Starke Gröbnerbasen über Euklidischen Ringen

UNIVERSITÄT
LEIPZIG

gemeinsames Projekt mit

Gerhard Pfister und

Adrian Popescu

#0
Ausgangssituation

$\mathcal{R}$ bezeichnet einen Euklidischen Ring, hier meistens $\mathcal{R} = \mathbb{Z}$, $\mathcal{R}$ nullteilerfrei

Polynomring $\mathcal{P}$ über $\mathcal{R}$ in n Variablen:

$$\mathcal{P} = \mathcal{R}[x_1, \ldots, x_n] = \mathcal{R}[x]$$

Wir haben eine **Monomordnung** $<$ auf $\mathcal{P}$ gegeben.

Hier ist $<$ **global**, also $x_i > 1$ für alle i.

Für Terme eventuell Auflösung in $\mathcal{R}$, z.B.

$4x < -15x$ in $\mathbb{Z}[x]$ da $|4| < |-15|$ in $\mathbb{Z}$.

Wir können dann für $f \in \mathcal{P}$

den **Leitterm** $\mathrm{lt}(f)$,
den **Leitkoeffizienten** $\mathrm{lc}(f)$
und das **Leitmonom** $\mathrm{lm}(f)$

eindeutig angeben.

Beispiel:

$f = 12x^2 - 17xy^2 + 4 \in \mathbb{Z}[x, y]$ mit $<$ DRL

$$\begin{aligned} \mathrm{lt}(f) &= -17xy^2 \\ \mathrm{lc}(f) &= -17 \\ \mathrm{lm}(f) &= xy^2 \end{aligned}$$

Es gilt $\mathrm{lt}(f) = \mathrm{lc}(f)\,\mathrm{lm}(f)$.

Sei $I \lhd \mathcal{P}$ ein Ideal. Wir definieren
das **Leitideal von** I als das Ideal $L(I)$ erzeugt
von allen Leittermen von allen Elementen in I.

Sei $F \subset \mathcal{P}$ eine Menge. Wir definieren
das **Leitideal von** F durch $L(F) = \langle lt(f) \mid f \in F \rangle$.

Gegeben $I \lhd \mathcal{P}, G \subset \mathcal{P}$, so heißt G **Gröbnerbasis** für I falls gilt:

$G \subset I$ und $L(G) = L(I)$.

Gröbnerbasen können wir berechnen mit **Buchbergers Algorithmus**

Grundlegende Struktur:

Für $f, g \in \mathcal{P} \setminus \{0\}$ definieren wir das **S-Polynom**

$$\mathrm{spoly}(f, g) = \lambda f - \sigma g$$

mit $\lambda \,\mathrm{lt}(f) = \sigma \,\mathrm{lt}(g)$ wobei λ, σ minimale Terme mit dieser Eigenschaft sind.

Spezialfall: **Reduktion**

Falls $\lambda = 1$ festgelegt brauchen wir g mit

$\mathrm{lt}(f) = \sigma\,\mathrm{lt}(g)$, so dass $\mathrm{lt}(f - \sigma g) < \mathrm{lt}(f)$.

Schreibweise $\overline{f}^{G}$ meint

(1) Solange $f \neq 0$, suche passendes $g \in G$.
(2) Falls erfolgreich, setze $f \leftarrow f - \sigma g$.
    Zurück zu Schritt 1.
(3) Gib f zurück.

Buchbergers Kriterium:

Falls $G \subset \mathcal{P}$ und **für alle** $f, g \in G$ gilt

$$\overline{\text{spoly}(f, g)}^{G} = 0,$$

dann ist G eine Gröbnerbasis für $\langle G \rangle$.

$I = \langle f_1, \ldots, f_r \rangle \subset \mathcal{P}$

$G \leftarrow \{f_1, \ldots, f_r\}$

$P \leftarrow \{(f_i, f_j) \mid 1 \leq i < j \leq r\}$

While $(P \neq \emptyset)$ do

  Wähle (p, q), $P \leftarrow P \setminus \{(p, q)\}$

  $h \leftarrow \mathrm{spoly}(p, q) = \lambda p - \sigma q$

  $h \leftarrow \overline{h}^{G}$

  If $h \neq 0$?

    $P \leftarrow P \cup \{(h, g) \mid g \in G\}$

    $G \leftarrow G \cup \{h\}$

Return G

Ist $\mathcal{R}$ ein **Körper**, $G \subset I$, so gilt:

$$L(I) = L(G)$$

$$\Longleftrightarrow$$

Für alle $f \in I \setminus \{0\}$ existiert $g \in G$ mit $\mathrm{lt}(g) \mid \mathrm{lt}(f)$.

Leider gilt diese Äquivalenz **nicht** über beliebigen Euklidischen Ringen:

$\Longleftarrow$ 

$\Longrightarrow$ 

Beispiel:

Betrachte $I = \langle x \rangle \lhd \mathbb{Z}[x]$.

$G = \{2x, 3x\}$ ist eine Gröbnerbasis für I:

$G \subset I$, $L(I) = \langle x \rangle$ und $x = 3x - 2x \in L(G)$.

aber $2x \nmid x$ und $3x \nmid x$.

Gegeben $I \triangleleft \mathcal{P}, G \subset \mathcal{P}$ nennen wir G **starke Gröbnerbasis** für I falls gilt:

Für alle $f \in I \setminus \{0\}$ existiert $g \in G$ mit $\mathrm{lt}(g) \mid \mathrm{lt}(f)$.

Problem in unserem Beispiel?

$\text{spoly}(2x, 3x) = 0$

Müssen $\gcd(2, 3) = 1$ erreichen **ohne** das Monom zu kürzen.

Idee:

G-Polynom von $2x$ und $3x$ bilden:

$$\text{gpoly}(2x, 3x) = (-1) \cdot (2x) + 1 \cdot (3x) = x.$$

Neue Struktur:

Für $f, g \in \mathcal{P} \setminus \{0\}$ definieren wir das **G-Polynom**

$$\mathrm{gpoly}(f, g) = a u f + b v g$$

mit $u\,\mathrm{lm}(f) = v\,\mathrm{lm}(g)$, u, v minimale Monome und
$a\,\mathrm{lc}(f) + b\,\mathrm{lc}(g) = \gcd(\mathrm{lc}(f), \mathrm{lc}(g))$, $a, b \in \mathcal{R}$.

S-Polynom $\Longrightarrow$ Leitmonom wird gekürzt

G-Polynom $\Longrightarrow$ Leitkoeffizient wird gcd,
Leitmonom bleibt erhalten

Verallgemeinertes Buchberger Kriterium:

Falls $G \subset \mathcal{P}$ und **für alle** $f, g \in G$ gilt

$\overline{\text{spoly}(f,g)}^{G} = 0$ **und** $\overline{\textbf{gpoly}(f,g)}^{G} = 0$,

dann ist G eine **starke** Gröbnerbasis für $\langle G \rangle$.

#1
Unnötige Paare

Für $f, g \in G$ mit $lc(f) \mid lc(g)$ gilt:

$$\overline{\text{gpoly}(f, g)}^{\{f,g\}} = 0.$$

Buchbergers Produktkriterium

Für $f, g \in G$ mit $\mathrm{lc}(f), \mathrm{lc}(g)$ **teilerfremd** und $\mathrm{lm}(f), \mathrm{lm}(g)$ **teilerfremd** gilt:

$$\overline{\mathrm{spoly}(f,g)}^{\{f,g\}} = 0.$$

Gilt nicht für G-Polynome:

$$\mathrm{gpoly}(3x, 2y) = y \cdot 3x - x \cdot 2y = xy \neq 0.$$

Buchbergers Kettenkriterium (spoly)

Für $f, g, h \in G$ mit

$\mathrm{lm}(f) \mid \mathrm{lcm}(\mathrm{lm}(g), \mathrm{lm}(h))$ und
$\mathrm{lc}(f) \mid \mathrm{lcm}(\mathrm{lc}(g), \mathrm{lc}(h))$

können wir $\mathrm{spoly}(g, h)$ löschen, solange wir $\mathrm{spoly}(f, g)$ und $\mathrm{spoly}(f, h)$ betrachten.

Buchbergers Kettenkriterium (gpoly)

Für $f, g, h \in G$ mit

$\mathrm{lm}(f) \mid \mathrm{lcm}(\mathrm{lm}(g), \mathrm{lm}(h))$ und
$\mathrm{lc}(f) \mid \gcd(\mathrm{lc}(g), \mathrm{lc}(h))$

können wir $\mathrm{gpoly}(g, h)$ löschen, solange wir $\mathrm{gpoly}(f, g)$ und $\mathrm{gpoly}(f, h)$ betrachten.

Ergebnis von Lichtblau

Für $f, g \in G$ betrachte **nur**

- $\mathrm{spoly}(f, g)$ falls $\mathrm{lc}(f) \mid \mathrm{lc}(g)$ oder $\mathrm{lc}(g) \mid \mathrm{lc}(f)$,
- $\mathrm{gpoly}(f, g)$ falls $\mathrm{lc}(f) \nmid \mathrm{lc}(g)$ und $\mathrm{lc}(g) \nmid \mathrm{lc}(f)$.

#2
Koeffizientenwachstum vermeiden

Modulare Techniken funktionieren meist **nicht**:

$I = \langle 6x, 8x \rangle \triangleleft \mathbb{Z}[x]$, dann ist $G = \{2x, 6x, 8x\}$ eine starke Gröbnerbasis.

Gröbnerbasen bzgl. Primzahlen $p > 3$ würden immer $G_p = \{x\}$ sein.

Idee: Versuche **Konstante** oder **Monom**
zu finden, die / das in $\mathrm{I} \lhd \mathcal{P}$ liegt.

Kürze damit bei Reduktionen die Koeffizienten.

Sei $I = \langle f_1, \ldots, f_r \rangle \triangleleft \mathbb{Z}[x]$.

- Betrachte I über $\mathbb{Q}$.
- Berechne Gröbnerbasis G von I **über** $\mathbb{Q}$.
- Gilt $G = 1$ so existiert Konstante c in I über $\mathbb{Z}$.
- Berechne $S = \mathrm{syz}(1, f_1, \ldots, f_r) \subset \sum_{i=0}^{r} \mathbb{Q}[x] e_i$.
  Dann $\exists\, \sigma \in S$ der Form $se_0 + \ldots$ mit $s \in \mathbb{Q}$.
  Finde $k \in \mathbb{Z}$ so dass $k\sigma \in \sum_{i=0}^{r} \mathbb{Z}[x] e_i$.
- Setze $I = \langle ks, f_1, \ldots, f_r \rangle$.

#3
Reduktionen verallgemeinern

Bislang kürzen wir f mit g falls $\mathrm{lt}(g) \mid \mathrm{lt}(f)$, d.h. $\lambda \mathrm{lt}(g) = \mathrm{lt}(f)$.

Dann gilt $\mathrm{lt}(f - \lambda g) < \mathrm{lt}(f)$.

Wollen aber **auch Leitkoeffizienten klein** halten.

Verallgemeinerte Reduktion von f bzgl. G:

Suche $g \in G$ mit $\mathbf{lm}(g) \mid \mathbf{lm}(f)$.

1.

Falls $\mathrm{lc}(g) \mid \mathrm{lc}(f)$ kürze Leitterm:

$\mathrm{lt}(f - \lambda g) < \mathrm{lt}(f)$ **und** $\mathrm{lm}(f - \lambda g) < \mathrm{lm}(f)$

2.

Falls $\mathrm{lc}(g) \nmid \mathrm{lc}(f)$ und $\mathbf{lm}(g) < \mathbf{lm}(f)$
so kürze den Leitkoeffizienten falls
$a \in \mathcal{R}$ existiert mit $\mathrm{lc}(f) - a\,\mathrm{lc}(g) < \mathrm{lc}(f)$:

$\mathrm{lt}(f - \lambda g) < \mathrm{lt}(f)$ **aber** $\mathrm{lm}(f - \lambda g) = \mathrm{lm}(f)$

3.

Und falls $\mathrm{lc}(g) \nmid \mathrm{lc}(f)$ und $\mathbf{lm}(g) = \mathbf{lm}(f)$**?**

Tausche f, g mit $\mathrm{spoly}(f, g), \mathrm{gpoly}(f, g)$ aus.

Lemma

$$\langle f, g \rangle = \langle \mathrm{spoly}(f, g), \mathrm{gpoly}(f, g) \rangle$$

falls $\mathrm{lm}(f) = \mathrm{lm}(g)$.

Beweis:

Zeige, dass beide Paare das gleiche Gitter aufspannen.

Betrachte hierzu $M = \begin{pmatrix} u & v \\ \frac{lc(g)}{d} & -\frac{lc(f)}{d} \end{pmatrix}$ wobei

$$\begin{aligned} gpoly(f,g) &= u\ f + v\ g \\ spoly(f,g) &= \frac{lc(g)}{d}\ f - \frac{lc(f)}{d}\ g \\ gcd(lc(f), lc(g)) &= d \end{aligned}$$

$$\det(M) = -u\frac{lc(f)}{d} - v\frac{lc(g)}{d} = -\frac{1}{d}\left(u\,lc(f) + v\,lc(g)\right) = -1.$$

Also ist M invertierbar.

#4
Implementierung

Verfügbar in **Singular** $4-1-2$.

Beispiele	**Singular** (Lichtblau)	**Singular**	**Macaulay2**	**Magma**
Cyclic-6	0,330	0,320	4,708	2,799
Cyclic-7	18.731,820	5.636,210	out of memory	366,060
Katsura-7	2,200	2,250	204,928	251,630
Katsura-8	133,390	135,360	64.555,420	(> 24h)
Katsura-9	13.366,590	12.951,160	(> 24h)	(> 24h)
Eco-9	3,920	4,050	870,409	22,520
Eco-10	38,760	40,670	(> 24h)	289,540
F-633	0,140	0,120	14,982	12,880
F-744	118,610	117,890	(> 24h)	(> 24h)
Noon-7	34,930	32,700	(> 24h)	(> 24h)
Noon-8	3.1390,060	3.079,370	(> 24h)	(> 24h)
Reimer-5	3,620	3,590	out of memory	1.932,400
Reimer-6	1.216,960	1.232,530	out of memory	(> 24h)
Lichtblau	1,910	1,830	69,536	2.242,900
Bayes-148	9,970	9,900	117,635	46,240
Mayr-42	212,320	212,770	218,635	40,270
Yang-1	149,120	147,250	181,210	50,330
Jason-210	47,010	46,780	(> 24h)	(> 24h)

#5
Nähere Zukunft

Neue Ideen für $\mathbb{Z}_N$ falls N keine Primzahl

mit **Tommy Hofmann**

F4 Algorithmus über Euklidischen Ringen in **gb / GB.jl** für **OSCAR**.

Danke für Ihre Aufmerksamkeit

Fragen? Anmerkungen?