Beispiel Gröbnerbasen-Berechnung

Bsp:

- Seien $f_1 = x^2y + xy$, $f_2 = xy^2 + 1 \in \mathbb{R}[x, y]$ in grlex-Ordnung.
- $S(f_1, f_2) = yf_1 - xf_2 = xy^2 - x$. Division liefert
$$S(f_1, f_2) = 1 \cdot f_2 - x - 1.$$
- Wir fügen $f_3 = -x - 1$ zur Basis hinzu.
- $S(f_1, f_3) = f_1 + xyf_3 = 0$ und $S(f_2, f_3) = f_2 + y^2 f_3 = -y^2 + 1$.
- Wir fügen $f_4 = -y^2 + 1$ zur Basis hinzu.
- $S(f_1, f_4)$, $S(f_2, f_4)$, $S(f_3, f_4)$ verschwinden bei Basisdivision.
- D.h. $\{x^2y + xy, xy^2 + 1, -x - 1, -y^2 + 1\}$ ist Gröbnerbasis für I.

Notation für Ideale und Division

Sei $G = \{g_1, \ldots, g_m\}$ und $f \in \mathbb{F}[x_1, \ldots, x_n]$. Wir schreiben vereinfacht

$$\langle G \rangle = \langle g_1, \ldots, g_m \rangle \text{ und } \langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_m) \rangle.$$

Wir notieren mit $\overline{f}^G$ den Rest der Division von f durch G.

Korrektheit von BUCHBERGER

Satz

Algorithmus BUCHBERGER terminiert nach endlich vielen Schritten mit einer Gröbnerbasis.

Beweis:

Korrektheit: Als Invariante gilt, dass G das Ideal I generiert.

- Sei $S(g_i, g_j) = \sum_i a_i g_i + r$. Da $S(g_i, g_j), \sum_i a_i g_i \in I$ ist auch $r \in I$.
- Wir fügen also nur Element aus I zu G hinzu.
- Buchberger Kriterium: G ist bei Terminierung eine Gröbnerbasis.

Terminierung: Sei $G = \{g_1, \ldots, g_m\}$.

- Sei $G' = G \cup \{r\}$ in Schritt 2.1. Da r in G aufgenommen wird, wird $LT(r)$ von keinem der $LT(g_i)$ geteilt. D.h.
  $\langle LT(G)\rangle \subset \langle LT(G')\rangle$, da $G \subset G'$ und $LT(r) \in \langle LT(G')\rangle \setminus \langle LT(G)\rangle$.
- Damit entsteht in Schritt 2.1 eine aufsteigende Kette von Idealen
  $$\langle LT(G)\rangle \subset \langle LT(G')\rangle \subset \langle LT(G'')\rangle \subset \ldots.$$
- Nach ACC stabilisiert die Kette nach endlichen vielen Schritten.

Minimale Gröbnerbasis

Beobachtung: Gröbnerbasen enthalten oft unnötige Generatoren.

Satz Elimination von Generatoren

Sei G eine Gröbnerbasis für I. Sei $g \in G$ mit $LT(g) \in \langle LT(G \setminus \{g\})\rangle$. Dann ist $G \setminus \{g\}$ eine Gröbnerbasis von I.

Beweis:

- Da G eine Gröbnerbasis ist, gilt $\langle LT(G)\rangle = \langle LT(I)\rangle$.
- Wegen $LT(g) \in \langle LT(G \setminus \{g\})\rangle$ folgt
$$\langle LT(G \setminus \{g\})\rangle = \langle LT(G)\rangle = \langle LT(I)\rangle.$$
- Damit ist auch $G \setminus \{g\}$ eine Gröbnerbasis.

Definition Minimale Gröbnerbasis

Wir nennen eine Gröbnerbasis G *minimal*, falls für alle $g \in G$ gilt:

1. $LT(g) \notin \langle LT(G \setminus \{g\})\rangle$.
2. $LC(g) = 1$.

Minimierung einer Gröbnerbasis

Algorithmus MINIMIERE GRÖBNER

EINGABE: Gröbnerbasis B

1. Für alle $g \in G$: Falls $LT(g) \in \langle LT(G \setminus \{g\})\rangle$, setze $G := G \setminus \{g\}$.
2. Für alle $g \in G$: Setze $g := \frac{g}{LC(g)}$.

AUSGABE: minimale Gröbnerbasis

Beispiel: Gröbnerbasis $\{x^2y + xy, xy^2 + 1, -x - 1, -y^2 + 1\}$ (grlex)

- Wir können g_1 eliminieren, da $LT(g_1) = x^2y = -xy \cdot LT(g_3)$.
- Ferner können wir g_2 eliminieren, da $LT(g_2) = xy^2 = -x \cdot LT(g_4)$.
- Damit ist $\{x + 1, y^2 - 1\}$ eine minimale Gröbnerbasis.
- Leider sind minimale Gröbnerbasen nicht eindeutig.
- Die folgenden Basen sind ebenfalls minimal für die grlex-Ordnung

$$\{x + 1, y^2 + a(x + 1) - 1\} \text{ mit } a \in \mathbb{Z}.$$

Reduzierte Gröbnerbasis

Definition reduzierte Gröbnerbasis

Wir nennen eine Gröbnerbasis G *reduziert*, falls für alle $g \in G$ gilt:

1. Kein Monom von g liegt in $\langle LT(G \setminus \{g\})\rangle$.
2. $LC(g) = 1$.

Algorithmus REDUZIERE GRÖBNER

EINGABE: minimale Gröbnerbasis G

1. Für alle $g \in G$
   1. Setze $g' := \overline{g}^{G\setminus\{g\}}$.
   2. Setze $G := G \setminus \{g\} \cup \{g'\}$.

AUSGABE: reduzierte Gröbnerbasis G

Reduzierte Gröbnerbasis

Satz Korrektheit REDUZIERE GRÖBNER

Algorithmus REDUZIERE GRÖBNER berechnet eine reduzierte Gröbnerbasis.

Beweis:

- Wir bezeichnen ein Polynom $g \in G$ als reduziert, falls kein Monom von g in $\langle LT(G \setminus \{g\})\rangle$ liegt (Eigenschaft 1).
- Ein reduziertes g bleibt reduziert, sofern sich die führenden Terme von G nicht ändern.
- In Schritt 1.1 gilt $LT(g') = LT(g)$, da aufgrund von G's Minimalität $LT(g)$ von keinem der führenden Terme in $LT(G \setminus \{g\})$ geteilt wird.
- D.h. führendeTerme bleiben unverändert und $\langle LT(G')\rangle = \langle LT(G)\rangle$.
- Damit ist G' in Schritt 1.2 ebenfalls eine minimale Gröbnerbasis.
- Da wir alle $g \in G$ reduzieren, ist G bei Terminierung reduziert.

Eindeutigkeit reduzierter Gröbnerbasen

Satz Existenz und Eindeutigkeit reduzierter Gröbnerbasen

Jedes Ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ besitzt für eine feste Monomordnung 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 in $g - g'$ der Term $LT(g)$ eliminiert.
- Da G, G' reduziert sind, wird keiner der sonstigen 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 $\alpha = (\alpha_1, \ldots, \alpha_n)$.
- Sei der Grad definiert als $d = \sum_{i=1}^{n} \alpha_i$.
- 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.