

Discrete Wiskunde
2WC15, Lente 2010

Jan Draisma

HOOFDSTUK 4

Eliminatie

1. Projecteren en elimineren

Eliminatie gaat, meetkundig gezien, over het *projecteren* van variëteiten.

PROPOSITIE 1.1. *Laat $x = (x_1, \dots, x_n)$ en $y = (y_1, \dots, y_m)$ variabelen zijn. Zij $V \subseteq K^{n+m}$ een variëteit en zij $\mathcal{I}(V) \subseteq K[x, y]$ het ideaal van alle polynomen die op V verdwijnen. Definieer*

$$W := \{q \in K^m \mid \exists p \in K^n : (p, q) \in V\}$$

Dan is $\mathcal{I}(W) \subseteq K[y]$ gelijk aan $\mathcal{I}(V) \cap K[y]$.

Merk op dat W in het algemeen geen variëteit is. Zo is de projectie van de variëteit in K^{1+1} gegeven door $x_1 y_1 = 1$ op de tweede coördinaat gelijk aan K^* . In dit geval is $\mathcal{I}(W)$ dus gelijk aan $\{0\}$.

BEWIJS. Als $f \in \mathcal{I}(W)$ en $(p, q) \in V$, dan geldt $q \in W$ en dus $f(q) = 0$, dus $f \in \mathcal{I}(V) \cap K[y]$. Omgekeerd, als $f \in \mathcal{I}(V) \cap K[y]$ en $q \in W$, dan is er een $p \in K^n$ met $(p, q) \in V$ en dus $f(p, q) = f(q) = 0$, dus $f \in \mathcal{I}(W)$. $\square$

GEVOLG 1.2. *Laat $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, en neem aan dat K oneindig is. Zij $I \subseteq K[x, y]$ het ideaal voortgebracht door $y_j - f_j$ voor $j = 1, \dots, m$. Dan is $I \cap K[y]$ het ideaal van alle polynomen die overal op het beeld van de afbeelding $K^n \rightarrow K^m$, $x \mapsto (f_1(x), \dots, f_m(x))$ verdwijnen.*

BEWIJS. Dit volgt direct uit de propositie met $V = \{(x, f(x)) \mid x \in K^n\}$, als we tenminste kunnen inzien dat I gelijk is aan $\mathcal{I}(V)$. Alleen de inclusie $I \supseteq \mathcal{I}(V)$ is niet meteen duidelijk. Maar als $h \in \mathcal{I}(V)$, dan geldt $h = h'(y_i - f_i) + h''$ voor zekere $h'' \in \mathcal{I}(V)$ waar y_i niet meer in voorkomt. Doe dit met alle y_i en je vindt dat $h = r + s$ met $r \in I$ en $s \in \mathcal{I} \cap K[x]$. Maar dan verdwijnt s op alle punten in K^n en is dus het nulpolynoom omdat K oneindig is. $\square$

OPMERKING 1.3. Merk op dat in de situatie in het voorgaande bewijs het ideaal $K[y] \cap I$ gelijk is aan de *kern* van het unieke K -algebrahomomorfisme $K[y] \rightarrow K[x]$ dat elke y_i naar $f_i(x)$ stuurt.

DEFINITION 1.4. Laat x en y als boven zijn en zij I een ideaal in $K[x, y]$. Dan heet $I \cap K[y]$ het *eliminatie-ideaal* van I met betrekking tot de variabelen in x .

De volgende stelling laat zien dat je eliminatie-idealén ook echt kunt uitrekenen.

STELLING 1.1. *Zij I een ideaal in $K[x, y]$ en zij $\leq$ een monomiale ordening op de monomen in $M(x, y)$ met de eigenschap dat elk monoom uit $M(x, y) \setminus M(y)$ groter is dan elk monoom in $M(y)$. Zij B een Gröbnerbasis van I met betrekking tot $\leq$. Dan is $B \cap K[y]$ een Gröbnerbasis van $I \cap K[y]$ met betrekking tot de beperking van $\leq$ tot $M(x)$.*

In het bijzonder betekent dit, dat $B \cap K[y]$ het ideaal $I \cap K[y]$ voortbrengt.

OPGAVE 1.5. Bereken met Singular voortbrengers voor het ideaal van het beeld van de afbeelding $\mathbb{Q}^2 \rightarrow \mathbb{Q}^3$, $(m, n) \mapsto (m^2 - n^2, 2mn, m^2 + n^2)$.

OPGAVE 1.6. De *paraplu van Whitney* is het oppervlak in $\mathbb{C}^3$ gegeven door $x = uv, y = v, z = u^2$. Teken een plaatje in $\mathbb{R}^3$ van de door *reële* u, v geparametriseerde punten van die paraplu. Vind het ideaal $I \subseteq \mathbb{C}[x, y, z]$ van de paraplu en laat zien dat elk punt in $V(I) \subseteq \mathbb{C}^3$ ook door geschikte $(u, v) \in \mathbb{C}^2$ geparametriseerd wordt. Geldt dit ook voor $\mathbb{C}$ vervangen door $\mathbb{R}$?

2. Markovbases

Een concept dat op het eerste gezicht niets met Gröbnerbases te maken heeft is het volgende.

DEFINITIE 2.1. Zij A een $n \times m$ -matrix met entrees uit $\mathbb{N} = \{0, 1, 2, \dots\}$. In wat volgt schrijven we $\ker A$ voor de verzameling van alle *kolomvectoren* $u \in \mathbb{Z}^m$ zo dat $Au = 0$. Een *Markov basis* voor A is deelverzameling $M \subseteq \ker A$ met de eigenschap dat er voor elk paar $u, v \in \mathbb{N}^m$ dat voldoet aan $Au = Av$ een rij $u_0 := u, u_1, u_2, \dots, u_k := v$ van vectoren in $\mathbb{N}^m$ bestaat met de eigenschap dat $u_{i+1} - u_i \in \pm M$ voor alle i .

VOORBEELD 2.2. Neem

$$A = \begin{bmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{bmatrix}.$$

De vectoren $m_1 = (-1, 2, -1, 0)^T$ en $m_2 = (0, -1, 2, -1)^T$ spannen $\ker A$ op, maar vormen geen Markovbasis—immers, er geldt

$$A(1, 0, 0, 1)^T = A(0, 1, 1, 0)^T,$$

maar er is geen pad van $(1, 0, 0, 1)^T$ naar $(0, 1, 1, 0)^T$ met stappen uit $\pm\{m_1, m_2\}$ dat geheel binnen $\mathbb{N}^4$ blijft. De verzameling $M = \{m_1, m_2, m_3 := (-1, 1, 1, -1)^T\}$ daarentegen is *wel* een Markovbasis. Zij namelijk $u \in \mathbb{N}^4$. Dan kun je u met stappen uit $\pm M$ verbinden met een u' die hooguit twee positieve entrees heeft, die dan bovendien nog opeenvolgend moeten zijn. Zij nu $v \in \mathbb{N}^4$ met $Au = Av$, en verbind v met stappen uit $\pm M$ met een v' met dezelfde eigenschappen. Uit $Au' = Av'$ en het feit dat $u', v' \in \mathbb{N}^4$ allebei hooguit twee positieve entrees hebben die dan bovendien naast elkaar moeten zitten volgt eenvoudig dat $u' = v'$.

OPGAVE 2.3. Veralgemeen dit voorbeeld naar het geval waar

$$A = \begin{bmatrix} n & n-1 & \dots & 0 \\ 0 & 1 & \dots & n \end{bmatrix}.$$

De link met Gröbnerbases en affiene variëteiten komt als volgt tot stand. De matrix A definieert een *monomiale afbeelding* $\mathbb{C}^n \rightarrow \mathbb{C}^m$ gedefinieerd door

$$x = (x_1, \dots, x_n) \mapsto (y_1, \dots, y_m)$$

met

$$y_j = \prod_{i=1}^n x_i^{a_{ij}}.$$

Het ideaal van het beeld wordt vanwege Gevolg 1.2 gegeven door de doorsnede met $\mathbb{C}[y]$ van het ideaal I in $\mathbb{C}[x, y]$ voortgebracht door de polynomen

$$y_j - \prod_{i=1}^n x_i^{a_{ij}}, \quad j = 1, \dots, m.$$

Met de verkorte notatie x^b voor $\prod_{i=1}^n x_i^{b_i}$ voor kolomvectoren $b = (b_1, \dots, b_n)^T \in \mathbb{N}^n$, kunnen we bovenstaand polynoom ook schrijven als $y_j - x^{a_j}$, waar a_j de j -de kolom van A is. Voor $u \in \mathbb{N}^m$ geldt nu

$$y^u = \prod_j y_j^{u_j} = \prod_j (x^{a_j})^{u_j} = x^{Au} \pmod{I},$$

zodat als $u, v \in \mathbb{N}^m$ voldoen aan $Au = Av$, dan $y^u - y^v \in I$. Dit gaan we als volgt gebruiken. Als $w \in \ker A$, dan kunnen we w schrijven als $w_+ - w_-$ met $w_+, w_- \in \mathbb{N}^m$ gedefinieerd door $(w_+)_i = \max\{w_i, 0\}$ en $(w_-)_i = -\min\{w_i, 0\}$. Nu geldt $Aw_+ = Aw_-$ en dus is het polynoom $p_w := y^{w_+} - y^{w_-} \in K[y]$ een element van I .

LEMMA 2.4. *Het ideaal $I \cap \mathbb{C}[y]$ wordt voortgebracht (zelfs opgespannen over $\mathbb{C}$) door binomen van de vorm $y^u - y^v$ met $u, v \in \mathbb{N}^m$ zo dat $Au = Av$.*

BEWIJS. Stel $f = \sum_u c_u y^u \in I$. Dit betekent dat het polynoom 0 wordt als je elke y_j vervangt door het monoom x^{a_j} . In dat proces kunnen alleen termen $c_u y^u, c_v y^v$ tegen elkaar wegvallen die hetzelfde monoom in x geven, dus waarvoor geldt $Au = Av$. Van alle termen $c_u y^u$ met Au gelijk aan een vaste vector w moeten de coëfficiënten dus tot nul optellen. Maar dat betekent dat de som van die termen een lineaire combinatie is van binomen $y^u - y^v$ met $Au = Av = w$. Omdat dit voor alle w geldt, is f ook zo'n lineaire combinatie. $\square$

THEOREM 2.5 (Diaconis-Sturmfels). *Zij $M \subseteq \ker A$ een deelverzameling. Dan is M een Markovbasis voor A als en alleen als de polynomen $p_w := y^{w_+} - y^{w_-}$, $w \in M$ het ideaal $I \cap K[y]$ voortbrengen.*

Een belangrijk gevolg van deze stelling is dat elke matrix A met natuurlijke getallen als entrees een *eindige* Markovbasis heeft. Bovendien kun je dankzij Stelling 1.1 met het Buchbergeralgoritme (ten opzichte van een geschikte monomiale ordening) een eindige Markovbasis van A uitrekenen.

BEWIJS. Van beide uitspraken verandert de waarheid niet als we M door $M \cup -M$ vervangen. Dus we mogen wel aannemen dat $M = -M$.

Neem eerst aan dat M een Markovbasis is. Om te bewijzen dat de p_w het ideaal $I \cap K[y]$ voortbrengen is het op grond van voorgaand lemma voldoende te bewijzen dat als $u, v \in \mathbb{N}^m$ met $Au = Av$, dan $y^u - y^v \in J := \langle \{p_w \mid w \in M\} \rangle$. Omdat M een Markov basis is, bestaan er $u_0 := u, u_1, \dots, u_k := v$, alle in $\mathbb{N}^m$, zo dat $u_i - u_{i+1} \in \pm M$. We laten zien dat dit betekent dat y^{u_i} modulo J gelijk is aan $y^{u_{i+1}}$. Immers, schrijf $u_i - u_{i+1} = w = w_+ - w_- \in M$. Dan volgt

$$y^{u_i} - y^{u_{i+1}} = y^{u_{i+1} + w_+ - w_-} - y^{u_{i+1}} = y^{u_{i+1} - w_-} (y^{w_+} - y^{w_-}) \in J.$$

Hier hebben we gebruikt dat $u_{i+1} - w_-$ enkel niet-negatieve componenten heeft. Omgekeerd, neem aan dat de p_w , $w \in M$ het ideaal $I \cap K[y]$ voortbrengen. Voor een paar $u, v \in \mathbb{N}^m$ met $Au = Av$ geldt

$$y^u - y^v = \sum_{i=1}^k y^{m_i} (y^{w_{i+}} - y^{w_{i-}})$$

voor geschikte $m_i \in \mathbb{N}$ en $w_1, \dots, w_k \in M$. Hieruit vinden we als volgt een M -pad van u naar v dat helemaal in $\mathbb{N}^m$ blijft: aan de linkerkant komt het monoom y^v met een minteken voor, dus dat moet ook aan de rechterkant met een minteken voorkomen. Kies een j waarvoor $y^{m_j} y^{w_{j-}} = y^v$, en zij $v' := m_j + w_{j+}$. Dan geldt dus $v' - v = w_{j+} - w_{j-} = w_j \in M$ en $y^v = y^{v'} + y^{m_j} (y^{w_{j+}} - y^{w_{j-}})$, zodat

$$y^u - y^{v'} = \sum_{i \neq j} y^{m_i} (y^{w_{i+}} - y^{w_{i-}}).$$

Aan de linkerkant staan minder termen, dus zo kunnen we doorgaan tot we een M -pad $v, v', \dots, u$ hebben. $\square$

3. Rang-1 matrices

We willen het ideaal bepalen van alle relaties tussen de enties van rang-1 matrices. Laat hiertoe z_{ij}, x_i, y_j , $i \in \{1, \dots, p\}, j \in \{1, \dots, q\}$ variabelen zijn en bekijk het ideaal $I \subseteq K[x, y, z]$ voortgebracht door de polynomen $z_{ij} - x_i y_j$ met $i = 1, \dots, p$ en $j = 1, \dots, q$. Het gaat ons om de relaties tussen de z_{ij} , dus we zijn geïnteresseerd in de doorsnede van I met $K[z]$. Zij A de $(p+q) \times pq$ -matrix waarvan de kolommen gelabeld zijn door de variabelen z_{ij} en de rijen door de variabelen $x_1, \dots, x_p, y_1, \dots, y_q$ en de kolom behorende bij z_{ij} precies twee enen heeft, in de rijen behorende bij x_i en bij y_j , en verder nullen. We zoeken een Markovbasis van A . Het is handig om A te interpreteren als de $\mathbb{Z}$ -lineaire afbeelding $\mathbb{Z}^{p \times q} \rightarrow \mathbb{Z}^p \times \mathbb{Z}^q$ die aan een $p \times q$ -matrix zijn p -tupel van rijssommen en zijn q -tupel van kolomsommen toevoegt. Zo bekeken is het eenvoudig elementen in de kern van A te vinden, zoals

$$\begin{bmatrix} 0 & 1 & 0 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = E_{ij} + E_{kl} - E_{il} - E_{kj}$$

(voor $p = 3, q = 4$). We bewijzen nu dat de verzameling

$$M = \{E_{ij} + E_{kl} - E_{il} - E_{kj} \mid i, k = 1, \dots, p; j, l = 1, \dots, q\}$$

een Markovbasis voor A is. Dit betekent dat als twee $p \times q$ matrices U en V met niet-negatieve geheeltallige enties dezelfde rij- en kolomsommen hebben, ze met elkaar kunnen worden verbonden door middel van een rij zetten uit M . Zolang $U - V$ niet nul is, kies de lexicografisch kleinste entry (i, j) waar ze verschillen. Neem aan dat $u_{ij} - v_{ij} > 0$. Dan bestaan er $k \neq i$ en $l \neq j$ zo dat $u_{il} - v_{il} < 0$ en $u_{kj} - v_{kj} < 0$ en $u_{kl} - v_{kl} > 0$ —waarom? Bewijs dit! Door nu bij V de matrix $E_{ij} + E_{kl} - E_{il} - E_{kj} \in M$ op te tellen blijf je binnen de matrices met niet-negatieve enties en lijkt het resultaat meer op U —hetzij de lexicografisch kleinste positie waar ze verschillen gaat omhoog, ofwel het verschil op die positie wordt kleiner. Na eindig veel zulke stappen is het resultaat U . Dit bewijst de volgende stelling.

STELLING 3.1. *Het ideaal $I \cap K[z]$ wordt voortgebracht door de 2×2 -subdeterminanten van de matrix z .*

OPGAVE 3.1. Reken met Singular een Markovbasis uit voor de $\mathbb{Z}$ -lineaire afbeelding die aan een $2 \times 2 \times 2$ -blok $b = (b_{ijk})$ van getallen een rijtje van 6 getallen, te weten $(\sum_{jk} b_{1jk}, \sum_{jk} b_{2jk}, \sum_{ik} b_{i1k}, \sum_{ik} b_{i2k}, \sum_{ij} b_{ij1}, \sum_{ij} b_{ij2})$ toevoegt.