Randbasen: wieso und wozu?

Martin Kreuzer

Fakultät für Informatik und Mathematik

Universität Passau

martin.kreuzer@uni-passau.de

Niederbayrisch-Oberösterreichisches Computeralgebraseminar

Universität Passau

3.12.2007

Inhaltsübersicht

1 – Definitionen

Will Rogers: Jeder ist ein Ignorant.
Aber auf verschiedenen Gebieten.

K Körper

$P = K[x_1, \ldots, x_n]$ Polynomring über K

$I \subseteq P$ Polynomideal

$\mathbb{T}^n = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid \alpha_i \geq 0\}$ Monoid der Terme

σ Termordnung of $\mathbb{T}^n$ (d.h. Wohlordnung und mit Multiplikation verträglich)

Ordnungsideale

Definition 1.1 **(a)** Eine Teilmenge $\mathcal{O} \subset \mathbb{T}^n$ heißt ein **Ordnungsideal**, wenn für jeden Term in $\mathcal{O}$ auch alle seine Teiler in $\mathcal{O}$ liegen.

(b) Der **Rand** eines Ordnungsideals $\mathcal{O}$ ist die Menge

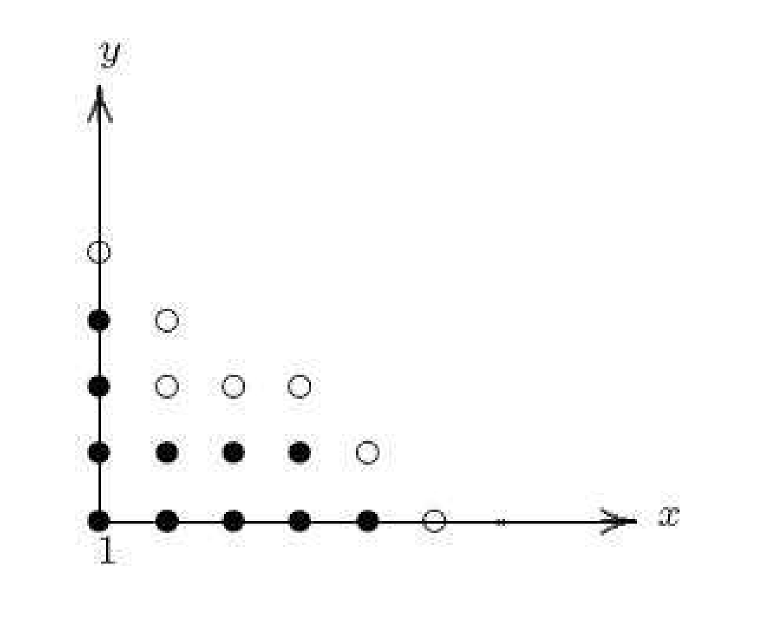
$$\partial\mathcal{O} = (x_1\,\mathcal{O} \cup \cdots \cup x_n\,\mathcal{O}) \setminus \mathcal{O}.$$

Beispiel 1.2 In $\mathbb{T}^2$ bildet die folgende Termmenge ein Ordnungsideal:

$$\mathcal{O} = \{1,\, x,\, y,\, x^2,\, xy,\, y^2,\, x^3,\, x^2y,\, y^3,\, x^4\}$$

Ihr Rand ist $\partial\mathcal{O} = \{x^5,\, x^4y,\, x^3y^2,\, x^2y^2,\, xy^2,\, xy^3,\, y^4\}$:

Bild dieses Ordnungsideals und seines Rands



• Term im Ordnungsideal ◦ Term im Rand

Sei $\mathcal{O} = \{t_1, \ldots, t_\mu\} \subseteq \mathbb{T}^n$ ein Ordnungsideal mit Rand $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$.

Definition 1.3 **(a)** Eine Menge von Polynomen $G = \{g_1, \ldots, g_\nu\}$ heißt eine **$\mathcal{O}$-Randpräbasis**, wenn gilt:

$$g_j = b_j - \sum_{i=1}^{\mu} c_{ij} t_i \qquad \text{mit } c_{ij} \in K$$

(b) Eine $\mathcal{O}$-Randpräbasis G heißt **$\mathcal{O}$-Randbasis**, wenn die Restklassen der Elemente von $\mathcal{O}$ eine Vektorraumbasis von $P/\langle G \rangle$ darstellen.

Genau dann ist G eine $\mathcal{O}$-Randbasis, wenn das Ideal $I = \langle G \rangle$ die Bedingung $I \oplus \langle \mathcal{O} \rangle_K = P$ erfüllt.

Beispiel für eine Randbasis

Beispiel 1.4 Sei $P = \mathbb{Q}[x, y]$ und sei $I \subseteq P$ das Verschwindungsideal der fünf Punkte $X = \{(0,0), (0,-1), (1,0), (1,1), (-1,1)\}$ im affinen Raum $\mathbb{A}^2(\mathbb{Q})$, d.h. es sei $I = \{f \in P \mid f(p) = 0 \text{ für alle } p \in X\}$. Es ist bekannt, dass $\dim_K(P/I) = 5$ gilt. In $\mathbb{T}^2$ enthalten die folgenden Ordnungsideale genau fünf Elemente:

$$\mathcal{O}_1 = \{1,\ x,\ x^2,\ x^3,\ x^4\},\ \mathcal{O}_2 = \{1,\ x,\ x^2,\ x^3,\ y\},\ \mathcal{O}_3 = \{1,\ x,\ x^2,\ y,\ y^2\}$$
$$\mathcal{O}_4 = \{1,\ x,\ x^2,\ y,\ xy\},\ \mathcal{O}_5 = \{1,\ x,\ y,\ y^2,\ y^3\},\ \mathcal{O}_6 = \{1,\ y,\ y^2,\ y^3,\ y^4\}$$

Nicht alle davon sind geeignet für Randbasen von I. Z.B. können die Restklassen von $\mathcal{O}_1$ keine Vektorraumbasis von P/I bilden, denn es gilt $x^3 - x \in I$. Ebenso kann I keine $\mathcal{O}_6$-Randbasis besitzen, denn $y^3 - y \in I$.

Jedoch besitzt X eine Randbasis bzgl. $\mathcal{O}_3 = \{1,\, x,\, x^2,\, y,\, y^2\}$. Der Rand von $\mathcal{O}$ ist $\partial\mathcal{O} = \{xy, x^3, y^3, xy^2, x^2y\}$. Die $\mathcal{O}$-Randbasis von I ist $G = \{g_1, \ldots, g_5\}$ mit

$$\begin{aligned} g_1 &= x^3 - x \\ g_2 &= x^2y - 0.5\,y - 0.5\,y^2 \\ g_3 &= xy - x - 0.5\,y + x^2 - 0.5\,y^2 \\ g_4 &= xy^2 - x - 0.5\,y + x^2 - 0.5\,y^2 \\ g_5 &= y^3 - y \end{aligned}$$

Die Menge $\mathcal{O}_3$ kommt nicht von einer Gröbner-Basis von I. Um dies zu sehen, betrachten wir g_3 genauer. Für jede Termordnung σ gilt $x^2 >_\sigma xy >_\sigma y^2$ oder $y^2 >_\sigma xy >_\sigma x^2$. Also ist x^2 oder y^2 der Leitterm von g_3. Da diese Terme in $\mathcal{O}_3$ liegen, kann $\mathcal{O}_3$ nicht das Komplement eines Leittermideal von I sein.

2 – Randbasen und Gröbner-Basen

Definition 2.1 **(a)** Für ein Polynom $f \in P \setminus \{0\}$ heißt der bzgl. σ größte Term in seinem Träger der **Leitterm** von f. Er wird mit $\mathrm{LT}_\sigma(f)$ bezeichnet.

(b) Das Polynomideal $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\} \rangle$ heißt das **Leittermideal** von I bzgl. σ.

(c) Eine Menge $G = \{g_1, \ldots, g_s\}$ von Polynomen aus I heißt eine **σ-Gröbner-Basis** von I wenn gilt:

$$\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_s) \rangle$$

Randbasen verallgemeinern Gröbner-Basen

1. Ist σ eine Termordnung und G die reduzierte σ-Gröbner-Basis eines 0-dimensionalen Polynomideals I, so kann man G zu einer Randbasis von I bzgl. $\mathcal{O}_\sigma(I) = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ ergänzen.

2. Ist das Ordnungideal von der Form $\mathcal{O}_\sigma(I) = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$, so besitzt I eine $\mathcal{O}_\sigma(I)$-Randbasis. Diese enthält die reduzierte σ-Gröbner-Basis als die Randbasispolynome, die zu den Ecken des Rands von $\mathcal{O}_\sigma(I)$ gehören.

3. Ein 0-dimensionales Polynomideal muss bzgl eines gegebenen Ordnungsideals $\mathcal{O}$ keine Randbasis besitzen. Falls es aber eine hat, so ist diese **eindeutig** bestimmt.

4. Das Ideal I besitzt im Allgemeinen **viel mehr** Randbasen als reduzierte Gröbner-Basen.

Multiplikationsmatrizen

Sei $G = \{g_1, \ldots, g_\nu\}$ eine $\mathcal{O}$-Randpräbasis. Für $r \in \{1, \ldots, n\}$ definiere die r-te **formale Multiplikationsmatrix** $\mathcal{M}_r$ wie folgt:

Multipliziere $t_i \in \mathcal{O}$ mit x_r. Ist $x_r t_i = b_j$ im Rand von $\mathcal{O}$, so reduziere mit dem Randpräbasispolynom $g_j = b_j - \sum_{k=1}^{\mu} c_{kj} t_k$ und setze $(c_1, \ldots, c_\mu)$ in die i-te Spalte von $\mathcal{M}_r$. Ist aber $x_r t_i = t_j$ so setze den j-ten Einheitsvektor in die i-te Spalte von $\mathcal{M}_r$.

Theorem 2.2 *Genau dann ist G eine $\mathcal{O}$-Randbasis von $I = \langle G \rangle$, wenn die formalen Multiplikationsmatrizen paarweise kommutieren, d.h. wenn $\mathcal{M}_i \, \mathcal{M}_j = \mathcal{M}_j \, \mathcal{M}_i$ gilt für $1 \leq i < j \leq n$.*

3 – Lösung algebraischer Gleichungssysteme

Theorem 3.1 **(Das Verfahren von Auzinger-Stetter)**
Sei $\mathcal{O}$ ein Ordnungsideal bzgl. dem das Ideal $I = \langle f_1, \ldots, f_s \rangle$ eine Randbasis $G = \{g_1, \ldots, g_\nu\}$ besitzt. O.E. sei $t_1 = 1$, $t_2 = x_1, \ldots,$ $t_{n+1} = x_n$.

(1) *Bestimme die formalen Multiplikationsmatrizen $\mathcal{M}_1, \ldots, \mathcal{M}_n$ mit Hilfe von G.*

(2) *Bestimme die gemeinsamen Eigenvektoren $v_1, \ldots, v_n$ dieser Multiplikationsmatrizen.*

(3) *Schreibe $v_i = (a_{i1}, a_{i2}, \ldots, a_{i\mu})$ mit $a_{ij} \in K$. Dann sind die Punkte $(a_{i2}, \ldots, a_{i\,n+1})$ die Lösungen von $(*)$.*

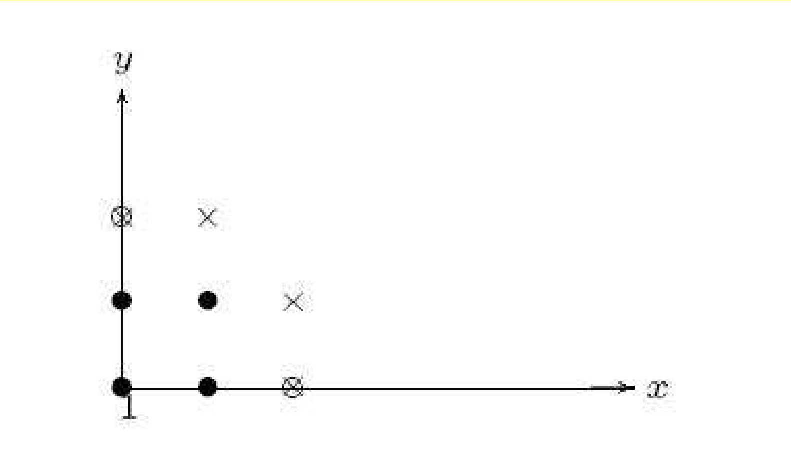
Beispiel 3.2 Sei $P = \mathbb{R}[x, y]$ und sei I das Ideal

$$I = \langle 0.25\, x^2 + y^2 - 1,\ x^2 + 0.25\, y^2 - 1 \rangle$$

von P. Dann besitzt I eine Randbasis bzgl. dem Ordnungsideal $\mathcal{O} = \{1,\, x,\, y,\, xy\}$. Es gilt nämlich $\partial\mathcal{O} = \{x^2, x^2y, xy^2, y^2\}$ und die $\mathcal{O}$-Randbasis von I ist $G = \{g_1, g_2, g_3, g_4\}$ mit

$$\begin{aligned} g_1 &= x^2 - \tfrac{4}{5} \\ g_2 &= x^2y - \tfrac{4}{5}y \\ g_3 &= xy^2 - \tfrac{4}{5}x \\ g_4 &= y^2 - \tfrac{4}{5} \end{aligned}$$

Bild dieses Ordnungsideals und seines Rands



Die Berechnung der Multiplikationsmatrizen ergibt

$$\mathcal{M}_x = \begin{pmatrix} 0 & 0.8 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.8 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{und} \quad \mathcal{M}_y = \begin{pmatrix} 0 & 0 & 0.8 & 0 \\ 0 & 0 & 0 & 0.8 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Die gemeinsamen Eigenvektoren dieser beiden Matrizen sind

$$v_1 = (1,\ \sqrt{0.8},\ \sqrt{0.8},\ 0.8) \quad v_2 = (1,\ -\sqrt{0.8},\ \sqrt{0.8},\ -0.8)$$

$$v_3 = (1,\ \sqrt{0.8},\ -\sqrt{0.8},\ -0.8) \quad v_4 = (1,\ -\sqrt{0.8},\ -\sqrt{0.8},\ 0.8)$$

Hieraus können wir die Lösungen $\{(\pm\sqrt{0.8}, \pm\sqrt{0.8})\}$ des Gleichungssystems an den zweiten und dritten Koordinaten ablesen.

4 – Symmetrieerhaltung

Beispiel 4.1 Sei $P = \mathbb{Q}[x, y]$ und
$I = \langle x^2 + xy + y^2,\ x^3,\ x^2y,\ xy^2,\ y^3\rangle$. Betrachte das Ordnungsideal

$$\mathcal{O} = \{1,\ x,\ y,\ x^2,\ y^2\}$$

Es gilt $\partial\mathcal{O} = \{x^3,\ x^2y,\ xy,\ xy^2,\ y^3\}$. Das Ideal I hat die $\mathcal{O}$-Randbasis

$$G = \{x^3,\ x^2y,\ xy + x^2 + y^2,\ xy^2,\ y^3\}$$

Sowohl $\mathcal{O}$ als auch G sind symmetrisch!

Jedoch besitzt das Ideal I keine symmetrische Basis $\mathcal{O}_\sigma(I)$, denn für das Polynom $f = x^2 + xy + y^2$ gilt $\mathrm{LT}_\sigma(f) = x^2$ oder $\mathrm{LT}_\sigma(f) = y^2$.

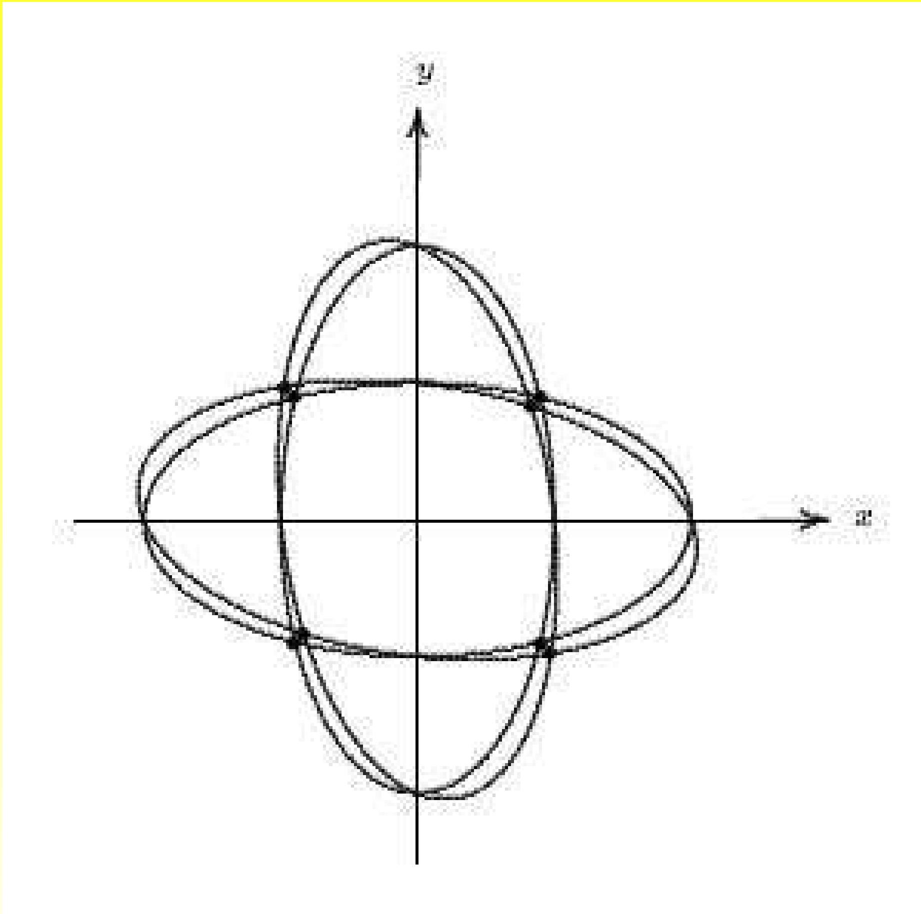
5 – Numerische Stabilität

Beispiel 5.1 Wir betrachten noch einmal das Beispiel 3.2, führen jedoch eine kleine numerische Störung ein. Sei also $P = \mathbb{R}[x,y]$, sei $I = \langle 0.25\,x^2 + y^2 - 1,\, x^2 + 0.25\,y^2 - 1\rangle$ und

$$\widetilde{I} = \langle 0.25\,x^2 + y^2 + \varepsilon xy - 1,\; x^2 + 0.25\,y^2 + \varepsilon xy - 1\rangle$$

mit einer "kleinen" Zahl $\varepsilon > 0$.

Skizze der alten und neuen Lösungsmenge



1. Die Berechnung der reduzierten `DegLex`-Gröbner-Basis von $\tilde{I}$ liefert:

$$\tilde{g}_1 = x^2 - y^2$$
$$\tilde{g}_2 = xy - \frac{5}{4\varepsilon}\, y^2 - \frac{1}{\varepsilon}$$
$$\tilde{g}_3 = y^3 - \frac{16\varepsilon}{16\varepsilon^2 - 25}\, x + \frac{20}{16\varepsilon^2 - 25}\, y$$

Für $\varepsilon \longrightarrow 0$ strebt diese **nicht** gegen die reduzierte `DegLex`-Gröbner-Basis von I. Es handelt sich um eine

Repräsentations-Singularität.

2. Die Berechnung der Randbasis von $\tilde{I}$ bzgl. $\mathcal{O} = \{1, x, y, xy\}$ liefert:

$$\tilde{h}_1 = x^2 + \tfrac{4\varepsilon}{5}\, xy - \tfrac{4}{5}$$
$$\tilde{h}_2 = x^2 y - \tfrac{16\varepsilon}{16\varepsilon^2 - 25}\, x + \tfrac{20}{16\varepsilon^2 - 25}\, y$$
$$\tilde{h}_3 = xy^2 + \tfrac{20}{16\varepsilon^2 - 25}\, x - \tfrac{16\varepsilon}{16\varepsilon^2 - 25}\, y$$
$$\tilde{h}_4 = y^2 + \tfrac{4\varepsilon}{5}\, xy - \tfrac{4}{5}$$

Für $\varepsilon \longrightarrow 0$ strebt diese gegen die Randbasis von I. Randbasen sind **numerisch stabil**.

6 – Deformation von Randbasen

Sei $\mathcal{O} = \{t_1, \ldots, t_\mu\} \subseteq \mathbb{T}^n$ ein Ordnungsideal mit Rand $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ und $G = \{g_1, \ldots, g_\nu\}$ eine **$\mathcal{O}$-Randpräbasis**.

Ziel: Zeige, dass man jede Randbasis mit Hilfe einer flachen Familie in ihr **Randtermideal** $\langle b_1, \ldots, b_\nu \rangle$ deformieren kann.

Definition 6.1 Ein Gewichtsvektor $W = (w_1, \ldots, w_n) \in \mathbb{N}^n_+$ definiert eine Graduierung auf P durch $\deg_W(x_i) = w_i$. Das **Gradformenideal** von I ist

$$\mathrm{DF}_W(I) = \langle \mathrm{DF}_W(f) \mid f \in I \setminus \{0\} \rangle.$$

Dabei ist die **Gradform** $\mathrm{DF}_W(f)$ die homogene Komponente höchsten Grades von f bzgl. der durch W gegebenen Graduierung.

Satz 6.2 (Deformation auf das Gradformenideal)

(a) *Besitzt* $\mathrm{DF}_W(I)$ *eine* $\mathcal{O}$*-Randbasis, so besitzt auch* I *eine* $\mathcal{O}$*-Randbasis und es gibt eine flache Familie* $K[x_0] \longrightarrow \overline{P}/I^{\mathrm{hom}}$ *mit* **allgemeiner Faser** P/I *und* **spezieller Faser** $P/\,\mathrm{DF}_W(I)$*. Hierbei sei* $\overline{P} = K[x_0, \ldots, x_n]$ *und* I^{hom} *die* **Homogenisierung** *von* I*.*

(b) *Besitzt* $\mathcal{O}$ *einen* maxdeg_W*-Rand, d.h. gilt* $\deg_W(b_j) \geq \deg_W(t_i)$ *für alle* i, j*, und besitzt* I *eine* $\mathcal{O}$*-Randbasis* $G = \{g_1, \ldots, g_\nu\}$*, so hat* $\mathrm{DF}_W(I)$ *die* $\mathcal{O}$*-Randbasis* $\mathrm{DF}_W(G)$ *und es gibt eine flache Familie* $K[x_0] \longrightarrow \overline{P}/I^{\mathrm{hom}}$ *wie in* **(a)***.*

Dabei gilt im Allgemeinen **nicht**, dass sich jede $\mathcal{O}$-Randbasis von I zu einer $\mathcal{O}$-Randbasis von $\mathrm{DF}_W(I)$ deformiert.

7 – Das Randbasisschema

Sei $\mathcal{O} = \{t_1, \ldots, t_\mu\} \subseteq \mathbb{T}^n$ ein Ordnungsideal mit Rand $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ und $G = \{g_1, \ldots, g_\nu\}$ eine $\mathcal{O}$-Randpräbasis. Wir betrachten die Koeffizienten c_{ij} in der Darstellung $g_j = b_j - \sum_{i=1}^{\mu} c_{ij} t_i$ als Unbestimmte und nennen G die **generische $\mathcal{O}$-Randpräbasis**.

Definition 7.1 Die Bedingungen $\mathcal{M}_i \, \mathcal{M}_j = \mathcal{M}_j \, \mathcal{M}_i$, also dass die formalen Multiplikationsmatrizen kommutieren, definieren ein Ideal $J \subset K[c_{ij} \mid 1 \le i \le \mu,\ 1 \le j \le \nu]$. Die Nullstellenmenge dieses Ideals heißt das **$\mathcal{O}$-Randbasisschema** $\mathbb{B}$. Sein Koordinatenring ist $B = K[c_{ij}]/J$.

Die flache universelle Familie

Satz 7.2 *Der kanonische Ringhomomorphismus* $B \longrightarrow B[x_1, \ldots, x_n]/\langle g_1, \ldots, g_\nu \rangle$ *ist flach. Genauer ist* $\mathcal{O}$ *eine* B*-Basis der rechten Seite.*

Die Faser dieser Familie über einem Punkt $(a_{11}, \ldots, a_{\mu\nu})$ *ist dabei die* $\mathcal{O}$*-Randbasis, die entsteht, indem man in der generischen* $\mathcal{O}$*-Randbasis* $c_{ij} \mapsto a_{ij}$ *substituiert.*

Das Randbasisschema parametrisiert also alle 0-dimensionalen Polynomideale, die eine $\mathcal{O}$-Randbasis besitzen.

Die universelle Familie enthält zu jedem Punkt des Randbasisschemas das zugehörige Ideal.

Der Punkt $(0,\ldots,0)$ auf dem Randbasisschema entspricht gerade dem Randtermideal $\langle b_1,\ldots,b_\nu\rangle$. Daher können wir die gesucht flache Deformation auf das Randtermideal wie folgt erhalten:

Korollar 7.3 *Gibt es eine* **rationale Kurve** $B \longrightarrow K[x_0]$ *auf* $\mathbb{B}$*, die den vorgegebenen Punkt mit* $(0,\ldots,0)$ *verbindet, so existiert eine flache Familie* $K[x_0] \longrightarrow B[x_1,\ldots,x_n]/\langle g_1,\ldots,g_\nu\rangle \otimes K[x_0]$ *mit* **allgemeiner Faser** P/I *und* **spezieller Faser** $P/\langle b_1,\ldots,b_\nu\rangle$*.*

Frage: Ist das Randbasisschema zusammenhängend?

Es ist bekannt, dass es eine offene Teilmenge des zusammenhängenden Hilbert-Schemas darstellt.

Weitere Forschungen

• Man kann analog ein **homogenes Randbasisschema** definieren, das die homogenen Ideale parametrisiert, die eine Randbasis haben.

• Besitzt $\mathcal{O}$ einen maxdeg_W-Rand, so ist das homogene Randbasisschema ein affiner Raum.

• Man kann die Gleichungen für das Randbasisschema auch auf andere Weise konstruieren: Eine Randpräbasis ist genau dann eine Randbasis, wenn die **Nachbarsyzygien** liften.

• Es gilt das **Analogon des Satzes von Schreyer:** Ist G eine Randbasis, so erzeugen die Liftungen der Nachbarsyzygien den Syzygienmodul $\mathrm{Syz}(G)$ der Randbasispolynome.

Literaturhinweise

1. (mit A. Kehrein und L. Robbiano) *An algebraist's view on border bases*, in: Solving polynomial equations, Springer 2005, 169 – 202
2. (mit A. Kehrein) *Characterizations of border bases*, J. Pure Appl. Alg. **196** (2005), 251 – 270
3. (mit A. Kehrein) *Computing border bases*, J. Pure Appl. Alg. **205** (2006), 279 – 295
4. (mit L. Robbiano) *Deformations of border bases*, Preprint 2007, siehe `www.arxiv.org`

Vielen Dank für Ihre Aufmerksamkeit!