Opgave Computeralgebra, week 11: Gröbner-basis *(zie boek, §21.5)*

Zie ook de inleiding bij de opgave van week 9 (PolynomialReduce). De notatie en begrippen uit dat stuk worden hier ook gebruikt.

Zij F een lichaam en zij $R := F[x_1, \ldots, x_n]$ de ring van polynomen in n variabelen $x_1, \ldots, x_n$. Zij I een ideaal in R, d.w.z., $f, g \in I \Rightarrow f + g \in I$; $f \in I, q \in R \Rightarrow qf \in I$. Een deelverzameling B van I heet een *basis* van I als I het kleinste ideaal in R is dat B bevat. Omgekeerd is er bij elke deelverzameling B van R een kleinste ideaal I dat B bevat. We zeggen ook dat B het ideaal I *voortbrengt*. I.h.b., als $B = \{f_1, \ldots, f_s\}$ eindig is, dan is I gelijk aan de verzameling

$$\langle f_1, \ldots, f_s \rangle := \{q_1 f_1 + \cdots q_s f_s \mid q_1, \ldots, q_s \in R\}. \tag{1}$$

Omgekeerd, voor gegeven $f_1, \ldots, f_s \in R$ definieert de verzameling (1) een ideaal I, waarvan $\{f_1, \ldots, f_s\}$ een basis vormen. Dan brengt $\{f_1, \ldots, f_s\}$ het ideaal I voort.

Laat $\mathbb{N} := \{0, 1, 2, \ldots\}$. Neem op $\mathbb{N}^n$ een totale ordening (genoteerd $\prec$) zo dat:

(a) Als $\alpha, \beta, \gamma \in \mathbb{N}^n$ en $\alpha \prec \beta$ dan $\alpha + \gamma \prec \beta + \gamma$.

(b) Elke deelverzameling van $\mathbb{N}^n$ heeft een mininaal element t.o.v. $\prec$.

Definitie Een basis $G = \{g_1, \ldots, g_s\}$ van een ideaal I in R heet een *Gröbner-basis* als de verzameling $\mathrm{lt}(I) := \{\mathrm{lt}(f) \mid f \in I\}$ hetzelfde ideaal voortbrengt als de verzameling $\mathrm{lt}(G) := \{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s)\}$.

Definieer voor $f, g \in R \backslash \{0\}$ het *S-polynoom* $S(f, g)$ als volgt. Laat

$$\mathrm{mdeg}(f) := (\alpha_1, \ldots, \alpha_n), \quad \mathrm{mdeg}(g) := (\beta_1, \ldots, \beta_n), \quad \gamma_i := \max(\alpha_i, \beta_i).$$

Dan

$$S(f, g) := \frac{x^\gamma}{\mathrm{lt}(f)}\, f - \frac{x^\gamma}{\mathrm{lt}(g)}\, g.$$

Het algoritme PolynomialReduce van week 9 leverde voor gegeven $f, f_1, \ldots, f_s \in R$ een unieke $r \in R$. Noteer deze r als $r = f \operatorname{rem} (f_1, \ldots, f_s)$. Als $G = \{f_1, \ldots, f_s\}$ dan zullen we ook schrijven $f \operatorname{rem} G$, waarbij voor G de $f_1, \ldots, f_s$ in de een of andere volgorde moeten worden geschreven. Het resultaat kan van de volgorde afhangen, maar deze niet-uniciteit is niet van belang bij het onderstaande algoritme.

Buchberger's algoritme om Gröbner-basis van $\langle f_1, \ldots, f_s \rangle$ te bepalen

$G := \{f_1, \ldots, f_s\}$ (allemaal verschillend en $\neq 0$)
$B := \{(f, g) \mid f, g \in G, f \neq g\}$
while $B \neq \emptyset$ **do**
    select a pair (f, g) in B
    $B := B \backslash \{(f, g)\}$
    $h := S(f, g) \operatorname{rem} GB$.
    if $h \neq 0$ **and** $h \notin GB$ **then** $GB := GB \cup \{h\}$; $B := B \cup \{(f, h) \mid f \in GB\}$ **end if**
end do
return(GB)

Algoritme om uit een Gröbner-basis een minimale Gröbner-basis te bepalen

$G := \{g_1, \ldots, g_s\}$ (gegeven Gröbner-basis, allemaal verschillend en $\neq 0$)

for i **from** 1 **to** s **do**

if $\exists j \neq i$ such that $g_j \in G$ and $\mathrm{lt}(g_i)$ divisible by $\mathrm{lt}(g_j)$ **then** $G := G \backslash \{g_i\}$

else $g_i := g_i / \mathrm{lc}(g_i)$