RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

**Hausübungen zur Vorlesung**

# Kryptanalyse

**WS 2012/2013**

Blatt 13 / 23. Januar 2013 / Abgabe bis spätestens **Donnerstag** 31. Januar 2013, 14 Uhr (gerne auch früher) in dem Kasten auf NA 02 oder in NA5/74 beim Übungsleiter

**AUFGABE 1** (4 Punkte)**:**
Sei $>$ eine Monomordnung und sei $I = \langle g_1, \ldots, g_m \rangle \subset \mathbb{F}[X_1, \ldots, X_n]$ ein Ideal, wobei $G = \{g_1, \ldots, g_m\}$ nicht notwendig Gröbnerbasis. Wähle $1 \leq i \leq m$, $0 \neq c \in \mathbb{F}$ beliebig und setze $\widetilde{G_1} = (G \setminus \{g_i\}) \cup \{\overline{g_i}^{G \setminus \{g_i\}}\}$ (wie im Algorithmus `Reduziere Gröbner`) d.h. reduziere $g_i$ mittels der anderen Erzeuger (Beachte, dass dies nicht eindeutig sein muss; wir wählen einfach irgendein Ergebnis).
Ausserdem sei $\widetilde{G_2} = (G \setminus \{g_i\}) \cup \{c \cdot g_i\}$, d.h. wir ersetzen $g_i$ durch $c \cdot g_i$ mit $c \neq 0$.
Zeigen Sie:

(a) $I = \langle G \rangle = \langle \widetilde{G_1} \rangle = \langle \widetilde{G_2} \rangle$

(b) $\langle \mathrm{LM}(G) \rangle = \langle \mathrm{LM}(\widetilde{G_2}) \rangle \subset \langle \mathrm{LM}(\widetilde{G_1}) \rangle \subset \langle \mathrm{LM}(I) \rangle$

**AUFGABE 2** (4 Punkte)**:**
Sei wieder $>$ eine Monomordnung und sei $I = \langle G \rangle \subset \mathbb{F}[X_1, \ldots, X_n]$ ein Ideal mit endlicher Erzeugermenge $G$, wobei $G$ nicht notwendig Gröbnerbasis. Seien $f \neq g \in G$, wobei gelten soll, dass $\mathrm{LM}(f) \mid \mathrm{LM}(g)$. Sei $h := S(f, g) \bmod G$ ein möglicher Divisionsrest des Syzygienpolynoms $S(f, g)$ bei Division durch $G$.
Zeigen Sie:
$g \bmod (G \setminus \{g\}) \cup \{h\} = 0$, d.h. 0 ist ein möglicher Divisionsrest bei Division von $g$ durch $(G \setminus \{g\}) \cup \{h\}$.

Hinweis: Berechnen Sie $g \bmod f$. Wo taucht hierbei $S(f, g)$ auf?

Bemerkung: Als Konsequenzen von Aufgabe 1 und 2 ergeben sich (vgl. den Satz über die Korrektheit des Buchberger-Algorithmus), dass man den Algorithmus `Reduziere Gröbner` auch vor oder während des Buchberger-Algorithmus durchführen darf (was die Laufzeit verbessern kann) sowie, dass man die Erzeuger normieren darf (indem man $c = \frac{1}{\mathrm{LC}(g_i)}$ setzt). Dabei kann Schritt 1 von `Minimiere Gröbner` von `Reduziere Gröbner` miterledigt werden: Für $f, g \in G$ mit $\mathrm{LM}(f) \mid \mathrm{LM}(g)$ wird zunächst $S(f, g) \bmod G$ hinzugefügt und dann $f$ von `Reduziere Gröbner` duch 0 ersetzt (wenn man bei der Division geschickt vorgeht).

**AUFGABE 3** (8 Punkte)**:**
Betrachten Sie folgendes Erzeugendensystem für ein Ideal, das ein Subset-Sum Problem mit potenziellen Summanden $a_1 = 1, a_2 = 3, a_3 = 4$ und Zielsumme $S = 5$ formalisiert (ohne die Einschränkung, dass man genau die Hälfte der Summanden wählen muss):

$$\begin{aligned} f_1 &:= X_1^2 - X_1 \\ f_2 &:= X_2^2 - X_2 \\ f_3 &:= X_3^3 - X_3 \\ f_4 &:= X_1 + 3X_2 + 4X_3 - 5 \end{aligned}$$

Wir wollen das Subset-Sum Problem nun mittels Gröbnerbasen lösen. Berechnen Sie dazu mit dem Buchberger-Algorithmus und `Reduziere Göbner` die reduzierte Gröbnerbasis für $I = \langle f_1, f_2, f_3, f_4 \rangle \subset \mathbb{F}[X_1, X_2, X_3]$. Die Monomordnung sei dabei so zu wählen, dass $X_1 > X_2 > X_3$ gilt. $\mathbb{F}$ dürfen Sie dabei als $\mathbb{Q}$ oder $\mathbb{Z}/(11)$ wählen.

Bemerkung:
Die Wahl von $\mathbb{F} = \mathbb{Z}/(11)$ ist zulässig, da für jede Lösung $(x_1, x_2, x_3) \in V(I)$ des Gleichungssystems wegen $f_1$ bis $f_3$ jedes $x_i \in \{0, 1\}$ liegen muss und somit in Gleichung $f_4$ keine modulare Reduktion stattfinden kann. Insofern erhält man die gleichen Lösungen, egal, ob man modulo 11 rechnet oder nicht. Der Vorteil bei der Rechnung modulo 11 ist, dass nur kleine Zahlen und keine Brüche während der Rechnung auftreten. Sie dürfen die Bemerkung nach Aufgabe 1,2 sowie das Ergebnis von Aufgabe 4 nutzen.

**AUFGABE 4** (4 Punkte)**:**
Sei $\mathbb{F}$ ein Körper und seien $0 \neq f, g \in \mathbb{F}[X_1, \ldots, X_n]$ mit fest gewählter Monomordnung. Wir nehmen an, dass die Leitmonome von $f$ und $g$ keine gemeinsamen Variablen involvieren. Insbesondere gilt $\mathrm{kgV}(\mathrm{LM}(f), \mathrm{LM}(g)) = \mathrm{LM}(f) \cdot \mathrm{LM}(g)$. Zeigen Sie (ohne das Buchberger-Kriterium zu benutzen!), dass $f, g$ eine Gröbnerbasis für $I = \langle f, g \rangle$ sind.

Hinweis:
Gehen Sie so vor wie im Beweis des Buchberger-Kriteriums. Um zu zeigen, dass $\mathrm{LT}(h) \in \langle \mathrm{LM}(f), \mathrm{LM}(g) \rangle$ liegt für beliebiges $h \in I$ empfiehlt es sich $h = t_1 \cdot f + t_2 \cdot g$ zu schreiben mit (bzgl. $>$) *minimalem* $t_1$.

Bemerkung:
Für solche $f, g$ folgt damit (nach dem Buchberger-Kriterium) $S(f, g) \bmod \{f, g\} = 0$. Insbesondere muss man beim Buchberger-Algorithmus solche Paare nicht betrachten.