RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 12 / 18. Januar 2012 / Abgabe bis spätestens 25. Januar 2012, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Beweisen Sie, dass $>_{grlex}$ eine Monomordnung ist.

Hinweis: Zeigen Sie zunächst, dass $>_{lex}$ eine Monomordnung ist.

AUFGABE 2 (5 Punkte)**:**
Seien $f, g \in \mathbb{F}[x_1, \ldots, x_n] \backslash \{0\}$. Beweisen Sie folgende Aussagen.

i) $\text{multigrad}(f \cdot g) = \text{multigrad}(f) + \text{multigrad}(g)$,

ii) $\text{multigrad}(f + g) \leq \max\{\text{multigrad}(f), \text{multigrad}(g)\}$ für $f + g \neq 0$.

Geben Sie in ii) jeweils ein Beispiel an, für das der Ausdruck $=$ bzw. $<$ annimmt.

Ziel der nächsten Aufgabe ist es zu beweisen, dass die Berechnung von Resten r von f bei Division durch $F = (f_1, \ldots, f_s)$ in $\mathbb{F}[x_1, \ldots, x_n]$ als eine $\mathbb{F}$-lineare Abbildung aufgefasst werden kann, d.h. wenn r_i die Reste von g_i bei Division durch F sind für $i = 1, 2$, dann ist für beliebige $c_1, c_2 \in \mathbb{F}$ das Polynom $c_1 r_1 + c_2 r_2$ der Rest, den man bei Division von $c_1 g_1 + c_2 g_2$ durch F erhält. Hierzu ist es nötig, eine Eigenschaft der durch den Divisionsalgorithmus erzeugten Darstellung $f = a_1 f_1 + \ldots a_s f_s + r$ zu finden, welche die Darstellung eindeutig beschreibt.

BONUSAUFGABE 3 (10 Punkte)**:**
Sei $\mathrm{LM}(f_i) = x^{\alpha(i)}$ und definiere folgende Mengen

$$\begin{aligned}
\Delta_1 &:= \alpha(1) + \mathbb{N}_0^n \\
\Delta_2 &:= (\alpha(2) + \mathbb{N}_0^n) \setminus \Delta_1 \\
&\vdots \\
\Delta_s &:= (\alpha(s) + \mathbb{N}_0^n) \setminus \bigcup_{i=1}^{s-1} \Delta_i \\
\bar{\Delta} &:= \mathbb{N}_0^n \setminus \bigcup_{i=1}^{s} \Delta_i \ .
\end{aligned}$$

Man beachte, dass $\mathbb{N}_0^n$ damit die disjunkte Vereinigung der Δ_i und $\bar{\Delta}$ ist (es kann hilfreich sein, einige der Mengen zu skizzieren). Beweisen Sie:

a) $\beta \in \Delta_i$ genau dann, wenn $x^{\alpha(i)} \mid x^\beta$ und $x^{\alpha(j)} \nmid x^\beta$ für $j < i$.

b) $\gamma \in \bar{\Delta}$ genau dann, wenn $x^{\alpha(i)} \nmid x^\gamma$ für alle i.

c) Für eine vom Divisionsalgorithmus erzeugte Darstellung $f = a_1 f_1 + \ldots a_s f_s + r$ gilt:

   i) Für jedes i und jedes Monom x^β in a_i gilt $\beta + \alpha(i) \in \Delta_i$.

   ii) Für jedes Monom x^γ in r gilt $\gamma \in \bar{\Delta}$.

d) Für ein festes f gibt es genau einen Ausdruck $f = a_1 f_1 + \ldots + a_s f_s + r$ der i) und ii) aus Teil c) erfüllt.

e) Die Abbildung $f \mapsto_F r$ (d.h. ordne jedem f seinen Rest r bei Division durch F zu) ist eine $\mathbb{F}$-lineare Abbildung.