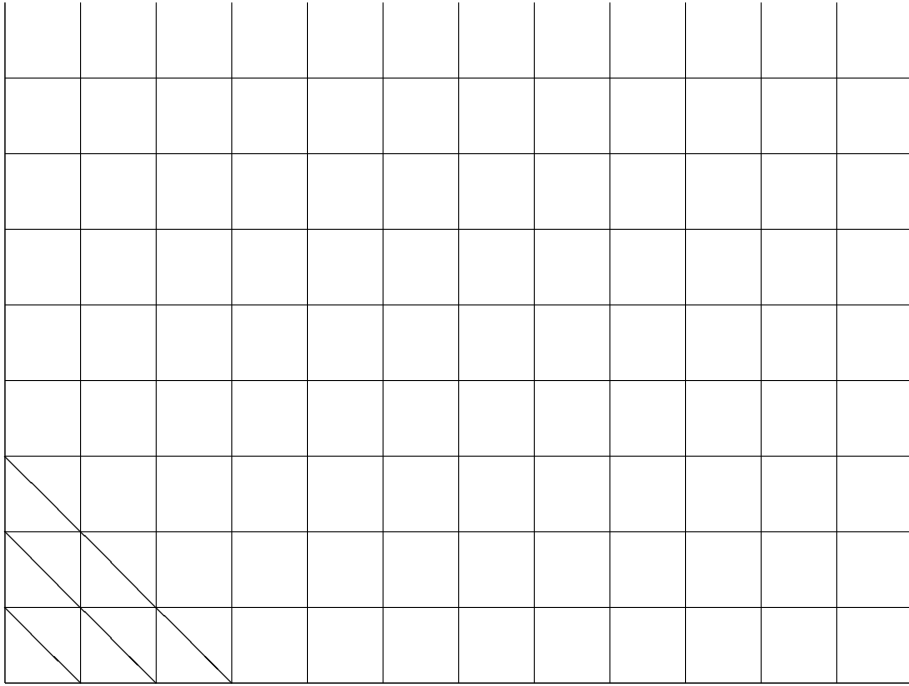
- –  $R = \mathbb{F}[X]$ 
  - $\rho = \deg$
- –  $R = K_P(\mathcal{X})$  the ring of rational functions on an algebraic curve  $\mathcal{X}$  with no poles outside the point  $P$ 
  - $\rho = -v_P$  the pole order at  $P$ ,  
 $v_P$  is the valuation at  $P$ .

- $R = \mathbb{F}[X, Y]$
- $\Gamma = \mathbb{N}_0^2$  with lexicographic order  $<_{lex}$ .
  - $(\alpha_1, \alpha_2) <_{lex} (\beta_1, \beta_2)$  iff
  - $\alpha_1 < \beta_1$ , or  $\alpha_1 = \beta_1$  and  $\alpha_2 < \beta_2$ .
- Multi-index notation:  $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2}$
- – Let  $f = \sum_{\alpha \leq \gamma} a_\alpha X^\alpha$ 
  - with  $a_\alpha \in \mathbb{F}$  and  $a_\gamma \neq 0$ .
- Then  $\rho(f) = \gamma$ .



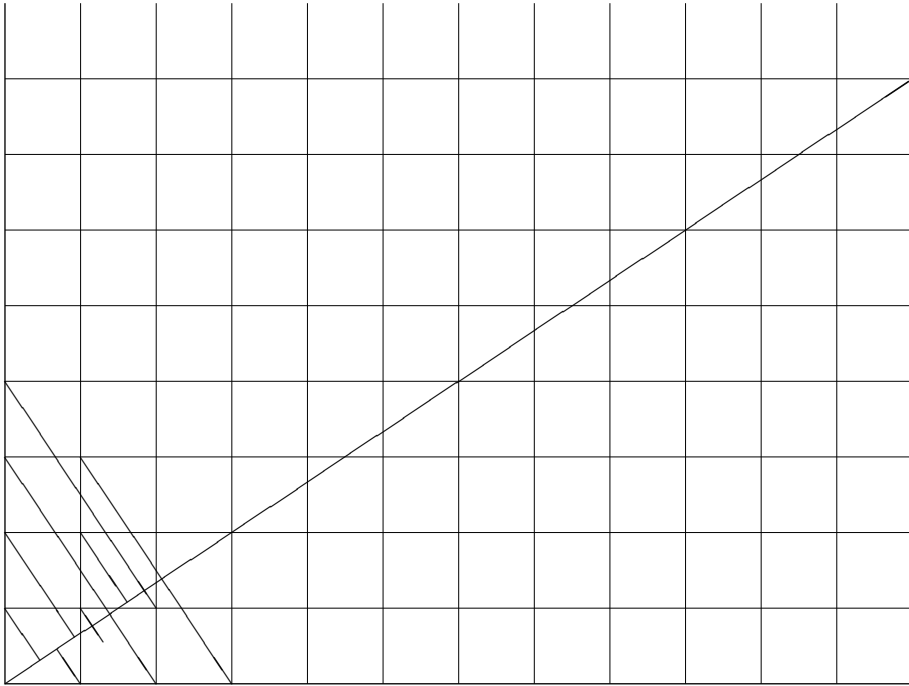
$$\begin{array}{cccccccc} & (0, 0) & < & (0, 1) & < & \dots & < & (0, n) & < & \dots \\ < & (1, 0) & < & (1, 1) & < & \dots & < & (1, n) & < & \dots \\ & & & & & & \vdots & & & & \\ < & (m, 0) & < & (m, 1) & & \dots & < & (m, n) & < & \dots \end{array}$$

- $R = \mathbb{F}[X, Y]$
- $\Gamma = \mathbb{N}_0^2$ 
  - with total degree lexicographic order  $<_{dlex}$ .
  - $(\alpha_1, \alpha_2) <_{dlex} (\beta_1, \beta_2)$  iff
  - $\alpha_1 + \alpha_2 < \beta_1 + \beta_2$ , or
  - $\alpha_1 + \alpha_2 = \beta_1 + \beta_2$  and  $\alpha <_{lex} \beta$ .



$(0, 0) <$   
 $(0, 1) < (1, 0) <$   
 $(0, 2) < (1, 1) < (2, 0) <$   
 $(0, 3) < (1, 2) < (2, 1) < (3, 0) < \dots$

- $R = \mathbb{F}[X, Y]$
- $\Gamma = \mathbb{N}_0^2$
- $\mathbf{w} = (w_1, w_2) \in \mathbb{N}^2$ 
  - with total weighted degree lexicographic order  $<_{wlex}$ .
  - $(\alpha_1, \alpha_2) <_{wlex} (\beta_1, \beta_2)$  iff
  - $\alpha_1 w_1 + \alpha_2 w_2 < \beta_1 w_1 + \beta_2 w_2$ , or
  - $\alpha_1 w_1 + \alpha_2 w_2 = \beta_1 w_1 + \beta_2 w_2$
  - and  $\alpha <_{wlex} \beta$ .



$(0, 0) <$   
 $(0, 1) < (1, 0) <$   
 $(0, 2) < (1, 1) < (0, 3) < (2, 0) <$   
 $< (1, 2) < (0, 4) < (2, 1) <$   
 $< (1, 3) < (3, 0)$

- $R = \mathbb{F}[X, Y]$

- $\Gamma = \mathbb{N}_0^2$

- with order  $<$ .

- $(\alpha_1, \alpha_2) < (\beta_1, \beta_2)$  iff

- $\alpha_1\sqrt{2} + \beta_1 < \alpha_2\sqrt{2} + \beta_2$ .





$(0, 0) <$   
 $(0, 1) < (1, 0) <$   
 $(0, 2) < (1, 1) < (2, 0) <$   
 $(0, 3) < (1, 2) < (2, 1) <$   
 $(0, 4) < (3, 0) < (1, 3) < (2, 2) < \dots$

- The admissible well-orders on  $\mathbb{N}_0^r$  are all classified (Robbiano).
- Let  $\mathbf{a} \cdot \mathbf{b}$  be the standard innerproduct.
- – There exist  $\mathbf{a}_1, \dots, \mathbf{a}_s$  in  $\mathbb{R}_+^r$  such that
  - for  $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^r$ :  $\mathbf{a} < \mathbf{b}$
  - if and only if there exists a  $t$  such that
  - $\mathbf{a} \cdot \mathbf{a}_i = \mathbf{b} \cdot \mathbf{a}_i$  for all  $i < t$  and  $\mathbf{a} \cdot \mathbf{a}_t < \mathbf{b} \cdot \mathbf{a}_t$ .
- The smallest  $s$  is called the *height* of the order.

- The order  $<$  is isomorphic to
  - $(\mathbb{N}_0, <)$  iff the coordinates of  $\mathbf{a}_1$  are all positive.
  - $<_{lex}$  iff  $s = r$  and  $\mathbf{a}_1 = \mathbf{e}_1, \dots, \mathbf{a}_r = \mathbf{e}_r$  the standard basis.
  - $<_{dlex}$  iff  $s = r$  and  $\mathbf{a}_1 = (1, 1, \dots, 1)$  and  $\mathbf{a}_2 = \mathbf{e}_2, \dots, \mathbf{a}_r = \mathbf{e}_r$ .
  - $<_{wlex}$  iff  $s = r$  and  $\mathbf{a}_1 = (w_1, w_2, \dots, w_r)$  and  $\mathbf{a}_2 = \mathbf{e}_2, \dots, \mathbf{a}_r = \mathbf{e}_r$ .



- **Proposition:**

If there exists an order function on  $R$ ,  
then  $R$  is an integral domain

- $(R, \rho, \Gamma)$  is called an *order structure* over  $\mathbb{F}$   
if

- $\mathbb{F}$  is a field

- $R$  is an  $\mathbb{F}$ -algebra

- $\Gamma$  a well-order

- $\rho : R \rightarrow \Gamma_{-\infty}$  an order function

- Then  $R$  is called an *order domain*.

- **Question:**

Which rings are order domains and how do  
we construct them ?

## Well-behaving bases

- Let  $R$  be an  $\mathbb{F}$ -algebra.
- Let  $\Gamma$  be a well-order.
- Let  $(f_\alpha \mid \alpha \in \Gamma)$  be a basis of  $R$  over  $\mathbb{F}$ .
- $R_\gamma$  be the subspace of  $R$  generated by  $(f_\alpha \mid \alpha \leq \gamma)$ .
- Define

$$l(\alpha, \beta) = \min\{ \gamma \in \Gamma \mid f_\alpha f_\beta \in R_\gamma \}.$$

- The basis is called *well-behaving*, if

$$\alpha < \beta \quad \Rightarrow \quad l(\alpha, \gamma) < l(\beta, \gamma)$$

for all  $\alpha, \beta, \gamma \in \Gamma$ .

## Proposition:

- Let  $(R, \rho, \Gamma)$  be an order structure.
- Let  $(f_\alpha \mid \alpha \in \Gamma)$  be a sequence of elements in  $R$  such that  $\rho(f_\alpha) = \alpha$  for all  $\alpha \in \Gamma$ .
- Then this is a well-behaving basis.
- So there exists a well-behaving basis.

## Proposition:

- Let  $(\Gamma, <)$  be a well-order.
- Let  $(f_\alpha \mid \alpha \in \Gamma)$  be a well-behaving basis.
- Define  $\rho(f) = -\infty$  if  $f = 0$ .
- Otherwise  $\rho(f) = \gamma$ , where  $\gamma$  is the minimal element of  $\Gamma$  such that  $f \in R_\gamma$ .
- Then  $(R, \rho, \Gamma)$  is an order structure.



## Proposition:

- Let  $\mathbb{F}$  be a subfield of  $\mathbb{G}$ .
- Let  $(R, \rho, \Gamma)$  be an order structure over  $\mathbb{F}$ .
- Then  $(R \otimes_{\mathbb{F}} \mathbb{G}, \rho, \Gamma)$  is an order structure over  $\mathbb{G}$ .

## The value semigroup

- Let  $(R, \rho, \Gamma)$  be an order structure.
- The function  $l(\alpha, \beta)$  does not depend on the chosen well-behaving basis, since
  - $R_\gamma = \{ f \in R \mid \rho(f) \leq \gamma \}$ .
  - $l(\alpha, \beta) = \min\{ \gamma \mid R_\alpha R_\beta \subseteq R_\gamma \}$ .
- The binary operation  $+$  on  $\Gamma$  is defined by

$$\alpha + \beta = l(\alpha, \beta).$$

- The minimum element of  $\Gamma$  is denoted by

0

.

- Let  $(R, \rho, \Gamma)$  be an order structure.
- Then  $(\Gamma, +, 0, <)$  is a well-ordered semi-group.
- That means that the operation  $+$  is
  - associative:  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ ,
  - commutative:  $\alpha + \beta = \beta + \alpha$ ,
  - cancellative:  $\alpha + \gamma = \beta + \gamma \Rightarrow \alpha = \beta$ ,
  - 0 is the neutral element:  $\alpha + 0 = \alpha$ ;
- and the well-order  $<$  is admissible:
 
$$0 \leq \alpha \text{ and, } \alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma.$$
- Furthermore  $+$  is inverse free:
 
$$\alpha + \beta = 0 \Rightarrow \alpha = \beta = 0.$$

- Let  $(R, \rho, \Gamma)$  be an order structure.
- From now on the well-order  $\Gamma$  is a well-ordered semigroup.
- Thus  $\rho(fg) = \rho(f) + \rho(g)$  for all  $f, g \in R$ .

- Let  $(\Gamma, +, 0, <)$  be a well-ordered semigroup.

- The *semigroup algebra*  $\mathbb{F}[\Gamma]$  has as basis  $( X^\alpha \mid \alpha \in \Gamma )$ .

- The multiplication is defined by

$$X^\alpha X^\beta = X^{\alpha+\beta}$$

and extended linearly.

- Then the basis  $( X^\alpha \mid \alpha \in \Gamma )$  is well-behaving, and

- $\mathbb{F}[\Gamma]$  is an order domain.

- Let  $(R, \rho, \Gamma)$  be an order structure.
- If  $\Gamma$  is a finitely generated semigroup, then  $R$  is a finitely generated algebra over  $\mathbb{F}$ .
- Then  $R \cong \mathbb{F}[X_1, \dots, X_m]/I$ .
- The converse is not true.
- The order structure is called *finitely generated* or *Noetherian* if  $(\Gamma, +)$  is a finitely generated semigroup.

- Let  $(\Gamma, +, 0)$  be a semigroup.
- Let  $D(\Gamma)$  be the *group of differences* of  $\Gamma$ .
- The *rank* of  $\Gamma$  is defined by

$$\dim_{\mathbb{Q}} D(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

- If  $\Gamma$  is finitely generated semigroup, then  $D(\Gamma)$  is a finitely generated abelian group.
- Hence

$$D(\Gamma) \cong \mathbb{Z}^r \oplus T,$$

- where  $r$  is the rank of  $\Gamma$ ,
- and  $T$  a (finite) torsion group.

## Proposition:

- Let  $(\Gamma, +, 0)$  be an inverse-free semigroup.
- Let  $\Gamma$  be finitely generated and of rank  $r$ .
- Then there exists an embedding

$$\varphi : \Gamma \rightarrow \mathbb{N}_0^r$$

of semigroups such that

$$D(\varphi(\Gamma)) = \mathbb{Z}^r.$$

- Furthermore  $r$  is the smallest integer such that there exist an embedding of  $\Gamma$  in  $\mathbb{N}_0^r$ .



- Let  $(R, \rho, \Gamma)$  be a finitely generated order structure of rank  $r$ .
- Then  $\Gamma$  is a finitely generated inverse-free semigroup.
- Hence  $\Gamma$  can be viewed as a sub semigroup of  $\mathbb{N}_0^r$  such that

$$D(\Gamma) = D(\mathbb{N}_0^r).$$

- The well-order has an extension to an admissible well-order on  $\mathbb{N}_0^r$ .
- Hence  $\rho : R \rightarrow \mathbb{N}_0^r \cup \{-\infty\}$  is a *weight function* of rank  $r$ , i.e.
  - it satisfies the conditions of an order function,
  - and  $\rho(fg) = \rho(f) + \rho(g)$  for all  $f, g \in R$ .

- Let  $R$  and  $S$  be affine  $\mathbb{F}$ -algebras.
- Then  $R = \mathbb{F}[X_1, \dots, X_m]/I$  and  $S = \mathbb{F}[Y_1, \dots, Y_n]/J$  are the coordinate rings of the varieties  $\mathcal{X}$  and  $\mathcal{Y}$ .
- The tensor product  $R \otimes_{\mathbb{F}} S$  is given by
 
$$R \otimes_{\mathbb{F}} S = \mathbb{F}[X_1, \dots, X_m, Y_1, \dots, Y_n]/(I + J).$$
- It is the coordinate ring of  $\mathcal{X} \times \mathcal{Y}$ .
- – Let  $R$  be an order domains with value semigroup  $\Gamma$ .
- Let  $S$  be an order domains with value semigroup  $\Lambda$ .
- Then  $R \otimes_{\mathbb{F}} S$  is an order domain with  $\Gamma \oplus \Lambda$  as value semigroup.

- Let  $(\Gamma, +, 0, <)$  be a well-ordered semigroup.
- – The partial order  $\leq_p$  is defined by
  - $\alpha \leq_p \beta$  if and only if
  - $\beta = \alpha + \gamma$  for some  $\gamma \in \Gamma$ .
- – Let  $\Sigma$  be a subset of  $\Gamma$ .
- Define

$$\min \Sigma =$$

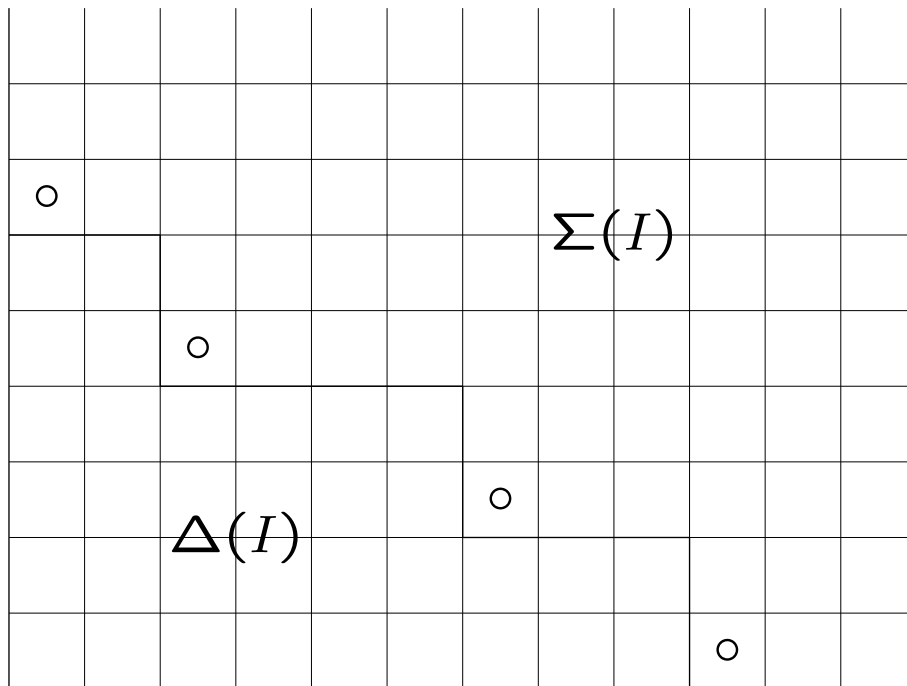
$$\{ \alpha \in \Sigma \mid \beta \in \Sigma, \beta \leq_p \alpha \Rightarrow \beta = \alpha \},$$

the set of *minimal elements* of  $\Sigma$ .

- For every  $\beta \in \Sigma$  there exists an  $\alpha \in \min \Sigma$  such that  $\alpha \leq_p \beta$ .

- Let  $(R, \rho, \Gamma)$  be an order structure.
- Let  $I$  be an ideal in  $R$ .
- – Define  $\Sigma(I) = \{ \rho(f) \mid f \in I, f \neq 0 \}$ .
- – and  $\sigma(I) = \min \Sigma(I)$ .
- – If  $\Gamma$  is finitely generated, then  $\sigma(I)$  is finite.
- The *footprint* or *delta set* of  $I$  is by definition

$$\Delta(I) = \Gamma \setminus \Sigma(I).$$



The circles  $\circ$  denote the positions of the elements of  $\sigma(I)$ .

- Let  $\mathcal{G}$  be a subset of  $I$ .
- –  $\mathcal{G}$  is called a *Gröbner basis* of  $I$ 
  - if  $\sigma(I) \subseteq \{ \rho(g) \mid g \in \mathcal{G} \}$ .
- –  $\mathcal{G}$  is called a *minimal Gröbner basis* of  $I$ 
  - if for every  $\gamma \in \sigma(I)$  there is exactly one  $g \in \mathcal{G}$  such that  $\gamma = \rho(g)$ .

## Proposition:

- Let  $I$  be an ideal in the order domain  $R$ .
- Let  $\mathcal{G}$  be a Gröbner basis of  $I$ .
- Then  $\Sigma(I)$  is an ideal in  $\Gamma$ ,
- Let  $( f_\alpha \mid \alpha \in \Gamma )$  be a well-behaving basis.
- $\mathcal{G}$  generates  $I$  in  $R$ , and
- every  $f \in R$  is equivalent modulo  $I$  to

$$\sum_{\alpha \in \Delta(I)} a_\alpha f_\alpha$$

- this expression is unique.
- $\dim_{\mathbb{F}}(R/I) = \#\Delta(I)$

## Factor ring theorem:

- Let  $w : \Gamma \rightarrow \Lambda$  be a surjective morphism of well-ordered semigroups.
- Let  $(R, \rho, \Gamma)$  be an order structure with  $(f_\alpha \mid \alpha \in \Gamma)$  as well-behaving basis.
- $I$  is an ideal in  $R$  with Gröbner bases  $\mathcal{G}$ .
- Suppose that  $w : \Delta(I) \rightarrow \Lambda$  is injective.
- Suppose that every element  $g$  of  $\mathcal{G}$ :
$$g = af_\alpha + bf_\beta + \sum_{w(\gamma) < \delta} c_\gamma f_\gamma,$$
where  $\alpha \neq \beta$  and  $\delta := w(\alpha) = w(\beta)$ .
- Then  $(R/I, \sigma, \Lambda)$  is an order structure.



- Let  $w : \mathbb{N}_0^m \rightarrow \mathbb{N}_0^r$  be a morphism of semi-groups.
- Let  $<$  be an admissible order on  $\mathbb{N}_0^r$ .
- Let  $\prec$  be an admissible order on  $\mathbb{N}_0^m$ .
- Define
  - $\prec_w$  by  $\alpha \prec_w \beta$  iff
  - $w(\alpha) < w(\beta)$ , or  $w(\alpha) = w(\beta)$  and  $\alpha \prec \beta$ .
- Then
  - $\prec_w$  is an admissible well-order on  $\mathbb{N}_0^m$
  - and  $w$  is a morphism of ordered semi-groups.

- The map  $w$  induces a map on the monomials by  $w(X^\alpha) = w(\alpha)$
- and on the nonzero polynomials, by

$$w\left(\sum a_\alpha X^\alpha\right) = \max\{w(\alpha) \mid a_\alpha \neq 0\},$$

where the maximum is taken with respect to  $<$ .

$$w(X^\alpha Y^\beta) = w(\alpha, \beta) = 4\alpha + 5\beta.$$

⋮	⋮	⋮	⋮	⋮	⋮	⋮
(0, 6)	.	.	.	.	.	⋮
(0, 5)	(1, 5)	.	.	.	.	⋮
(0, 4)	(1, 4)	(2, 4)	.	.	.	⋮
(0, 3)	(1, 3)	(2, 3)	(3, 3)	.	.	⋮
(0, 2)	(1, 2)	(2, 2)	(3, 2)	(4, 2)	(5, 2)	
(0, 1)	(1, 1)	(2, 1)	(3, 1)	(4, 1)	(5, 1)	
(0, 0)	(1, 0)	(2, 0)	(3, 0)	(4, 0)	(5, 0)	

⋮	⋮	⋮	⋮	⋮	⋮	⋮
30	.	.	.	.	.	⋮
25	29	.	.	.	.	⋮
20	24	28	.	.	.	⋮
15	19	23	27	.	.	⋮
10	14	18	22	26	30	
5	9	13	17	21	25	
0	4	8	12	16	20	

$$w(X^5) = w(Y^4).$$

- $R = \mathbb{F}[X, Y]$  and  $\Gamma = \mathbb{N}_0^2$  with  $<_{lex}$ .
- $\Lambda = \mathbb{N}_0\langle 4, 5 \rangle$ .
- –  $w : \mathbb{N}_0^2 \rightarrow \Lambda$  with
  - $w(\alpha, \beta) = 4\alpha + 5\beta$ .
- – Let  $G = X^5 - Y^4 - Y$ ,  $I = (X^5 - Y^4 - Y)$ .
  - Then  $\mathcal{G} = \{G\}$  is a Gröbner basis for  $I$ .
- – Then  $S = \mathbb{F}[X, Y]/(X^5 - Y^4 - Y)$  is an order domain,
  - with  $\Lambda$  as value semigroup,
  - with  $(x^\alpha y^\beta \mid \alpha < 5)$  as well-behaving basis.

- $R = \mathbb{F}[X, Y, Z]$  and  $\Gamma = \mathbb{N}_0^3$  with  $<_{lex}$ .
- $\Lambda = \mathbb{N}_0\langle(4, 0), (5, 0), (1, 1)\rangle$ .
- –  $w : \mathbb{N}_0^3 \rightarrow \Lambda$  with
  - $w(\alpha, \beta, \gamma) = \alpha(4, 0) + \beta(5, 0) + \gamma(1, 1)$ .
- – Let  $G = X^5 - Y^4 - Z$ ,  $I = (X^5 - Y^4 - Z)$ .
  - Then  $\mathcal{G} = \{G\}$  is a Gröbner basis for  $I$ .
- – Then
  - $S = \mathbb{F}[X, Y, Z]/(X^5 - Y^4 - Z) \cong \mathbb{F}[X, Y]$
  - is an order domain,
  - with  $\Lambda$  as value semigroup.

- Let  $R = \mathbb{F}[X_1, X_2, \dots, X_n, \dots]$ , the polynomial ring with infinitely many variables.

- Take the lexicographic order on the monomials with

$$1 < X_1 < X_2 < \dots < X_n < \dots$$

- Let  $\Gamma = \mathbb{N}_0^{(\infty)}$  the set of all sequences of nonnegative integers such that at most finitely many of them are nonzero.
- So  $R = \mathbb{F}[\mathbb{N}_0^{(\infty)}]$ .

- Let  $\lambda_i = \frac{1}{3} (2^i + 2^{-i+1})$  for all  $i \in \mathbb{N}$ .
- Let  $\Lambda = \mathbb{N}_0 \langle \lambda_i \mid i \in \mathbb{N} \rangle$ .
- Then:  $2\lambda_{i+1} = 3\lambda_i + \sum_{j=0}^{i-1} \lambda_j$ .
- Define  $w : \mathbb{N}_0^{(\infty)} \rightarrow \Lambda$  by  $w(\alpha) = \sum_i \alpha_i \lambda_i$ .
- Let  $G_i = X_{i+1}^2 - X_i^3 \prod_{j \leq i-1} X_j + X_{i+2}$ .
- Then

$$w(X_{i+1}^2) = 2\lambda_{i+1} = 3\lambda_i + \sum_{j=0}^{i-1} \lambda_j =$$

$$w \left( X_i^3 \prod_{j \leq i-1} X_j \right) > w(X_{i+2}).$$

- Let the  $G_i = X_{i+1}^2 - X_i^3 \prod_{j \leq i-1} X_j + X_{i+2}$  generate the ideal  $I$ .

- Then  $\mathcal{G} = \{G_i \mid i \in \mathbb{N}\}$  is a Gröbner basis for  $I$ .

- and

$$S = \mathbb{F}[X_1, X_2, \dots, X_n, \dots]/I \cong \mathbb{F}[X_1, X_2]$$

is an order domain of dimension 2,

- with  $\Lambda$  as value semigroup.

- $\Lambda \subset \mathbb{Q}$ , so  $\Lambda$  has rank 1.



- Let  $(R, \rho, \Gamma)$  be a finitely generated order structure.
- May assume that  $\Gamma$  is embedded in  $\mathbb{N}_0^r$ .
- Let  $\mathcal{A} = \{\gamma_1, \dots, \gamma_m\}$  be a set of generators of  $\Gamma$ .
- Choose  $x_1, \dots, x_m \in R$  such that  $\rho(x_i) = \gamma_i$ .
- Then  $R = \mathbb{F}[x_1, \dots, x_m]$ .
- Identify  $R$  with  $\mathbb{F}[X_1, \dots, X_m]/I$ .
- Define the map  $w : \mathbb{N}_0^m \rightarrow \mathbb{N}_0^r$  by  $w(\alpha) = \sum \alpha_i \gamma_i$ .

## The presentation theorem:

- $\Delta(\mathcal{A}) := \{\alpha \in \mathbb{N}_0^m \mid w(\alpha) \leq w(\beta) \Rightarrow \alpha \preceq_w \beta\}$ .
- Then  $\Delta(I) = \Delta(\mathcal{A})$ .
- Let  $\sigma(\mathcal{A}) = \min \mathbb{N}_0^m \setminus \Delta(\mathcal{A})$ .
- For each  $\alpha \in \sigma(\mathcal{A})$  there is a unique  $\alpha' \in \Delta(\mathcal{A})$  such that  $w(\alpha') = w(\alpha)$  and we can write  $x^\alpha$  in a unique way as
$$x^{\alpha'} + \sum_{\gamma \in \Delta(\mathcal{A}), w(\gamma) < w(\alpha)} c_{\alpha\gamma} x^\gamma.$$
- $G_\alpha := X^\alpha - X^{\alpha'} - \sum_{\gamma \in \Delta(\mathcal{A}), w(\gamma) < w(\alpha)} c_{\alpha\gamma} X^\gamma$ .
- Then  $\{G_\alpha \mid \alpha \in \sigma(\mathcal{A})\}$  is a Gröbner basis of  $I$ .

- Let  $R$  be an affine domain over a field  $\mathbb{F}$ .
- Let  $\mathbb{Q}(R)$  be the field of fractions of  $R$ .
- The dimension of  $R$  is the transcendence degree of  $\mathbb{Q}(R)$  over  $\mathbb{F}$ .
- The dimension of an order domain is at least the rank of the value semigroup.
- Not always equal.
- **Theorem:**
  - Let  $(R, \rho, \Gamma)$  be a finitely generated order structure.
  - Then the dimension of  $R$  is equal to the rank of the semigroup.

## Proof:

- Assume for simplicity  $(\Gamma, <) \cong (\mathbb{N}_0, <)$ .
- Let  $r$  be the rank of  $(\Gamma, +)$ .
- Then  $(\Gamma, +)$  is a sub semigroup of  $(\mathbb{N}_0^r, +)$ .
- The well-order  $<$  on  $\Gamma$  is induced by a well-order on  $\mathbb{N}_0^r$ .
- – These are all classified.
  - We can find  $\mathbf{a}_1, \dots, \mathbf{a}_s$  in  $\mathbb{R}_+^r$
  - such that for  $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^r$ :  $\mathbf{a} < \mathbf{b}$  iff
  - there exists a  $t$  such that  $\mathbf{a} \cdot \mathbf{a}_t < \mathbf{b} \cdot \mathbf{a}_t$
  - and  $\mathbf{a} \cdot \mathbf{a}_i = \mathbf{b} \cdot \mathbf{a}_i$  for all  $i < t$ .

- Now the coordinates of  $\mathbf{a}_1$  are all positive, since  $(\Gamma, <) \cong (\mathbb{N}_0, <)$ .

- Define

$$R(n) = \{f \in R \mid \rho(f) \cdot \mathbf{a}_1 \leq n\}.$$

- Then  $R(n)$  is a vector space over  $\mathbb{F}$ .
- Its dimension is at most equal to the number of integral points  $\mathbf{b} \in \mathbb{N}_0^r$  such that  $\mathbf{b} \cdot \mathbf{a}_1 \leq n$ .
- Suppose that  $\dim R = s$ .

- Then there exists a transcendence basis  $x_1, \dots, x_s$  of  $R$ .
- $b := \max\{ \rho(x_i) \cdot a_1 \mid \text{for all } i = 1, \dots, s \}$ .
- Then  $R(b)$  contains  $x_1, \dots, x_s$  and
- $R(bn)$  contains all monomials in  $x_1, \dots, x_s$  of degree at most  $n$ .
- These are independent and the number of these is

$$p(n) := \binom{n+s}{s} = \frac{n^s}{s!} + \text{L.O.T. in } n$$

- This is a polynomial in  $n$  of degree  $s$ .
- $\deg \dim R(bn) \geq \deg p(n) = s$ .

- Let  $c$  be the minimum of all the coordinates of  $\mathbf{a}_1$ .
- Then  $c > 0$ .
- $\{\mathbf{b} \in \mathbb{N}_0^r \mid \mathbf{b} \cdot \mathbf{a}_1 \leq bn\} \subseteq \{\mathbf{b} \in \mathbb{N}_0^r \mid b_i \leq bn/c \text{ for all } i\}$ .
- $\dim_{\mathbb{F}} R(bn) \leq (1 + bn/c)^r$ .
- Therefore  $s \leq r$ .
- Always  $s \geq r$ .