

Effiziente Berechnung von Gröbnerbasen

Martin Kreuzer

Fachbereich Mathematik

Universität Dortmund

Situation.

$P = K[x_1, \dots, x_n]$ Polynomring über einem Körper K

P sei graduiert durch eine Matrix $W \in \text{Mat}_{m,n}(\mathbb{Z})$ in deren Spalten die Multigrade von $x_1, \dots, x_n$ stehen.

Die Graduierung sei positiv, d.h. der oberste von Null verschiedene Eintrag in jeder Spalte ist positiv.

Beispiel. $W = (1, \dots, 1)$ definiert die Standardgraduierung.

$F = \bigoplus_{i=1}^r P(-\delta_i)$ sei ein graduiert-freier P -Modul, d.h. ein freier P -Modul dessen i -tes Basiselement e_i den Multigrad $\delta_i \in \mathbb{Z}^m$ besitzt.

$M \subseteq F$ sei ein graduierter Untermodul, gegeben durch ein Erzeugendensystem $\mathcal{V} = (v_1, \dots, v_s)$ bestehend aus homogenen Vektoren von Polynomen.

Beispiel. Ist $F = P$, so ist M ein homogenes Ideal in P .

σ sei eine Modultermordnung auf $\mathbb{T}(e_1, \dots, e_r)$.

Ziele. Berechne eine σ -Gröbner Basis von M möglichst effizient. Ggf. berechne auch den Syzygienmodul von $\mathcal{V}$. Dabei gilt

$$\text{Syz}(\mathcal{V}) = \{(f_1, \dots, f_s) \mid f_1 v_1 + \dots + f_s v_s = 0\}$$

Notation. Wenn ein Vektor $g_i \in F$ vorkommt, schreibe

$$\text{LM}_\sigma(g_i) = c_i t_i e_{\gamma_i}$$

mit $c_i \in K$ Leitkoeffizient, t_i Potenzprodukt, $1 \leq \gamma_i \leq r$.

(i, j) mit $i < j$ und $\gamma_i = \gamma_j$ heisst **kritisches Paar**.

Setze $t_{ij} = \frac{\text{kgV}(t_i, t_j)}{t_i}$ für alle i, j .

$\sigma_{ij} = \frac{1}{c_i} t_{ij} e_i - \frac{1}{c_j} t_{ji} e_j$ heisst **fundamentale Syzygie**.

$S_{ij} = \frac{1}{c_i} t_{ij} g_i - \frac{1}{c_j} t_{ji} g_j$ heisst **S-Vektor**.

Σ sei die Menge aller fundamentalen Syzygien.

Der Multihomogene Buchberger Algorithmus

- 1) Sei $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$ und $s' = 0$.
- 2) Sei d der Lex-kleinste Multigrad in B oder in $\mathcal{W}$. Bilde $B_d = \{(i, j) \in B \mid \deg_W(\sigma_{ij}) = d\}$ und $\mathcal{W}_d$ und streiche ihre Elemente in B bzw. $\mathcal{W}$.
- 3) Ist $B_d = \emptyset$, so fahre mit 6) fort. Andernfalls wähle $(i, j) \in B_d$ und streiche es in B_d .
- 4) Berechne den normalen Rest $S'_{ij} = \text{NR}_{\sigma, \mathcal{G}}(S_{ij})$ des S-Vektors. Ist $S'_{ij} = 0$, so fahre mit 3) fort.
- 5) Erhöhe s' um eins, füge $g_{s'} = S'_{ij}$ zu $\mathcal{G}$ hinzu und füge $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ zu B hinzu. Fahre mit 3) fort.
- 6) Ist $\mathcal{W}_d = \emptyset$, so fahre mit 9) fort. Andernfalls wähle $v \in \mathcal{W}_d$ und streiche es in $\mathcal{W}_d$.
- 7) Finde $v' = \text{NR}_{\sigma, \mathcal{G}}(v)$. Ist $v' = 0$, so fahre mit 6) fort.
- 8) Erhöhe s' um eins, füge $g_{s'} = v'$ zu $\mathcal{G}$ hinzu und füge $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ zu B hinzu. Fahre mit 6) fort.
- 9) Ist $B = \emptyset$ und $\mathcal{W} = \emptyset$, so gib $\mathcal{G}$ aus und stoppe. Andernfalls fahre mit 2) fort.

Dies ist ein Algorithmus, der ein multihomogenes, gradaufsteigendes Tupel $\mathcal{G} = (g_1, \dots, g_{s'})$ berechnet welches eine σ -Gröbner Basis von M darstellt.

Optimierungen.

1) Es genügt in 3) – 5) eine Menge von kritischen Paaren (i, j) abzuarbeiten für die die zugehörigen fundamentalen Syzygien σ_{ij} den Modul $S = \text{Syz}(\text{LM}_\sigma(g_1), \dots, \text{LM}_\sigma(g_{s'}))$ erzeugen.

2) Von manchen Paaren kann man vielleicht von vorneherein wissen, dass sich $\text{NR}_{\sigma, \mathcal{G}}(S_{ij}) = 0$ ergibt. (Z.B. triviale Syzygien im Fall $r = 1$.)

3) Verwende einen anderen Algorithmus, um die Gröbner Basis zu berechnen!

Probleme.

1) Es ist keine einfache Art bekannt, wie man eine Teilmenge von Σ findet die S minimal erzeugt.

Die Regeln von Buchberger und Gebauer-Möller zur Entdeckung nicht-minimaler fundamentaler Syzygien liefern im Allgemeinen nur ein *fast* minimales Erzeugendensystem.

2) Welche Paare man als überflüssig betrachtet hängt stark vom Kontext der Berechnung ab (siehe unten). Über 1) hinausgehende allgemein anwendbare Regeln sind unbekannt.

3) Nur für spezielle Arten von Gröbner-Basis-Berechnungen sind effiziente Algorithmen bekannt.

Beispiel 1. In $P = \mathbb{Q}[x, y, z]$ betrachte $f_1 = x^2 - y^2$ und $f_2 = y^2 - xz - z^2$. Verwende die Termordnung $\sigma = \text{DegRevLex}$. Wegen $\text{LT}_\sigma(f_1) = x^2$ und $\text{LT}_\sigma(f_2) = y^2$ und $\text{ggT}(x^2, y^2) = 1$ ist das Paar $(1, 2)$ überflüssig (*triviale Syzygie*).

Beispiel 2. Sei $P = \mathbb{Q}[x, y, z]$ standard graduiert und sei $F = P \oplus P(-2)$. In F betrachte $v_1 = (x^2 - y^2, 0)$ und $v_2 = (y^2 - xz - z^2, 1)$. Verwende die Modultermordnung $\sigma = \text{DegRevLexPos}$.

Dann gilt $\text{LT}_\sigma(v_1) = x^2 e_1$ und $\text{LT}_\sigma(v_2) = y^2 e_1$, aber das kritische Paar $(1, 2)$ ist nicht überflüssig, denn es liefert das neue Gröbner-Basiselement

$$y^2 v_1 - x^2 v_2 = (-y^4 + x^3 z + x^2 z^2, -x^2) \xrightarrow{v_1, v_2} (0, -x^2 + y^2)$$

In Fall von Idealen *überflüssige* Paare
können im Fall von Moduln *unverzichtbar* sein!

Beispiel 3. Sei $P = \mathbb{Q}[x, y, z]$ standard graduiert. Betrachte die Polynome $f_1 = x^2 - y^2 - z^2$ und $f_2 = xy - xz + z^2$. Verwende die Termordnung $\sigma = \text{Lex}$.

Wegen $\text{LT}_\sigma(f_1) = x^2$ und $\text{LT}_\sigma(f_2) = xy$ liefert das Paar $(1, 2)$ ein neues Gröbner-Basiselement $f_3 = xz^2 + y^3 - y^2z + yz^2 - z^3$ und neue Paare $(1, 3)$ sowie $(2, 3)$. Die Berechnung geht wie folgt weiter:

Grad	1	2	3	4		
3	$-y$	x			$\longrightarrow f_3$	
4	$-z^2$		x		$\longrightarrow 0$	fundamentale Syzygie
4		$-z^2$	y		$\longrightarrow f_4$	
5		$-y^3$		x	$\longrightarrow 0$	total überflüssig
6	$-y^4$			x^2	Regel 1	
7		$-y^4$		xz^2	Regel 1	

mit $f_4 = y^4 - 2y^3z + 2y^2z^2 - 2yz^3$.

Die in Grad 4 berechnete Syzygie ist die fundamentale Syzygie $(-f_2, f_1)$ von (f_1, f_2) . Sie ist überflüssig für die Berechnung der Gröbner-Basis aber wesentlich für die Berechnung des Syzygienmoduls. Die in Grad 5 berechnete Syzygie ist in jeder Hinsicht überflüssig.

Für die Berechnung der Gröbner-Basis *überflüssige* Paare können für die Syzygienberechnung *unverzichtbar* sein!

Die Regeln von Gebauer-Möller

Regel 1. Streiche in Σ alle Elemente σ_{jk} für die es einen Index $i \in \{1, \dots, j-1\}$ gibt so dass t_{ki} den Term t_{kj} teilt. Die verbleibende Menge heiße Σ' .

Regel 2. Streiche in Σ' alle Elemente σ_{ik} für die es einen Index $j \in \{i+1, \dots, k-1\}$ gibt so dass t_{kj} ein echter Teiler von t_{ki} ist. Die verbleibende Menge heiße Σ'' .

Regel 3. Streiche in Σ'' alle Elemente σ_{ij} für die es einen Index $k \in \{j+1, \dots, s\}$ gibt so dass t_{ik} ein echter Teiler von t_{ij} ist und t_{jk} ist ein echter Teiler von t_{ji} . Die verbleibende Menge heiße Σ''' .

Dann erzeugt die Menge Σ''' immer noch den Modul $S = \text{Syz}(t_1 e_{\gamma_1}, \dots, t_s e_{\gamma_s})$.

Ist Σ''' stets ein minimales Erzeugendensystem von S ?

Was ist die tiefere mathematische Bedeutung dieser Regeln?

Beispiel 4. Sei $P = \mathbb{Q}[x, y, z]$ standard graduiert, sei $\sigma = \text{DegLex}$, und sei I das homogene Ideal das erzeugt wird von

$$f_1 = x^3 z^2 + x^2 y^2 z$$

$$f_2 = x^3 y^8, \text{ und}$$

$$f_3 = y^{10} z^2.$$

Die Leiterterme sind $t_1 = x^3 z^2$, $t_2 = x^3 y^8$ und $t_3 = y^{10} z^2$.

Grad	1	2	3	4	
13	$-y^8$	z^2			$\longrightarrow f_4$
14		$-y^2 z$		x	$\longrightarrow 0$
14			$-x^2$	z	$\longrightarrow 0$
15	$-y^{10}$		x^3		NICHT von GM entdeckt
15		$-z^2 y^2$	x^3		von GM entdeckt
15	$-y^{10}$			xz	von GM entdeckt

wobei $f_4 = x^2 y^{10} z$. Das Paar $(1, 3)$ wird von den Gebauer-Möller Regeln nicht entdeckt, ist aber überflüssig wegen

$$\sigma_{13} = z \sigma_{24} - x \sigma_{34} + y^2 \sigma_{12}$$

Kann man alle überflüssigen Paare entdecken

und dabei genauso schnell sein wie die GM-Regeln?

Die erste Idee wäre die Menge Σ während der Berechnung der Gröbner-Basis mit einem Standardverfahren zu minimalisieren. Dies ist zu ineffizient.

Der Buchberger Algorithmus mit Minimalisierung

- 1) Sei $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$ und $\mathcal{V}_{\min} = \emptyset$.
- 2) Sei d der Lex-kleinste Multigrad in B oder in $\mathcal{W}$. Bilde $B_d = \{(i, j) \in B \mid \deg_W(\sigma_{ij}) = d\}$ und $\mathcal{W}_d$ und streiche ihre Elemente in B bzw. $\mathcal{W}$.
- 3) Ist $B_d = \emptyset$, so fahre mit 6) fort. Andernfalls wähle $(i, j) \in B_d$ und steiche es in B_d .
- 4) Berechne den normalen Rest $S'_{ij} = \text{NR}_{\sigma, \mathcal{G}}(S_{ij})$ des S-Vektors. Ist $S'_{ij} = 0$, so fahre mit 3) fort.
- 5) Erhöhe s' um eins, füge $g_{s'} = S'_{ij}$ zu $\mathcal{G}$ hinzu und füge $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ zu B hinzu. Fahre mit 3) fort.
- 6) Ist $\mathcal{W}_d = \emptyset$, so fahre mit 9) fort. Andernfalls wähle $v \in \mathcal{W}_d$ und streiche es in $\mathcal{W}_d$.
- 7) Finde $v' = \text{NR}_{\sigma, \mathcal{G}}(v)$. Ist $v' = 0$, so fahre mit 6) fort.
- 8) Erhöhe s' um eins, füge $g_{s'} = v'$ zu $\mathcal{G}$ und v zu $\mathcal{V}_{\min}$ hinzu und füge $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ zu B hinzu. Fahre mit 6) fort.
- 9) Ist $B = \emptyset$ und $\mathcal{W} = \emptyset$, so gib $(\mathcal{G}, \mathcal{V}_{\min})$ aus und stoppe. Andernfalls fahre mit 2) fort.

Dies ist ein Algorithmus, der eine Gröbner-Basis $\mathcal{G}$ und ein in $\mathcal{V}$ enthaltenes minimales Erzeugendensystem $\mathcal{V}_{\min}$ von M berechnet.

Definition. Auf der Menge $\mathbb{T}(e_1, \dots, e_s)$ definieren wir eine Relation τ durch

$$t e_i \geq_\tau t' e_j \Leftrightarrow \begin{cases} \text{LT}_\sigma(t t_i e_{\gamma_i}) >_\sigma \text{LT}_\sigma(t' t_j e_{\gamma_j}), \text{ oder} \\ \text{LT}_\sigma(t t_i e_{\gamma_i}) = \text{LT}_\sigma(t' t_j e_{\gamma_j}) \text{ und } i \geq j \end{cases}$$

für Potenzprodukte t, t' und $i, j \in \{1, \dots, s\}$.

Die Relation τ ist eine Modultermordnung. Sie heisst die von $\mathcal{G}$ *induzierte* Modultermordnung.

Satz. Sei $\Sigma'' \subseteq \Sigma$ die nach Anwendung der Regeln 1) und 2) von Gebauer-Möller verbleibende Menge.

Dann ist $\tilde{\Sigma} = \{-c_j \cdot \sigma_{ij} \mid \sigma_{ij} \in \Sigma''\}$ die **reduzierte τ -Gröbner Basis** des Moduls

$$\text{Syz}_P(\text{LM}_\sigma(\mathcal{G})) = \text{Syz}_P(c_1 t_1 e_{\gamma_1}, \dots, c_s t_s e_{\gamma_s})$$

Folgerung. Wir müssen eine reduzierte Gröbner-Basis minimalisieren. Dazu kann man den Buchberger Algorithmus stark verbessern.

Minimalisierung einer Reduzierten Gröbner Basis

Sei $\mathcal{V}$ die reduzierte σ -Gröbner Basis von M .

- 1) Sei $B = \emptyset$, $\mathcal{W} = \mathcal{V}$, $\mathcal{G} = \emptyset$, $s' = 0$ und $\mathcal{V}_{\min} = \emptyset$.
- 2) Sei d der kleinste Grad eines Elements von B oder $\mathcal{W}$.
Bilde B_d und $\mathcal{W}_d$ und streiche ihre Elemente aus B bzw. $\mathcal{W}$.
- 3) Ist $B_d = \emptyset$, so fahre mit 6) fort. Andernfalls wähle $(i, j) \in B_d$ und streiche es in B_d .
- 4) Sei $S'_{ij} = \text{NR}_{\sigma, \mathcal{G}}(S_{ij})$. Ist $S'_{ij} = 0$, so fahre mit 3) fort.
- 5) Erhöhe s' um eins, füge $g_{s'} = S'_{ij}$ zu $\mathcal{G}$ hinzu und füge $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ zu B hinzu. Fahre mit 3) fort.
- 6) Ist $\mathcal{W}_d = \emptyset$, so fahre mit 9) fort. Andernfalls wähle $v \in \mathcal{W}_d$ und streiche es in $\mathcal{W}_d$.
- 7) Ist $\text{LT}_{\sigma}(v) = \text{LT}_{\sigma}(g)$ für ein $g \in \mathcal{G}$, so ersetze g in $\mathcal{G}$ durch v . Fahre mit 6) fort.
- 8) Erhöhe s' um eins, füge $g_{s'} = v$ zu $\mathcal{G}$ und $\mathcal{V}_{\min}$ hinzu und füge $\{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$ zu B hinzu. Fahre mit 6) fort.
- 9) Ist $B = \emptyset$ und $\mathcal{W} = \emptyset$, so gib $\mathcal{V}_{\min}$ aus und stoppe. Andernfalls fahre mit 2) fort.

Die ist ein Algorithmus der ein in $\mathcal{V}$ enthaltenes minimales Erzeugendensystem $\mathcal{V}_{\min}$ von M berechnet.

Folgerungen. a) Wendet man diesen Algorithmus auf die reduzierte τ -Gröbner Basis $\tilde{\Sigma}$ von $\text{Syz}(\text{LM}_\sigma(\mathcal{G}))$ an, so kann man ihn noch weiter beschleunigen.

b) Man kann die so erhaltene Minimalisierung der kritischen Paare in den multihomogenen Buchberger Algorithmus einbauen. Das Resultat ist der optimierte Buchberger Algorithmus (siehe unten).

c) Die Minimalisierung der kritischen Paare ist dabei ebenso schnell und effizient wie die Anwendung der Regeln von Gebauer-Möller. Sie findet aber *alle* nicht-minimalen kritischen Paare.

Der Optimierte Buchberger-Algorithmus

- 1) Sei $\mathcal{W} = \mathcal{V}$, $A = \emptyset$, $B = \emptyset$, $B^* = \emptyset$, $\mathcal{G} = \emptyset$ und $s' = 0$.
- 2) Sei d der Lex-kleinste Grad eines Elements von B oder $\mathcal{W}$.
Bilde B_d , B_d^* , $\mathcal{W}_d$, und streiche ihre Elemente aus B , B^* ,
und $\mathcal{W}$.
- 3) *Wende* $\text{MinPairs}(A, B_d, B_d^*)$ *an*.
- 4) Ist $B_d = \emptyset$, so fahre mit 7) fort. Andernfalls wähle
 $(i, j) \in B_d$, streiche es in B_d , und füge es zu A hinzu.
- 5) Berechne S_{ij} und $S'_{ij} = \text{NR}_{\sigma, \mathcal{G}}(S_{ij})$. Ist $S'_{ij} = 0$, so fahre
mit 4) fort.
- 6) Erhöhe s' um eins, füge $g_{s'} = S'_{ij}$ zu $\mathcal{G}$ hinzu, führe
 $\text{Update}(B, B^*, g_{s'})$ durch und fahre mit 4) fort.
- 7) Ist $\mathcal{W}_d = \emptyset$ so fahre mit 10) fort. Andernfalls wähle
 $v \in \mathcal{W}_d$ und streiche es aus $\mathcal{W}_d$.
- 8) Berechne $v' = \text{NR}_{\sigma, \mathcal{G}}(v)$. Ist $v' = 0$, so fahre mit 7) fort.
- 9) Erhöhe s' um eins, füge $g_{s'} = v'$ zu $\mathcal{G}$ hinzu und führe
 $\text{Update}(B, B^*, g_{s'})$ durch. Dann fahre mit 7) fort.
- 10) Ist $B = \emptyset$ und $\mathcal{W} = \emptyset$, so gib $\mathcal{G}$ aus und stoppe. Andern-
falls fahre mit 2) fort.

Hierbei ist die Prozedur $\text{Update}(B, B^*, g_{s'})$ wie folgt definiert.

- U1) Bilde die Menge $C = \{(i, s') \mid 1 \leq i < s', \gamma_i = \gamma_{s'}\}$.
- U2) Streiche in C alle Paare (j, s') für die es ein $i \in \{1, \dots, j-1\}$ gibt so dass $t_{s'i}$ das Monom $t_{s'j}$ teilt.
- U3) Streiche in C alle Paare (i, s') für die es ein $j \in \{i+1, \dots, s'-1\}$ gibt so dass $t_{s'j}$ das Monom $t_{s'i}$ echt teilt.
- U4) Finde in C alle Paare (i, s') und (j, s') so dass $1 \leq i < j < s'$ und $\gcd(t_{is'}, t_{js'}) = 1$ gilt. Prüfe jeweils ob (i, j) schon in B^* liegt und füge es evtl. an.
- U5) Füge alle Elemente von C zu B hinzu und stoppe.

Ferner sei $\text{MinPairs}(A, B_d, B_d^*)$ die folgende Prozedur.

- M1) Ist $B_d^* = \emptyset$, so stoppe. Andernfalls wähle ein Paar (i, j) in B_d^* und streiche es aus B_d^* .
- M2) Ist $t_{ji} = t_{ji'}$ für $(i', j) \in A$, so fahre mit M1) fort.
- M3) Ist $t_{ji} = t_{ji'}$ für ein Paar $(i', j) \in B_d$, so streiche dieses Paar in B_d und füge es zu A hinzu. Fahre mit M1) fort.
- M4) Finde $(i', j) \in A$ so dass $t_{ji'}$ das Monom t_{ji} teilt. Sei $(k, \ell) = (\min\{i, i'\}, \max\{i, i'\})$. Ist $\gcd(t_{ij}, t_{i'j}) \neq 1$, so fahre mit M1) fort.
- M5) Ist $t_{\ell k} = t_{\ell k'}$ für $(k', \ell) \in A$, so fahre mit M1) fort.
- M6) Ist $t_{\ell k} = t_{\ell k'}$ für ein Paar $(k', \ell) \in B_d$, so streiche dieses Paar in B_d , füge es zu A hinzu und fahre mit M1) fort.
- M7) Ist $(k, \ell) \in B_d^*$, so streiche (k, ℓ) in B_d^* und fahre mit M4), angewendet auf dieses Paar, fort.
- M8) Fahre mit M1) fort.

Dies ist ein Algorithmus der ein gradweise aufsteigend geordnetes Tupel $\mathcal{G} = \{g_1, \dots, g_{s'}\}$ homogener Vektoren berechnet dessen Elemente eine homogene σ -Gröbner-Basis von M darstellen.

Ferner entsprechen die Paare, die irgendwann in den Schritten 4)–6) abgearbeitet werden, einem minimalen Erzeugendensystem des Moduls $\text{Syz}_P(c_1 t_1 e_{\gamma_1}, \dots, c_{s'} t_{s'} e_{\gamma_{s'}})$.

Der Buchberger-Möller Algorithmus

Sei $\varphi : P \longrightarrow K^s$ eine K -lineare Abbildung, deren Kern ein Ideal von P ist. Die Abbildung φ sei effizient berechenbar. Ferner sei σ eine Termordnung auf $\mathbb{T}^n$.

Frage. Kann man den Kern von φ effizient berechnen?

Beispiel 1 (Multivariate Interpolation). Seien Punkte $P_1, \dots, P_s \in K^n$ gegeben durch ihre Koordinaten

$$P_i = (p_{i1}, \dots, p_{in})$$

Die Abbildung φ sei die Auswertung

$$\varphi(f) = (f(P_1), \dots, f(P_s))$$

Dann ist $\ker(\varphi)$ das Verschwindungsideal von $\{P_1, \dots, P_s\}$, d.h. das Ideal aller Polynome, die an allen Punkten verschwinden.

Beispiel 2 (Hermite Interpolation).

Seien wieder Punkte $P_1, \dots, P_s \in K^n$ durch ihre Koordinaten gegeben. Ferner seien positive ganze Zahlen $d_1, \dots, d_s$ gegeben. Die Abbildung $\varphi : P \longrightarrow K^t$ mit $t = \binom{d_1+n-1}{n-1} + \dots + \binom{d_s+n-1}{n-1}$ sei dadurch gegeben dass man für $i = 1, \dots, s$ ein Polynom f an der Stelle P_i bis zum Grad $d_i - 1$ in eine Potenzreihe entwickelt und die Koeffizienten (bzgl. der Basis $\mathbb{T}^n$) aneinanderreihet.

Der Kern von φ besteht aus der Lösung des Hermiteschen Interpolationsproblems zu den Exponenten $(d_1, \dots, d_s)$, d.h. aus dem Ideal aller Polynome, die in P_i von mindestens d_i -ter Ordnung verschwinden. Die Abbildung φ ist durch eine geeignete Variante des Horner-Schemas effizient berechenbar.

Beispiel 3 (Projektive Punkte).

Gegeben seien Punkte $P_1, \dots, P_s$ im projektiven Raum $\mathbb{P}^n(K)$ über K . Für jeden Punkt wähle ein festes Koordinatentupel $P_i = (p_{i0}, \dots, p_{in})$.

Gesucht ist das homogene Verschwindungsideal I dieser Punkte, d.h. das Ideal das erzeugt wird von allen homogenen Polynomen, die an diesen Punkten verschwinden. Für jedes $d \geq 0$ betrachte

$$\varphi_d: P_d \longrightarrow K^s \quad \text{mit} \quad \varphi_d(f) = (f(P_1), \dots, f(P_s))$$

Berechnet man $\ker(\varphi_d)$ Grad für Grad nach dem Schema des Buchberger-Möller Algorithmus, so benötigt man ein *Stoppkriterium* dafür, dass man ein Erzeugendensystem von ganz I gefunden hat.

Beispiel 4 (Homogene Implizitisierung).

Gegeben sind homogene Polynome $f_1, \dots, f_m \in P$ vom gleichen Grad δ . Gesucht ist das Ideal der algebraischen Relationen zwischen diesen Polynomen, also das Ideal

$$I = \{g(y_1, \dots, y_m) \mid g(f_1, \dots, f_m) = 0\} \subseteq K[y_1, \dots, y_m]$$

Offenbar ist I ein homogenes Ideal und man kann es Grad für Grad berechnen. In jedem Grad d ist

$$\varphi_d : K[y_1, \dots, y_m]_d \longrightarrow K^s \cong P_{\delta d}$$

mit $\varphi_d(g) = g(f_1, \dots, f_m)$ eine lineare Abbildung mit Kern I_d . Wiederum braucht man ein Stoppkriterium, das im vorliegenden Fall z.B. aus der Kenntnis der Hilbert-Funktion von I abgeleitet sein könnte.

Der Buchberger-Möller Algorithmus

Sei σ eine Termordnung auf $\mathbb{T}^n$ und seien $P_1, \dots, P_s \in K^n$ mit $P_i = (p_{i1}, \dots, p_{in})$ gegeben.

- 1) Sei $G = \emptyset$, $S = \emptyset$, $L = (1)$ und $M = (m_{ij})$ eine $0 \times s$ Matrix.
- 2) Ist $L = \emptyset$ so gib G aus und stoppe. Andernfalls wähle $t = \min_{\sigma}(L)$ und streiche es in L .
- 3) Berechne $\varphi(t) = (t(P_1), \dots, t(P_s))$ und reduziere es gegen die Zeilen von M . Erhalte

$$(v_1, \dots, v_s) = (t(P_1), \dots, t(P_s)) - \sum_i a_i (m_{i1}, \dots, m_{is})$$

mit $a_i \in K$.

- 4) Ist $(v_1, \dots, v_s) = (0, \dots, 0)$ so füge $t - \sum_i a_i s_i$ zu G hinzu, wobei s_i das i -te Element von S ist. Streiche in L die Vielfachen von t . Fahre mit 2) fort.
- 5) Ist $(v_1, \dots, v_s) \neq (0, \dots, 0)$ so füge $(v_1, \dots, v_s)$ als neue Zeile zu M hinzu und $t - \sum_i a_i s_i$ als neues Element zu S . Füge zu L alle Terme in $\{x_1 t, \dots, x_n t\}$ hinzu, die weder Vielfaches eines Elements aus L noch aus $\text{LT}_{\sigma}(G)$ sind. Fahre mit 2) fort.

Dies ist ein Algorithmus, der die reduzierte σ -Gröbner Basis des Ideals $I = \ker(\varphi)$ berechnet.

Projektive Version des BM-Algorithmus

Sei σ eine Termordnung auf $\mathbb{T}^{n+1}$ und seien $P_1, \dots, P_s \in \mathbb{P}^n(K)$ mit $P_i = (p_{i0}, p_{i1}, \dots, p_{in})$ gegeben.

- 1) Sei $G = \emptyset$, $S = \emptyset$ und $L = (1)$. Sei $d = 0$.
- 2) *Gilt Stoppkriterium(G)=TRUE, so gib G aus und stoppe. Andernfalls erhöhe d um eins. Sei $M = (m_{ij})$ eine $0 \times s$ Matrix und $L = \mathbb{T}_d^n \setminus \text{LT}_\sigma(G)$.*
- 2) Ist $L = \emptyset$ so fahre mit 2) fort. Andernfalls wähle $t = \min_\sigma(L)$ und streiche es in L .
- 3) Berechne $\varphi(t) = (t(P_1), \dots, t(P_s))$ und reduziere es gegen die Zeilen von M . Erhalte $a_i \in K$ mit

$$(v_1, \dots, v_s) = (t(P_1), \dots, t(P_s)) - \sum_i a_i (m_{i1}, \dots, m_{is})$$

- 4) Ist $(v_1, \dots, v_s) = (0, \dots, 0)$ so füge $t - \sum_i a_i s_i$ zu G hinzu, wobei s_i das i -te Element von S ist. Streiche in L die Vielfachen von t . Fahre mit 3) fort.
- 5) Ist $(v_1, \dots, v_s) \neq (0, \dots, 0)$ so füge $(v_1, \dots, v_s)$ als neue Zeile zu M hinzu und $t - \sum_i a_i s_i$ als neues Element zu S . Fahre mit 3) fort.

Dies ist ein Algorithmus, der die reduzierte σ -Gröbner Basis des homogenen Verschwindungsideals von $\{P_1, \dots, P_s\}$ berechnet.

Problem. Wir brauchen ein möglichst gutes Stoppkriterium.

Das *naive* Stoppkriterium $d > s$ ist viel zu schwach. Wir bräuchten eine Gradschranke für die reduzierte Gröbner-Basis eines 1-dimensionalen Cohen-Macaulay Ideals.

Definition. Zwei Monome $t, t' \in \mathbb{T}_d^{n+1}$ heißen *verbunden* in einer Teilmenge Q , wenn es eine Kette

$$t = t_0, \quad t_1, \quad \dots, \quad t_r = t'$$

in Q gibt mit $t_i = t_{i-1} \cdot x_\alpha / x_\beta$ für $i = 1, \dots, r$.

Auf diese Weise zerfällt Q in Zusammenhangskomponenten.

Satz. Für $P_1, \dots, P_s \in \mathbb{P}^n(K)$ gebe es einen Grad d so dass Folgendes gilt:

- a) In $Q = \mathbb{T}_d^{n+1} \setminus \text{LT}_\sigma(I)_d$ liegen genau s Monome.
- b) Für $i = 0, \dots, n$ ist jedes Monom in der Zusammenhangskomponente von x_i^d in Q durch x_i teilbar.

Dann haben alle Elemente der reduzierten σ -Gröbner-Basis von I einen Grad $\leq d$.

Computeralgebrasystem CoCoA

- momentante Version 4.2, graphisches Interface, top-level Programmierung
- in einigen Wochen: Version 5, C++ Bibliothek, Source Code verfügbar

Dritte Int. Schule der Computeralgebra

- 2. – 5. Juni 2003 in Cadiz (Spanien)
- Zwei Kurse und ein Minikurs:
 - Computational Invariant Theory (G. Kemper)
 - Computing in Multigraded Structures (M. Kreuzer)
 - Computational Aspects of D-Modules (J-M. Ucha)

Konferenz CoCoA 8

- 5. – 7. Juni 2003 in Cadiz (Spanien)

Buch “Computational Commutative Algebra”

- Autoren M. Kreuzer und L. Robbiano
- Band 1: Springer, Heidelberg 2000 (Yellow Sale!)
- Band 2: erscheint 2004