Eindeutigkeit reduzierter Gröbnerbasen

Satz Existenz und Eindeutigkeit reduzierter Gröbnerbasen

Jedes Ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ besitzt eine eindeutige reduzierte Gröbnerbasis.

Beweis:

- **Existenz:** Hilbert Basissatz: $I = \langle G \rangle$ mit endlicher Basis G. Das G aus dem Beweis zum Basissatz ist bereits eine Gröbnerbasis.
- Anwendung der Algorithmen MINIMIERE GRÖBNER und REDUZIERE GRÖBNER führt zu einer reduzierten Basis G.
- **Eindeutigkeit:** Seien G und G' reduzierte Gröbnerbasen von I.
- Da G, G' Gröbnerbasen sind, gilt $\langle LT(G) \rangle = \langle LT(G') \rangle = \langle LT(I) \rangle$.
- $LT(I)$ ist ein Monomideal. Zwei Monomideal sind gleich gdw sie dieselben Monome enthalten. D.h es gilt $LT(G) = LT(G')$.
- Daher existiert für jedes $g \in G$ ein $g' \in G'$ mit $LT(g) = LT(g')$.

Gleichheit von Idealen

Beweis: (Fortsetzung)

- Es genügt zu zeigen, dass $g = g'$.
- Wegen $LT(g) = LT(g')$, wird $LT(g - g')$ eliminiert.
- Da G, G' reduziert sind, wird keiner der Terme in $g - g'$ von einem der $LT(g_i)$ geteilt. D.h.
$$\overline{g - g'}^{G} = g - g'.$$
- Da $g, g' \in I$, gilt $g - g' \in I$.
- Da G eine Gröbnerbasis ist, folgt damit
$$\overline{g - g'}^{G} = 0.$$
- Dies zeigt $g = g'$ und damit sind G und G' identisch.

Algorithmus GLEICHHEIT IDEALE

EINGABE: $I_1 = \langle f_1, \ldots, f_\ell \rangle$, $I_2 = \langle g_1, \ldots, g_m \rangle$.

1. Fixiere eine beliebige Monomordnung.
2. Berechne reduzierte Gröbnerbasen G_1, G_2 für I_1, I_2.

AUSGABE: $I_1 = I_2$ gdw $G_1 = G_2$.

Algorithmische Betrachtungen

Anmerkung: Effizienz

- Ziel: Effizienzsteigerung des BUCHBERGER-Algorithmus durch Vermeidung von unnötigen S-Polynom Berechnungen.
- Verwendet Verallgemeinerung von S-Polynomen.
- Implementierungen im F4- und F5-Algorithmus.

Laufzeit von BUCHBERGER:

- Sei I ein Ideal mit Generatoren vom Multigrad α.
- Sei der Grad definiert als $d = \sum_i \alpha$.
- Gröbnerbasis von I kann Polynome vom Grad 2^{2^d} enthalten.
- D.h. BUCHBERGER besitzt doppelt exponentielle Laufzeit.
- Probleme in der Praxis können aber oft effizient gelöst werden.
- grevlex-Ordnung erzeugt meist Polynome minimalen Grads.

BUCHBERGER versus GAUSS-ELIMINATION

Bsp: $I = \langle 3w - 6x - 2y, 2w - 4x + 4z, w - 2x - y - z \rangle \subseteq \mathbb{R}[w, x, y, z]$

- Wir stellen I in Matrixform dar.
$$\begin{pmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \\ 1 & -2 & -1 & -1 \end{pmatrix}$$
- Die normierte Stufenform davon ist
$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$
- Liefert eine minimale Gröbnerbasis $G = \{w - 2x - y - z, y + 3z\}$.
- Wir stellen sicher, dass führende Einsen in ihrer Spalte der einzige Nicht-Null Eintrag sind.
$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$
- Liefert die reduzierte Gröbnerbasis $G' = \{w - 2x + 2z, y + 3z\}$.
- Die Gauß-Elimination ist ein Spezialfall von BUCHBERGER.
- G' erlaubt einfaches Lösen des Gleichungssystems.

Lösen polynomieller Gleichungssysteme

Bsp:

- Wir suchen alle Lösungen in $\mathbb{C}$ des Gleichungssystems
$$\left| \begin{array}{rcl} x^2 + y^2 + z^2 & = & 1 \\ x^2 + z^2 & = & y \\ x & = & z \end{array} \right|.$$
- Sei $I = \langle x^2 + y^2 + z^2 - 1, x^2 - y + z^2, x - z \rangle$.
- Wir wollen $\mathbf{V}(I)$ bestimmen.
- BUCHBERGER liefert die reduzierte lex-Gröbnerbasis
$$G = \{x - z, y - 2z^2, z^4 + \tfrac{1}{2}z^2 - \tfrac{1}{4}\}.$$
- Offenbar eliminiert die lex-Ordnung x in g_2 und x, y in g_3.
- Der Generator g_3 hängt nur von z ab und liefert
$$z = \pm\tfrac{1}{2}\sqrt{\pm\sqrt{5} - 1}.$$
- Rücksubstitution von z in g_1, g_2 führt zu Lösungen in x und y.
- Damit erhalten wir alle Lösungen unseres Gleichungssystems.

Eliminationsideal

Definition Eliminationsideal

Sei $I = \langle g_1, \ldots, g_m \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Das *$\ell$-te Eliminationsideal I_ℓ* ist

$$I_\ell = I \cap \mathbb{F}[x_{\ell+1}, \ldots, x_n].$$

Anmerkung:

- In I_ℓ sind die Variablen $x_1, \ldots, x_\ell$ eliminiert.
- D.h. zum sukzessiven Lösen polynomieller Gleichungssysteme müssen wir Basen für I_ℓ für $\ell = 1, \ldots, n$ berechnen.

Eliminationstheorem

Satz Eliminationstheorem

Sei G eine lex-Gröbnerbasis für $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Dann ist

$$G_\ell = G \cap \mathbb{F}[x_{l+1}, \ldots, x_n] \text{ für } \ell = 0, \ldots, n$$

eine Gröbnerbasis des ℓ-ten Eliminationsideals I_ℓ.

Beweis:

- $\langle LT(G_\ell)\rangle \subseteq \langle LT(I_\ell)\rangle$: Nach Konstruktion gilt $G_\ell \subseteq I_\ell$. Daraus folgt
$$\langle LT(G_\ell)\rangle \subseteq \langle LT(I_\ell)\rangle.$$
- $\langle LT(I_\ell)\rangle \subseteq \langle LT(G_\ell)\rangle$: Sei $f \in I_\ell \subseteq \mathbb{F}[x_{\ell+1}, \ldots, x_\ell]$.
- zu zeigen: $LT(f)$ wird von einem der $LT(g)$ mit $g \in G_\ell$ geteilt.
- Da $f \in I$, wird $LT(f)$ von einem der $LT(g)$ mit $g \in G$ geteilt.
- Damit ist $LT(g) \in \mathbb{F}[x_{\ell+1}, \ldots, x_n]$. Da aber $x_1 > \ldots > x_{\ell+1}$, folgt
$$g \in \mathbb{F}[x_{\ell+1}, \ldots, x_n].$$
- D.h. insgesamt gilt $g \in G \cap \mathbb{F}[x_{\ell+1}, \ldots, x_n] = G_\ell$.

Erweitern partieller Lösungen

Bsp: Sei $I = \langle xy - 1, xz - 1 \rangle \subseteq \mathbb{C}[x, y, z]$.

- Das Ideal I besitzt Gröbnerbasis $G = \{xy - 1, xz - 1, y - z\}$.
- $G_1 = G \cap \mathbb{C}[y, z] = y - z$ und $G_2 = G \cap \mathbb{C}[z] = \emptyset$, d.h. $I_2 = \{0\}$.
- Damit ist jedes $z \in \mathbb{C}$ eine partielle Lösung.
- Wegen $y = z$ ist jedes $(y, z) = (c, c) \in \mathbb{C}^2$ eine partielle Lösung.
- Da $x = \frac{1}{y} = \frac{1}{z}$ lässt sich diese Lösung zu $(\frac{1}{c}, c, c) \in \mathbb{C}^3$ erweitern.
- Allerdings sind diese nur für $c = 0$ eine Lösung.
- D.h. alle Lösungen $(y, z) = (c, c), c \neq 0$ sind erweiterbar.

Erweiterungssatz

Satz Erweiterungssatz

Sei $I = \langle f_1, \ldots, f_m \rangle \subseteq \mathbb{C}[x_1, \ldots, x_n]$. Für $i = 1, \ldots, m$ sei

$$f_i = h_i(x_2, \ldots, x_n) x_1^{N_i} - (\text{Terme mit } \mathrm{grad}(x_1) \leq N_i) \text{ für } h_i \neq 0,\ N_i \in \mathbb{N}_0.$$

Sei $(a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Es existiert $a_1 \in \mathbb{C}$ mit $(a_1, \ldots, a_n) \in \mathbf{V}(I)$ falls

$$(a_1, \ldots, a_n) \notin \mathbf{V}(h_1, \ldots, h_m).$$

(ohne Beweis)

Beispiel: $I = \langle xy - 1, xz - 1 \rangle \subseteq \mathbb{C}[x, y, z]$

- $I_2 = \{0\}$ ist das erste Eliminationsideal von $I_1 = \langle y - z \rangle \subseteq \mathbb{C}[y, z]$.
- Es gilt $y - z = h(z) \cdot y - z$ mit $h(z) = 1$. D.h. $h(z) \neq 0$ für alle z.
- Damit lassen sich alle Lösungen $z = c$ zu $(y, z) = (c, c)$ erweitern.
- Es gilt $f_1 = \underbrace{y}_{h_1(y,z)} \cdot x - 1$ und $f_2 = \underbrace{z}_{h_2(y,z)} \cdot x - 1$.
- Ferner ist $\mathbf{V}(h_1(y, z), h_2(y, z)) = \{(0, 0)\}$.
- D.h. alle Lösungen außer $(y, z) = (0, 0)$ sind erweiterbar.

Hilberts schwacher Nullstellensatz

Satz Hilberts schwacher Nullstellensatz

Sei $I \in \mathbb{C}[x_1, \ldots, x_n]$ mit $\mathbf{V}(I) = \emptyset$. Dann gilt $I = \mathbb{C}[x_1, \ldots, x_n]$.

(ohne Beweis)

Satz Lösbarkeit von Gleichungssystemen in $\mathbb{C}$

Sei $I = \langle f_1, \ldots, f_m \rangle \in \mathbb{C}[x_1, \ldots, x_n]$, G reduzierte Gröbnerbasis von I. Falls $G \neq \{1\}$, dann besitzt das System $f_1 = \ldots = f_m = 0$ eine Lösung.

Beweis:

- Es gilt $\mathbb{C}[x_1, \ldots, x_n] = \langle 1 \rangle$. $\{1\}$ ist eine reduzierte Gröbnerbasis.
- D.h. falls $G \neq \{1\}$, dann gilt $I \neq \mathbb{C}[x_1, \ldots, x_n]$.
- Daraus folgt $\mathbf{V}(I) \neq \emptyset$ mit schwachem Nullstellensatz.
- Damit besitzt das Gleichungssystem mindestens eine Lösung.