Signaturbasierte Gröbner Basen Algorithmen

Christian Eder

Technische Universität Kaiserslautern

13. April 2012

Vereinbarungen

- $R = K[x_1, \dots, x_n]$, K Körper, $<$ Wohlordnung auf $\mathrm{Mon}(x_1, \dots, x_n)$

Vereinbarungen

- $R = K[x_1, \ldots, x_n]$, K Körper, $<$ Wohlordnung auf $\mathrm{Mon}(x_1, \ldots, x_n)$
- Durch $<$ ist ein Element $f \in R$ eindeutig bestimmt
  $\Rightarrow$ Es ergibt Sinn von $\mathrm{lc}(f)$, $\mathrm{lm}(f)$ und $\mathrm{lt}(f)$ zu sprechen.

Vereinbarungen

- $R = K[x_1, \ldots, x_n]$, K Körper, $<$ Wohlordnung auf $\mathrm{Mon}(x_1, \ldots, x_n)$
- Durch $<$ ist ein Element $f \in R$ eindeutig bestimmt
  $\Rightarrow$ Es ergibt Sinn von $\mathrm{lc}(f)$, $\mathrm{lm}(f)$ und $\mathrm{lt}(f)$ zu sprechen.
- Ein Ideal I in R ist eine additive Untergruppe von R, so dass für $f \in I$, $g \in R$ gilt: $fg \in I$.

- **Eine kleine Einführung in die Theorie der Gröbner Basen**
  - Grundsätzliches zu Gröbner Basen
  - Berechnung von Gröbner Basen
  - Das Problem der Nullreduktion
- **Signaturbasierter Ansatz**
  - Die grundlegende Idee
  - Signaturbasierte Berechnungen von Gröbner Basen
  - Signaturbasierte Kriterien
- **Implementierungen & Ausblick**
  - Effiziente Varianten
  - Zeiten
  - Ausblick

Definition

$G = \{g_1, \ldots, g_r\}$ ist eine **Gröbner Basis** von $I = \langle f_1, \ldots, f_m \rangle$ genau dann, wenn

1. $G \subset I$ und
2. $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_r) \rangle = \langle \mathrm{lm}(f) \mid f \in I \rangle$.

Definition

$G = \{g_1, \ldots, g_r\}$ ist eine **Gröbner Basis** von $I = \langle f_1, \ldots, f_m \rangle$ genau dann, wenn

1. $G \subset I$ und
2. $\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_r) \rangle = \langle \mathrm{lm}(f) \mid f \in I \rangle$.

Satz (Buchbergers Kriterium)

Die folgenden Aussagen sind äquivalent:

1. *G ist eine Gröbner Basis von $\langle G \rangle$.*
2. *Für alle $f, g \in G$ gilt, dass* $\mathrm{spol}(f, g) \xrightarrow{G} 0$, *wobei*

$$\mathrm{spol}(f,g) = \mathrm{lc}(g)\frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(f)} f - \mathrm{lc}(f)\frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(g)} g.$$

Beispiel

Sei $I = \langle g_1, g_2 \rangle \lhd \mathbb{Q}[x, y, z]$ mit $g_1 = xy - z^2$, $g_2 = y^2 - z^2$; $<$ graduierte, umgekehrt-lexikographische Ordnung.
Betrachten wir

$$\begin{aligned} \mathrm{spol}(g_2, g_1) &= xg_2 - yg_1 \\ &= \mathbf{xy^2} - xz^2 - \mathbf{xy^2} + yz^2 \\ &= -xz^2 + yz^2, \end{aligned}$$

so erhalten wir als Resultat

$$g_3 = xz^2 - yz^2.$$

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis G **von** I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{f_i\}$ **für alle** $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$

Eingabe: Ideal $I = \langle f_1, \dots, f_m \rangle$
Ausgabe: Gröbner Basis G **von** I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{f_i\}$ **für alle** $i \in \{1, \dots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. **Solange** $P \neq \emptyset$
   (a) **Wähle** $(f, g) \in P$, $P \leftarrow P \setminus \{(f, g)\}$
   (b) $h \leftarrow \mathrm{spol}(f, g)$

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis G **von** I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{f_i\}$ **für alle** $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. **Solange** $P \neq \emptyset$
   (a) **Wähle** $(f, g) \in P$**,** $P \leftarrow P \setminus \{(f, g)\}$
   (b) $h \leftarrow \mathrm{spol}(f, g)$
      (i) **Falls** $h \xrightarrow{G} 0$

Eingabe: Ideal $I = \langle f_1, \dots, f_m \rangle$
Ausgabe: Gröbner Basis G **von** I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{f_i\}$ **für alle** $i \in \{1, \dots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. **Solange** $P \neq \emptyset$
   (a) **Wähle** $(f, g) \in P$, $P \leftarrow P \setminus \{(f, g)\}$
   (b) $h \leftarrow \mathrm{spol}(f, g)$
      (i) **Falls** $h \xrightarrow{G} 0$
      (ii) **Falls** $h \xrightarrow{G} r \neq 0$

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis G **von** I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{f_i\}$ **für alle** $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. **Solange** $P \neq \emptyset$
   (a) **Wähle** $(f, g) \in P$, $P \leftarrow P \setminus \{(f, g)\}$
   (b) $h \leftarrow \mathrm{spol}(f, g)$
      (i) **Falls** $h \xrightarrow{G} 0$
      (ii) **Falls** $h \xrightarrow{G} r \neq 0$
      $P \leftarrow P \cup \{(r, g) \mid g \in G\}$
      $G \leftarrow G \cup \{r\}$
5. **Gebe** G **aus.**

Eingabe: Ideal $I = \langle f_1, \dots, f_m \rangle$
Ausgabe: Gröbner Basis G **von** I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{f_i\}$ **für alle** $i \in \{1, \dots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. **Solange** $P \neq \emptyset$
   (a) **Wähle** $(f, g) \in P$**,** $P \leftarrow P \setminus \{(f, g)\}$
   (b) $h \leftarrow \mathrm{spol}(f, g)$
      (i) **Falls** $h \xrightarrow{G} 0 \Rightarrow$ **keine neue Information**
      (ii) **Falls** $h \xrightarrow{G} r \neq 0 \Rightarrow$ **neue Information**
      $P \leftarrow P \cup \{(r, g) \mid g \in G\}$
      $G \leftarrow G \cup \{r\}$
5. **Gebe** G **aus.**

Nullreduktion in unserem Beispiel

Beispiel

Gegeben waren die Erzeuger $\mathbf{g_1 = xy - z^2}$, $\mathbf{g_2 = y^2 - z^2}$ von I. Wir haben spol(g_2, g_1) bzgl. G reduziert und das resultierende Element $\mathbf{g_3 = xz^2 - yz^2}$ wird zu G hinzugefügt.

Beispiel

Gegeben waren die Erzeuger $\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}$, $\mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$ von I.
Wir haben $\text{spol}(g_2, g_1)$ bzgl. G reduziert und das resultierende Element $\mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}$ wird zu G hinzugefügt.
Nun geht es weiter:

$$\text{spol}(g_3, g_1) = \mathbf{xyz^2} - y^2z^2 - \mathbf{xyz^2} + z^4 = -y^2z^2 + z^4.$$

Beispiel

Gegeben waren die Erzeuger $\mathbf{g_1 = xy - z^2}$, $\mathbf{g_2 = y^2 - z^2}$ von I. Wir haben $\mathrm{spol}(g_2, g_1)$ bzgl. G reduziert und das resultierende Element $\mathbf{g_3 = xz^2 - yz^2}$ wird zu G hinzugefügt.
Nun geht es weiter:

$$\mathrm{spol}(g_3, g_1) = \mathbf{xyz^2} - y^2z^2 - \mathbf{xyz^2} + z^4 = -y^2z^2 + z^4.$$

Wir können weiter reduzieren mit $z^2 g_2$:

$$-y^2z^2 + z^4 + y^2z^2 - z^4 = 0.$$

Nullreduktion in unserem Beispiel

Beispiel

Gegeben waren die Erzeuger $\mathbf{g_1 = xy - z^2}$, $\mathbf{g_2 = y^2 - z^2}$ von I.
Wir haben $\text{spol}(g_2, g_1)$ bzgl. G reduziert und das resultierende Element $\mathbf{g_3 = xz^2 - yz^2}$ wird zu G hinzugefügt.
Nun geht es weiter:

$$\text{spol}(g_3, g_1) = \mathbf{xyz^2} - y^2z^2 - \mathbf{xyz^2} + z^4 = -y^2z^2 + z^4.$$

Wir können weiter reduzieren mit $z^2 g_2$:

$$-y^2z^2 + z^4 + y^2z^2 - z^4 = 0.$$

$\Rightarrow$ **Wie können wir Nullreduktion vorhersagen?**

- **Eine kleine Einführung in die Theorie der Gröbner Basen**
  - Grundsätzliches zu Gröbner Basen
  - Berechnung von Gröbner Basen
  - Das Problem der Nullreduktion
- **Signaturbasierter Ansatz**
  - Die grundlegende Idee
  - Signaturbasierte Berechnungen von Gröbner Basen
  - Signaturbasierte Kriterien
- **Implementierungen & Ausblick**
  - Effiziente Varianten
  - Zeiten
  - Ausblick

Sei $I = \langle f_1, \ldots, f_m \rangle$.
Idee: Gib jedem Polynom $f \in I$ etwas mehr Struktur:

Sei $I = \langle f_1, \ldots, f_m \rangle$.
Idee: Gib jedem Polynom $f \in I$ etwas mehr Struktur:

1. Es sei R^m erzeugt von $e_1, \ldots, e_m$, $\prec$ eine Wohlordnung auf den Monomen in R^m und $\pi : R^m \to R$, so dass

$$\pi(e_i) = f_i \text{ für alle } i.$$

Sei $I = \langle f_1, \ldots, f_m \rangle$.
Idee: Gib jedem Polynom $f \in I$ etwas mehr Struktur:

1. Es sei R^m erzeugt von $e_1, \ldots, e_m$, $\prec$ eine Wohlordnung auf den Monomen in R^m und $\pi : R^m \to R$, so dass
$$\pi(e_i) = f_i \text{ für alle } i.$$
2. Jedes Polynom $p \in I$ kann beschrieben werden durch ein
$$s = \sum_{i=1}^{m} h_i e_i \in R^m \text{ mit } p = \pi(s).$$

Sei $I = \langle f_1, \ldots, f_m \rangle$.
Idee: Gib jedem Polynom $f \in I$ etwas mehr Struktur:

1. Es sei R^m erzeugt von $e_1, \ldots, e_m$, $\prec$ eine Wohlordnung auf den Monomen in R^m und $\pi : R^m \to R$, so dass

$$\pi(e_i) = f_i \text{ für alle } i.$$

2. Jedes Polynom $p \in I$ kann beschrieben werden durch ein

$$s = \sum_{i=1}^{m} h_i e_i \in R^m \text{ mit } p = \pi(s).$$

3. **Eine Signatur** von p ist gegeben durch

$$\mathrm{sig}(p) = \mathrm{lm}_{\prec}(s) \text{ mit } p = \pi(s).$$

Signaturen von Polynomen

Sei $I = \langle f_1, \ldots, f_m \rangle$.

Idee: Gib jedem Polynom $f \in I$ etwas mehr Struktur:

1. Es sei R^m erzeugt von $e_1, \ldots, e_m$, $\prec$ eine Wohlordnung auf den Monomen in R^m und $\pi : R^m \to R$, so dass
$$\pi(e_i) = f_i \text{ für alle } i.$$
2. Jedes Polynom $p \in I$ kann beschrieben werden durch ein
$$s = \sum_{i=1}^{m} h_i e_i \in R^m \text{ mit } p = \pi(s).$$
3. **Eine Signatur** von p ist gegeben durch
$$\mathrm{sig}(p) = \mathrm{lm}_{\prec}(s) \text{ mit } p = \pi(s).$$
4. **Die minimale Signatur** von p existiert durch $\prec$.

Unser Beispiel – nun mit Signaturen und $\prec_{\text{pot}}$

Wir hatten bislang folgendes:

$$
\begin{aligned}
g_1 &= xy - z^2, \\
g_2 &= y^2 - z^2, \\
g_3 &= \operatorname{spol}(g_2, g_1) = xg_2 - yg_1 \\
\Rightarrow \operatorname{sig}(g_3) &= x \operatorname{sig}(g_2) = xe_2.
\end{aligned}
$$

Unser Beispiel – nun mit Signaturen und $\prec_{\text{pot}}$

Wir hatten bislang folgendes:

$$\begin{aligned} g_1 &= xy - z^2, \\ g_2 &= y^2 - z^2, \\ g_3 &= \operatorname{spol}(g_2, g_1) = xg_2 - yg_1 \\ \Rightarrow \operatorname{sig}(g_3) &= x \operatorname{sig}(g_2) = xe_2. \end{aligned}$$

Weiter mit $\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$:

$$\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = y \operatorname{sig}(g_3) = xye_2.$$

Unser Beispiel – nun mit Signaturen und $\prec_{\text{pot}}$

Wir hatten bislang folgendes:

$$\begin{aligned} g_1 &= xy - z^2, \\ g_2 &= y^2 - z^2, \\ g_3 &= \operatorname{spol}(g_2, g_1) = xg_2 - yg_1 \\ \Rightarrow \operatorname{sig}(g_3) &= x \operatorname{sig}(g_2) = xe_2. \end{aligned}$$

Weiter mit $\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$:

$$\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = y \operatorname{sig}(g_3) = xye_2.$$

Beachte: $\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = xy\,e_2$ und $\operatorname{lm}(g_1) = xy$.

Unser Beispiel – nun mit Signaturen und $\prec_{\text{pot}}$

Wir hatten bislang folgendes:

$$\begin{aligned} g_1 &= xy - z^2, \\ g_2 &= y^2 - z^2, \\ g_3 &= \operatorname{spol}(g_2, g_1) = xg_2 - yg_1 \\ \Rightarrow \operatorname{sig}(g_3) &= x \operatorname{sig}(g_2) = xe_2. \end{aligned}$$

Weiter mit $\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$:

$$\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = y \operatorname{sig}(g_3) = xye_2.$$

Beachte: $\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = xy\, e_2$ und $\operatorname{lm}(g_1) = xy$.

$\Rightarrow$ **Wir wissen, dass $\operatorname{spol}(g_3, g_1)$ zu Null reduzieren wird.**

Woher wissen wir das?

Die generelle Idee ist es, die s-Polynome auf Minimalität ihrer zugehörigen Signaturen zu untersuchen.

Woher wissen wir das?

Die generelle Idee ist es, die s-Polynome auf Minimalität ihrer zugehörigen Signaturen zu untersuchen.

Falls $\text{sig}\big(\text{spol}(p, q)\big)$ nicht minimal für $\text{spol}(p, q)$ ist
$\Rightarrow$ $\text{spol}(p, q)$ wird nicht reduziert.

Woher wissen wir das?

Die generelle Idee ist es, die s-Polynome auf Minimalität ihrer zugehörigen Signaturen zu untersuchen.

Falls $\operatorname{sig}\big(\operatorname{spol}(p,q)\big)$ nicht minimal für $\operatorname{spol}(p,q)$ ist
$\Rightarrow \operatorname{spol}(p,q)$ wird nicht reduziert.

Unser Ziel

Versuche so gut es geht zu prüfen, ob die Signatur des s-Polynoms der minimal möglichen entspricht und handele entsprechend.

Woher wissen wir das?

Die generelle Idee ist es, die s-Polynome auf Minimalität ihrer zugehörigen Signaturen zu untersuchen.

Falls $\operatorname{sig}\big(\operatorname{spol}(p,q)\big)$ nicht minimal für $\operatorname{spol}(p,q)$ ist
$\Rightarrow \operatorname{spol}(p,q)$ wird nicht reduziert.

Unser Ziel

Versuche so gut es geht zu prüfen, ob die Signatur des s-Polynoms der minimal möglichen entspricht und handele entsprechend.

Unsere Aufgabe

Wir müssen auf die Korrektheit der Signaturen achten.

Signaturbasierte Berechnungen von Gröbner Basen

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis $\mathrm{poly}(G)$ von I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ für alle $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$

Signaturbasierte Berechnungen von Gröbner Basen

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis $\text{poly}(G)$ von I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ für alle $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. Solange $P \neq \emptyset$
   (a) Wähle $(f, g) \in P$ mit $\text{sig}(\text{spol}(f, g))$ minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) Falls $\text{sig}(\text{spol}(f, g))$ minimal für $\text{spol}(f, g)$:

Signaturbasierte Berechnungen von Gröbner Basen

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis poly(G) von I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ für alle $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. Solange $P \neq \emptyset$
   (a) Wähle $(f, g) \in P$ mit sig (spol(f, g)) minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) Falls sig (spol(f, g)) minimal für spol(f, g):
      (i) $h \leftarrow \text{spol}(f, g)$
      (ii) Falls poly$(h) \xrightarrow{G} 0$

Signaturbasierte Berechnungen von Gröbner Basen

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis $\text{poly}(G)$ von I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ für alle $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. Solange $P \neq \emptyset$
   (a) Wähle $(f, g) \in P$ mit $\text{sig}\,(\text{spol}(f, g))$ minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) Falls $\text{sig}\,(\text{spol}(f, g))$ minimal für $\text{spol}(f, g)$:
      (i) $h \leftarrow \text{spol}(f, g)$
      (ii) Falls $\text{poly}(h) \xrightarrow{G} 0$
      (iii) Falls $\text{poly}(h) \xrightarrow{G} \text{poly}(r) \neq 0$

      $P \leftarrow P \cup \{(r, g) \mid g \in G\}$
      $G \leftarrow G \cup \{r\}$
5. Gebe $\text{poly}(G)$ aus.

Signaturbasierte Berechnungen von Gröbner Basen

Eingabe: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Ausgabe: Gröbner Basis $\mathrm{poly}(G)$ von I

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ für alle $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. Solange $P \neq \emptyset$
   (a) Wähle $(f, g) \in P$ mit $\mathrm{sig}\,(\mathrm{spol}(f, g))$ minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) Falls $\mathrm{sig}\,(\mathrm{spol}(f, g))$ minimal für $\mathrm{spol}(f, g)$:
      (i) $h \leftarrow \mathrm{spol}(f, g)$
      (ii) Falls $\mathrm{poly}(h) \xrightarrow{G} 0 \Leftarrow$ **signaturerhaltend**
      (iii) Falls $\mathrm{poly}(h) \xrightarrow{G} \mathrm{poly}(r) \neq 0 \Leftarrow$ **signaturerhaltend**
      & $\nexists g \in G$ so dass $m\,\mathrm{sig}(g) = \mathrm{sig}(r)$ und
      $m\,\mathrm{lm}(\mathrm{poly}(g)) = \mathrm{lm}(\mathrm{poly}(r))$
      $P \leftarrow P \cup \{(r, g) \mid g \in G\}$
      $G \leftarrow G \cup \{r\}$
5. Gebe $\mathrm{poly}(G)$ aus.

Signaturerhaltende Reduktionen

Seien p und q in R gegeben, so dass $m\,\mathrm{lm}(q) = \mathrm{lm}(p)$, $c = \frac{\mathrm{lc}(p)}{\mathrm{lc}(q)}$.
Betrachte

$$p - cmq.$$

Seien p und q in R gegeben, so dass $m \operatorname{lm}(q) = \operatorname{lm}(p)$, $c = \frac{\operatorname{lc}(p)}{\operatorname{lc}(q)}$.
Betrachte

$$p - cmq.$$

signaturerhaltend: $\operatorname{sig}(p - cmq) \quad = \quad \operatorname{sig}(p)$

Seien p und q in R gegeben, so dass $m\,\mathrm{lm}(q) = \mathrm{lm}(p)$, $c = \frac{\mathrm{lc}(p)}{\mathrm{lc}(q)}$.
Betrachte

$$p - cmq.$$

$$\begin{array}{lrcl} \textbf{signaturerhaltend:} & \mathrm{sig}(p - cmq) & = & \mathrm{sig}(p) \\ \textbf{signaturerhöhend:} & \mathrm{sig}(p - cmq) & = & m\,\mathrm{sig}(q) \end{array}$$

Signaturerhaltende Reduktionen

Seien p und q in R gegeben, so dass $m\,\mathrm{lm}(q) = \mathrm{lm}(p)$, $c = \frac{\mathrm{lc}(p)}{\mathrm{lc}(q)}$. Betrachte

$$p - cmq.$$

$$\begin{array}{rrcl}
\textbf{signaturerhaltend:} & \mathrm{sig}(p - cmq) & = & \mathrm{sig}(p) \\[1em]
\textbf{signaturerhöhend:} & \mathrm{sig}(p - cmq) & = & m\,\mathrm{sig}(q) \\
\textbf{signaturerniedrigend:} & \mathrm{sig}(p - cmq) & \prec & \mathrm{sig}(p), m\,\mathrm{sig}(q)
\end{array}$$

Terminierung

- Falls $\operatorname{sig}(r) = m \operatorname{sig}(g)$ und $\operatorname{lm}(\operatorname{poly}(r)) = m \operatorname{lm}(\operatorname{poly}(g))$ wird r nicht zu G hinzugefügt.
- Jedes neue Element vergrößert $\langle (\operatorname{sig}(r), \operatorname{lm}(\operatorname{poly}(r))) \rangle$.

Funktioniert das?

Terminierung

- Falls $\operatorname{sig}(r) = m \operatorname{sig}(g)$ und $\operatorname{lm}(\operatorname{poly}(r)) = m \operatorname{lm}(\operatorname{poly}(g))$ wird r nicht zu G hinzugefügt.
- Jedes neue Element vergrößert $\langle(\operatorname{sig}(r), \operatorname{lm}(\operatorname{poly}(r)))\rangle$.

Korrektheit

- „Alle möglichen“ s-Polynome werden betrachtet: signaturerhöhende Reduktion $\Rightarrow$ neues Paar im nächsten Schritt
- Alle Elemente ungleich Null werden hinzugefügt außer wenn $\operatorname{sig}(r) = m \operatorname{sig}(g)$ und $\operatorname{lm}(\operatorname{poly}(r)) = m \operatorname{lm}(\operatorname{poly}(g))$

Non-minimal signature (NM)

$\mathrm{sig}(h)$ nicht minimal für h? $\Rightarrow$ Lösche h.

Non-minimal signature (NM)

$\mathrm{sig}(h)$ nicht minimal für h? $\Rightarrow$ Lösche h.

Beweisidee

1. Es existiert eine Syzygie $s \in R^m$ mit $\mathrm{lm}(s) = \mathrm{sig}(h)$.
   $\Rightarrow$ Wir können h mit kleinerer Signatur darstellen.
2. Elemente werden bzgl. aufsteigender Signaturen gehandhabt.
   $\Rightarrow$ Die zu h gehörenden Reduktionen sind unnötig.

□

Non-minimal signature (NM)

$\operatorname{sig}(h)$ nicht minimal für h? $\Rightarrow$ Lösche h.

Beweisidee

1. Es existiert eine Syzygie $s \in R^m$ mit $\operatorname{Im}(s) = \operatorname{sig}(h)$.
   $\Rightarrow$ Wir können h mit kleinerer Signatur darstellen.
2. Elemente werden bzgl. aufsteigender Signaturen gehandhabt.
   $\Rightarrow$ Die zu h gehörenden Reduktionen sind unnötig.

$\square$

Nochmal unser Beispiel mit $\prec_{\text{pot}}$

$$\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = xye_2$$

$$\left.\begin{array}{l} g_1 = xy - z^2 \\ g_2 = y^2 - z^2 \end{array}\right\} \Rightarrow \operatorname{psyz}(g_2, g_1) = g_1 e_2 - g_2 e_1 = xye_2 + \ldots$$

Rewritable signature (RW)

$\mathrm{sig}(g) = \mathrm{sig}(h)$? $\Rightarrow$ Lösche entweder g oder h.

Rewritable signature (RW)

$\text{sig}(g) = \text{sig}(h)? \Rightarrow$ Lösche entweder g oder h.

Beweisidee

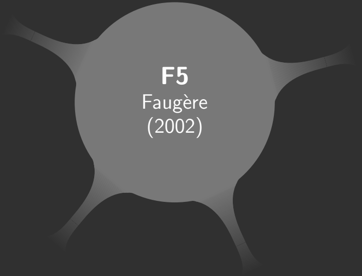
1. $\text{sig}(g - h) \prec \text{sig}(g), \text{sig}(h)$.
2. Elemente werden bzgl. aufsteigender Signaturen gehandhabt.
   $\Rightarrow$ Rechnungen bzgl. kleinerer Signaturen sind schon abgeschlossen.
   $\Rightarrow$ Wir können bspw. h darstellen durch

$$h = g + \text{ Elemente mit kleineren Signaturen.}$$

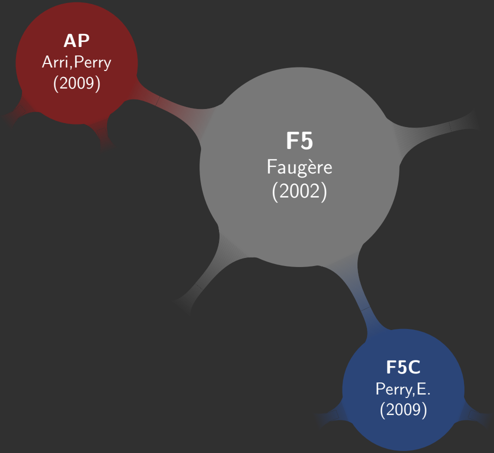
$\square$

- **Eine kleine Einführung in die Theorie der Gröbner Basen**
  - Grundsätzliches zu Gröbner Basen
  - Berechnung von Gröbner Basen
  - Das Problem der Nullreduktion
- **Signaturbasierter Ansatz**
  - Die grundlegende Idee
  - Signaturbasierte Berechnungen von Gröbner Basen
  - Signaturbasierte Kriterien
- **Implementierungen & Ausblick**
  - Effiziente Varianten
  - Zeiten
  - Ausblick

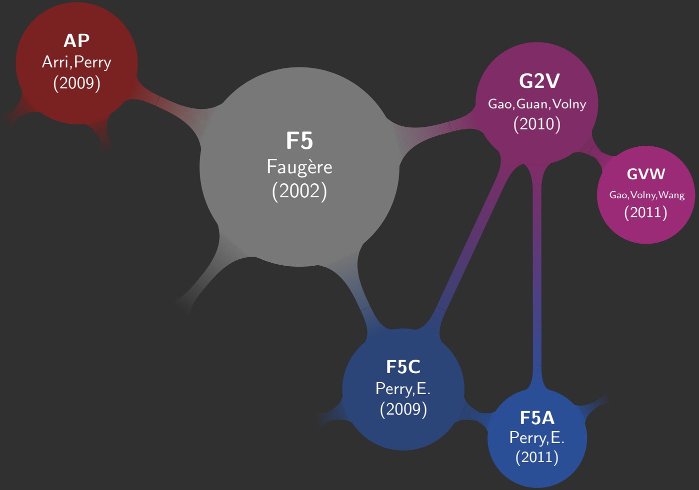
Effiziente Varianten



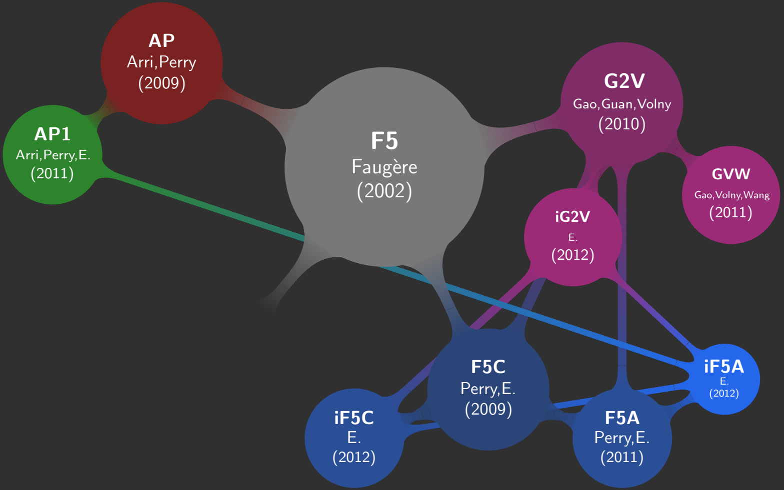
Effiziente Varianten



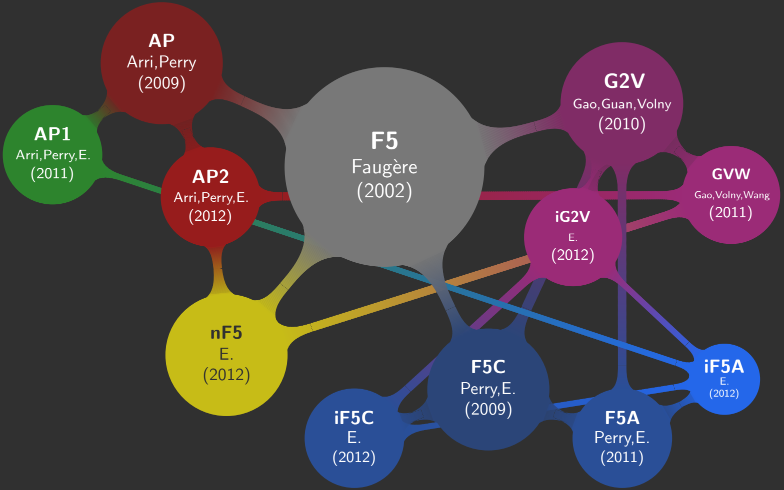
Effiziente Varianten



Effiziente Varianten

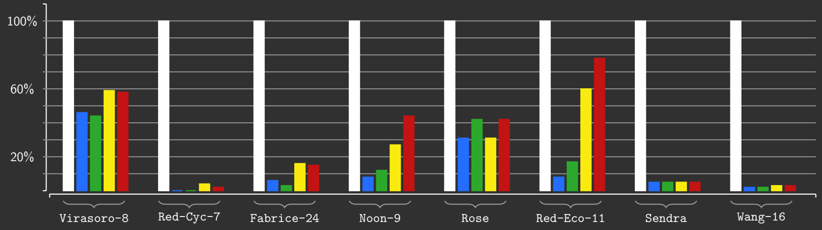


Effiziente Varianten

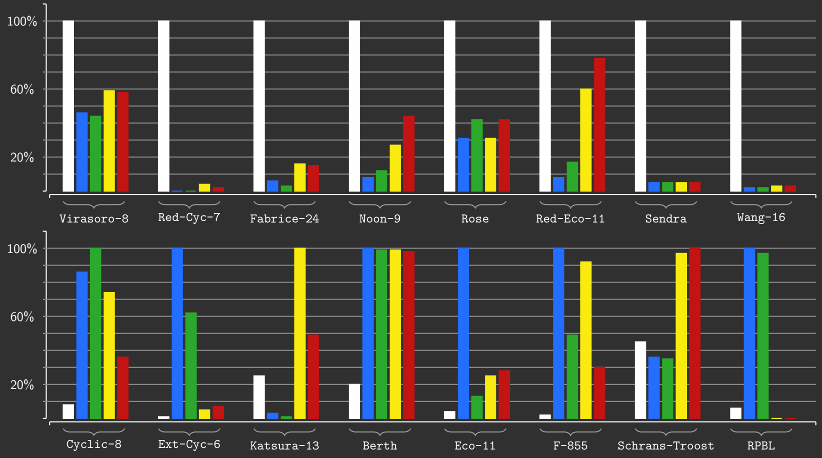


Effiziente Varianten

Zeiten


100%
60%
20%
Virasoro-8
Red-Cyc-7
Fabrice-24
Noon-9
Rose
Red-Eco-11
Sendra
Wang-16

Zeiten


100%
60%
20%
Virasoro-8
Red-Cyc-7
Fabrice-24
Noon-9
Rose
Red-Eco-11
Sendra
Wang-16
Cyclic-8
Ext-Cyc-6
Katsura-13
Berth
Eco-11
F-855
Schrans-Troost
RPBL

- **Heuristiken:**
  Ordnungen für Signaturen; Ordnung von Paaren, Reduzierern
- **F4:**
  Lineare Algebra zum Reduzieren
- **Parallelisierung:**
  modulare Methoden, paralleles Testen der Kriterien
- **Berechnung von Syzygien:**
  Implementierung
- **Verallgemeinerung der Kriterien:**
  mehr Datenstruktur in Signatur, Kombination mit Buchbergers Kriterien

Literaturverzeichnis

[AH09] G. Ars und A. Hashemi. Extended F5 Criteria

[AP11] A. Arri und J. Perry. The F5 Criterion revised

[E12a] C. Eder. Improving incremental signature-based Gröbner bases algorithms

[E12b] C. Eder. Sweetening the sour taste of inhomogeneous signature-based Gröbner basis computations

[EGP11] C. Eder, J. Gash und J. Perry. Modifying Faugre's F5 Algorithm to ensure termination

[EP10] C. Eder und J. Perry. F5C: A variant of Faugre's F5 Algorithm with reduced Gröbner bases

[EP11] C. Eder und J. Perry. Signature-based algorithms to compute Gröbner bases

[Fa02] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero F_5

[GGV10] S. Gao, Y. Guan und F. Volny IV. A New Incremental Algorithm for Computing Gröbner Bases

[GVW11] S. Gao, F. Volny IV und M. Wang. A New Algorithm For Computing Grobner Bases

[HS12] B. Hammersholt Roune und M. Stillman. Practical Gröbner Basis Computation

[SIN11] W. Decker, G.-M. Greuel, G. Pfister und H. Schönemann. SINGULAR 3-1-4. *A computer algebra system for polynomial computations*, University of Kaiserslautern, 2012, `http://www.singular.uni-kl.de`.

[SW10] Y. Sun und D. Wang. A new proof of the F5 Algorithm

[SW11] Y. Sun und D. Wang. A Generalized Criterion for Signature Related Gröbner Basis Algorithms