Applied algebraic geometry: algebraic statistics

Jan Draisma, Universität Bern

Monomial orders

A total order on monomials in $K[x_1, \ldots, x_n]$ is called a *monomial order* if it is a well-order and satisfies $x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma}$ (*)

Lemma

A total order on monomials satisfying (*) is a monomial order if and only if $x^\alpha \geq 1$ for all α.

Proof

If it is a monomial order, then $1 > x^\alpha =: m$ would imply $1 > m > m^2 > \cdots$, a contradiction. Conversely, assume that a total order on monomials satisfies $x^\alpha \geq 1$ for all α, and assume that there is an infinite decreasing sequence $x^{\alpha_1} > x^{\alpha_2} > \ldots$. Then by Dickson's lemma $\exists i < j$ with $\alpha_j - \alpha_i =: \beta \in \mathbb{Z}^n_{\geq 0}$. But now $x^\beta \geq 1$ and hence by (*) also $x^{\alpha_j} = x^{\beta+\alpha_i} \geq x^{\alpha_i}$, a contradiction. So $>$ is a well-order satisfying (*) and hence a monomial order. $\square$

Example
$x^\alpha > x^\beta$ if and only if $\alpha \neq \beta$ and the first non-zero entry of $\alpha - \beta$ is positive is a monomial order, called the *lexicographic order*.

There are many other monomial orders. (Uncountably many if the number of variables is > 1.)

Definition
Fix a monomial order. For $f \in K[x_1, \dots, x_n]$ the *leading monomial* $\mathrm{LM}(f)$ is the largest monomial with nonzero coefficient in f.

Definition
Let I be an ideal in $K[x_1, \dots, x_n]$. A subset $G \subseteq I$ is called a *Gröbner basis* relative to the monomial order $>$ if for each $f \in I$ nonzero there is some $g \in G$ with $\mathrm{LM}(g) | \mathrm{LM}(f)$.

Lemma
Any Gröbner basis of I generates I.

Theorem (Hilbert's basis theorem)
Every ideal in $K[x_1, \dots, x_n]$ has a finite Gröbner basis.

Proof: Dickson's lemma implies that $|$ is a wpo. Hence $\mathrm{LM}(I) := \{\mathrm{LM}(f) \mid f \in I\}$ has finitely many $|$-minimal elements $u_1, \dots, u_l$. Then pick $f_i \in I$ with $\mathrm{LM}(f_i) = u_i$; these form a GB. □

For every n set $R_n := K[x_{ij} \mid i = 1, \ldots, k, j = 1, \ldots n]$. For each increasing map $\pi : [m] \to [n]$ we have an algebra homomorphism $\pi : R_m \to R_n$ determined by $\pi x_{ij} = x_{i\pi(j)}$.

Theorem (Aschenbrenner-Hillar, Cohen)
For each n, let $I_n \subseteq R_n$ be an ideal, such that for each increasing map $\pi : [m] \to [n]$ we have $\pi I_m \subseteq I_n$. Then there is a finite sequence $n_1, \ldots, n_p$ such that for each n, I_n is generated by the images of $I_{n_1}, \ldots, I_{n_p}$ in I_n under all increasing maps $[n_i] \to [n]$.

Proof
• In each R_n choose a monomial order such that for all increasing maps $\pi : [m] \to [n]$ we have $x^\alpha > x^\beta$ in R_m implies $\pi x^\alpha > \pi x^\beta$ in R_n.

• Let $u := x^\alpha \in R_m$ and $v := x^\beta \in R_n$ with $n \geq m$. We write $u|v$ if there exists an increasing $\pi : [m] \to [n]$ such that πu divides v.

• In terms of the exponent vectors, think of $\alpha, \beta \in (\mathbb{Z}^k_{\geq 0})^*$. Then this is precisely the partial order in Higman's lemma applied to the componentwise order in $\mathbb{Z}_{\geq 0}$, so in particular a w.p.o.

• The set $U := \{\mathrm{LM}(f) \mid f \in I_n, n \in \mathbb{N}\}$ is upwards closed in the partial order $|$; let M be its $|$-minimal elements. By wpo, it is finite: $M = \{u_1, \ldots, u_l\}$

• For each i let f_i be an element of the corresponding I_{n_i} with $\mathrm{LM}(f) = u$.

• Like in the proof of Hilbert's basis theorem, one finds that for each $n \in \mathbb{N}$, the elements πf_i where $i = 1, \ldots, n$ and $\pi : [n_i] \to [n]$ increasing generate I_n. □

Setting
d random variables taking values in $[r_j]$, $j = 1, \ldots, d$

$\mathcal{F}$ a collection of subsets of $[d]$; for each $A \in \mathcal{F}$ and $\alpha \in \prod_{j \in A}[r_j]$ have a parameter $c_{A,\alpha}$

For $\alpha \in \prod_{j \in [d]}[r_j]$ have $\mathrm{Prob}(\alpha) = \prod_{A \in \mathcal{F}} c_{A,\alpha|_A}$ (forget normalisation).

Thus have monomial map
$\varphi : K[y_\alpha \mid \alpha \in \prod_j [r_j]] \to K[c_{A,\beta} \mid A \in \mathcal{F}, \beta \in \prod_{j \in A}[r_j]]$.

Theorem (Independent set theorem, Hillar-Sullivant)
Fix $\mathcal{F}$ and a subset $T \subseteq [d]$. If $|T \cap A| \leq 1$ for all $A \in \mathcal{F}$, then $\ker \varphi$ is generated in bounded degree if we fix the r_j with $j \in [d] \setminus T$ and we let the r_j with $j \in T$ be arbitrary elements of $\mathbb{Z}_{\geq 0}$.

Proof of independent set theorem

• restrict to the case where all r_j with $j \in T$ are equal to a single number, n, and where all $A \in \mathcal{F}$ contain precisely one element $j_A \in T$.

• Set $S_n := K[y_{\alpha,\gamma} \mid \alpha \in \prod_{j \notin T}[r_j], \gamma \in [n]^T]$ and $Q_n := K[x_{A,\beta,i} \mid A \in \mathcal{F}, \beta \in \prod_{j \in A \setminus T}[r_j], i \in [r_{j_A}]]$, and we study the kernel of the homomorphism $\varphi : S_n \to Q_n, y_{\alpha,\gamma} \mapsto \prod_{A \in \mathcal{F}} x_{A,\alpha|_{A \setminus T},\gamma_{j_A}}$

• Let $R_n := K[z_{\alpha,i} \mid \alpha \in \prod_{j \notin T}[r_j], i \in [n]]$, and note that φ decomposes as $\varphi_2 \circ \varphi_1$ where $\varphi_1 : S_n \to R_n, y_{\alpha,\gamma} \mapsto \prod_{j \in T} z_{\alpha,\gamma_j}$ and $\varphi_2 : R_n \to Q_n, z_{\alpha,i} \mapsto \prod_{A \in \mathcal{F}, i \in A} x_{A,\alpha|_{A \setminus T},i}$

• φ_1 is the parameterisation of $k := \prod_{j \notin T} r_j$-tuples of rank-one tensors, hence $\ker \varphi_1$ generated by 2×2-minors of flattenings. Its image is a subring of R_n, for which we have a Noetherianity result. This Noetherianity turns out to carry over to the image. $\square$