De complexiteit van Buchbergers algoritme

Zomervrucht, W.

Wouter Zomervrucht

De complexiteit van Buchbergers algoritme

Bachelorscriptie Wiskunde en Informatica, 25 augustus 2010

Scriptiebegeleiders:
Ronald van Luijk en Jeannette de Graaf

Mathematisch Instituut, LIACS, Universiteit Leiden

Inhoudsopgave

Inleiding

Gröbnerbases vormen een van de centrale objecten van de algebraïsche meetkunde, als het gaat om het expliciet uitvoeren van berekeningen. Een Gröbnerbasis van een ideaal in een polynoomring is een stel voortbrengers met fijne algoritmische eigenschappen. Met behulp van een Gröbnerbasis kunnen veel problemen eenvoudig worden opgelost. We noemen het oplossen van een stelsel polynomiale vergelijkingen, het bepalen of een polynoom in een ideaal ligt en het bepalen of twee idealen gelijk zijn. Zie [8] of [11] voor meer toepassingen. Al deze problemen hebben een hoge algoritmische complexiteit. Bijvoorbeeld, zelfs als we ons beperken tot polynomen in 4 variabelen is het ideaallidmaatschapsprobleem (bepalen of een polynoom in een gegeven ideaal ligt) NP-moeilijk, wat betekent dat ieder NP-compleet probleem in polynomiale tijd te reduceren is tot dit probleem [24].

Het volgt meteen dat de constructie van een Gröbnerbasis uit een willekeurig stel voortbrengers van een ideaal niet eenvoudig kan zijn. Een algoritme dat deze constructie uitvoert is gegeven door Buchberger, en het is naar hem genoemd. Het principe van dit algoritme is om net zolang voortbrengers van het ideaal te blijven toevoegen totdat we een Gröbnerbasis hebben. Buchbergers algoritme termineert altijd, maar het bewijs daarvan is niet constructief. Daarom is het onbekend hoelang het algoritme bezig is, oftewel wat de complexiteit ervan is. Hier is veel onderzoek naar gedaan, maar sluitende onder- en bovengrenzen zijn er niet. Naast Buchbergers algoritme zijn er andere algoritmes die Gröbnerbases construeren [19, 28]. Deze zijn echter van meer theoretisch belang en in de praktijk werkt Buchbergers algoritme het beste. We gaan hier in deze scriptie niet verder op in.

We beginnen deze scriptie met een behandeling van de onderliggende theorie. We definiëren Gröbnerbases, voeren Buchbergers algoritme in en formuleren de complexiteitsvragen. We eindigen dit hoofdstuk met een voorbeeld. De meeste stellingen bewijzen we niet: we verwijzen vaak naar het boek van Cox, Little en O'Shea [11]. De eerste twee hoofdstukken van dat boek zijn ook heel geschikt als een grondigere inleiding in Gröbnerbases dan we hier geven.

In hoofdstuk 2 geven we ondergrenzen voor de complexiteit. We laten zien dat de grootte van een Gröbnerbasis dubbelexponentieel kan groeien in het aantal variabelen in de polynoomring. Aan de andere kant is er altijd een Gröbnerbasis met grootte begrensd door een vergelijkbare bovengrens: dat bewijzen we in hoofdstuk 3.

Het is onbekend of deze bovengrens ook geldt voor de complexiteit van Buchbergers algoritme. In hoofdstuk 4, het belangrijkste deel van deze scriptie, leiden we een nieuwe bovengrens voor die complexiteit af, in termen van de Ackermannfunctie. We gebruiken daarbij alleen combinatorische argumenten. Tot dusver waren er vrijwel alleen bovengrenzen bekend onder beperkingen op de invoer (zoals het aantal variabelen of de gebruikte monoomordening), maar onze grens geldt algemeen. Kort geleden ontdekten we dat dit resultaat niet geheel nieuw is: vergelijkbare grenzen worden afgeleid in [13]. Toch zullen we op bladzijde 25 zien dat onze grenzen een nuttige toevoeging vormen.

Het laatste hoofdstuk behandelt enkele onderwerpen uit de literatuur rond Buchbergers algoritme en de complexiteit daarvan. We bespreken aanpassingen van het algoritme die de complexiteit verlagen. Ook geven we complexiteitsgrenzen wanneer het aantal variabelen in de polynoomring klein is. Ten slotte bekijken we de invloed van monoomordeningen op het algoritme, en hoe we daar gebruik van kunnen maken.

Ik wil mijn begeleiders Ronald van Luijk en Jeannette de Graaf, en ook Hendrik Lenstra, bedanken voor de tijd en moeite die ze hebben gestoken in de ondersteuning van dit bacheloronderzoek.

1 Algoritmische ideaaltheorie

Zij K een lichaam. De polynoomring $K[x]$ over K in de variabele x is een hoofdideaaldomein. Voor ieder ideaal $I \subset K[x]$ is er dus een polynoom $g \in K[x]$ met $I = (g)$. Dit polynoom vinden we uit een stel voortbrengers van I door middel van het algoritme van Euclides. Wanneer $f \in K[x]$ een ander polynoom is, bepalen we of f in I ligt door f door g te delen. Is de rest gelijk aan 0, dan geldt $f \in I$, en anders geldt $f \notin I$.

Laat nu $X = \{x_1, \ldots, x_n\}$ zijn. Voor $n > 1$ is de polynoomring $R = K[X] = K[x_1, \ldots, x_n]$ geen hoofdideaaldomein. In het algemeen zullen we voor een ideaal $I \subset R$ dus meerdere voortbrengers $g_1, \ldots, g_s$ nodig hebben. We kunnen volstaan met eindig veel voortbrengers omdat R noethers is. Om van $f \in R$ te bepalen of f in I ligt, willen we weten of er polynomen $h_1, \ldots, h_s$ zijn zodanig dat geldt

$$f = h_1 g_1 + \ldots + h_s g_s.$$

We proberen dus f tegelijk te delen door $g_1, \ldots, g_s$. Daarvoor zullen we een generalisatie van deling met rest invoeren. Deze generalisatie heeft echter niet alle gewenste eigenschappen. De rest is bijvoorbeeld niet uniek. Als de deling een rest geeft die niet 0 is, volgt niet noodzakelijk $f \notin I$. Dit probleem treedt niet op wanneer we een geschikt stel voortbrengers voor I kiezen: een Gröbnerbasis.

1.1 Deling met rest

Wanneer we polynomen $f, g \in K[x]$ op elkaar delen, delen we steeds de kopterm van f door de kopterm van g. We generaliseren het begrip kopterm naar polynomen in meerdere variabelen. Een product $x_1^{d_1} \cdots x_n^{d_n}$ met $d_1, \ldots, d_n \geq 0$ noemen we een *monoom* over $X = \{x_1, \ldots, x_n\}$.

Definitie 1.1. Een *monoomordening* $\succ$ op X is een welordening van de monomen over X met de volgende eigenschap: als M, N en P monomen zijn met $M \succ N$, dan geldt $MP \succ NP$. Als bovendien voor alle monomen M en N met $\deg(M) > \deg(N)$ geldt $M \succ N$, heet $\succ$ *graadrespecterend*.

Definitie 1.2. Zij $f \in R$ een niet-nul polynoom, en kies een monoomordening $\succ$. Het *leidende monoom* $\text{LM}(f)$ van f is het grootste monoom (ten opzichte van $\succ$) dat in f voorkomt met een niet-nul coëfficiënt. De *leidende term* $\text{LT}(f)$ van f is het leidende monoom van f vermenigvuldigd met zijn coëfficiënt in f.

Een voorbeeld van een monoomordening is de *lexicografische ordening*, kortweg *lex*. In deze ordening geldt $x_1^{d_1} \cdots x_n^{d_n} \succ x_1^{e_1} \cdots x_n^{e_n}$ als $d_i > e_i$ voor de kleinste i met $d_i \neq e_i$. De monomen zijn dus alfabetisch geordend met $x_1 \succ \ldots \succ x_n$. Verwant hieraan is de *graadlexicografische ordening* of *deglex*, waarin $M \succ N$ als $\deg(M) > \deg(N)$ of als $\deg(M) = \deg(N)$ en M lexicografisch groter is dan N. De lex ordening is niet graadrespecterend, deglex per definitie wel. Vanaf nu nemen we aan dat er een monoomordening $\succ$ gekozen is. Met behulp daarvan kunnen we als volgt deling met rest definiëren.

Algoritme 1.3 (Deling met rest).
Invoer: polynomen $f \in R$ en $g_1, \ldots, g_s \in R \setminus \{0\}$.
Uitvoer: rest bij deling van f door $g_1, \ldots, g_s$.

$r := 0$;
while $f \neq 0$ **do**
  $B := \{i \in \{1, \ldots, s\} : \text{LT}(g_i) \mid \text{LT}(f)\}$;
  if $B \neq \varnothing$ **then**
    kies $i \in B$;
    $f := f - \frac{\text{LT}(f)}{\text{LT}(g_i)} \cdot g_i$;
  else
    $r := r + \text{LT}(f)$;
    $f := f - \text{LT}(f)$;
return r;

Het algoritme termineert omdat het leidende monoom $\text{LM}(f)$ steeds kleiner wordt ten opzichte van de monoomordening $\succ$. Dit is een welordening, dus f wordt na een eindig aantal stappen 0.

Er is keuzevrijheid in het algoritme als B meerdere elementen bevat. De rest is afhankelijk van deze keuze. Wanneer $G = (g_1, \ldots, g_s)$ een geordend rijtje is, maken we het algoritme deterministisch door $i = \min(B)$ te eisen. De uitvoer noteren we dan met $\text{nf}_G(f)$, de *normaalvorm* van f ten opzichte van G. Het berekenen van de rest bij deling van f door G heet ook wel het *reduceren* van f ten opzichte van G. Als de rest bij deling van f door G gelijk is aan f, dan heet f *gereduceerd* ten opzichte van G.

1.2 Gröbnerbases

In analogie met het univariate geval willen we dat geldt $\text{nf}_G(f) = 0$ dan en slechts dan als $f \in I = (G)$. Het kan echter gebeuren dat er een $f \in I$ is met $\text{nf}_G(f) \neq 0$. Deling met rest gaat wel goed als we geschikte voortbrengers voor I kiezen. We noteren $\text{LM}(S) = \{\text{LM}(h) : h \in S \setminus \{0\}\}$ voor $S \subset R$.

Definitie 1.4. Kies een monoomordening en laat $I \subset R$ een ideaal zijn. Een eindige deelverzameling $G \subset I$ heet een *Gröbnerbasis* voor I als

$$(\text{LM}(I)) = (\text{LM}(G)).$$

In dat geval is $I = (G)$, zie [11, §2.5, Corollary 6].

Stelling 1.5. Laat G een Gröbnerbasis zijn voor een ideaal $I \subset R$. Voor een polynoom $f \in R$ zijn er unieke $g \in I$ en $r \in R$ waarvoor geldt dat $f = g + r$ en dat geen term van r deelbaar is door een term $\text{LT}(h)$ met $h \in G$.

Bewijs. Zie [11, §2.6, Proposition 1]. □

In het bijzonder is deze r gelijk aan de rest bij deling van f door G, ongeacht de ordening van de elementen van G. We kunnen in dit geval dus ook ondubbelzinnig $\text{nf}_G(f)$ schrijven hoewel G slechts een verzameling is. Bovendien geldt voor $f \in I$ dat $g = f$ en $r = 0$, zodat we eenvoudig kunnen beslissen of een polynoom al dan niet in I ligt.

Gevolg 1.6. Laat G een Gröbnerbasis voor een ideaal $I \subset R$ zijn. Voor een polynoom $f \in R$ geldt dat $f \in I$ dan en slechts dan als $\text{nf}_G(f) = 0$. □

Om Gröbnerbases beter te begrijpen noemen we de volgende eigenschap van *monoomidealen*. Dit zijn idealen die kunnen worden voortgebracht door een verzameling monomen.

Propositie 1.7. Zij $S \subset R$ een verzameling monomen en $M \in R$ een monoom. Dan geldt $M \in (S)$ dan en slechts dan als er een monoom $N \in S$ is met $N \mid M$.

Bewijs. Zie [11, §2.4, Lemma 2]. □

Een Gröbnerbasis is verre van uniek. Enkele gevallen verdienen extra aandacht.

Definitie 1.8. Een Gröbnerbasis G voor $I \subset R$ heet *minimaal* als geen echte deelverzameling van G een Gröbnerbasis voor I is.
Verder heet G *gereduceerd* als elk polynoom $g \in G$ monisch is en gereduceerd ten opzichte van $G \setminus \{g\}$.

Uit propositie 1.7 volgt dat G minimaal is dan en slechts dan als voor alle $g \in G$ het leidende monoom $\text{LM}(g)$ niet in $(\text{LM}(G \setminus \{g\}))$ zit. Bovendien zien we dat iedere gereduceerde Gröbnerbasis minimaal is.

Propositie 1.9. Zij $I \subset R$ een ideaal en kies een monoomordening. Dan is er een unieke gereduceerde Gröbnerbasis voor I.

Bewijs. Zie [11, §2.7, Proposition 6]. □

Met Gröbnerbases van twee idealen kunnen we wegens gevolg 1.6 bepalen of deze idealen gelijk zijn, door na te gaan of de voortbrengers van het ene ideaal in het andere liggen en andersom. Een andere methode is nu om de gereduceerde Gröbnerbases van de idealen te berekenen en te vergelijken.

Minimale Gröbnerbases hebben de kleinste verzameling leidende monomen.

Propositie 1.10. Zij G een minimale Gröbnerbasis voor een ideaal $I \subset R$ en H een willekeurige Gröbnerbasis voor I. Dan geldt $\text{LM}(G) \subset \text{LM}(H)$.

Bewijs. Neem $g \in G$. Wegens $(\text{LM}(G)) = (\text{LM}(I)) = (\text{LM}(H))$ en propositie 1.7 is er een $h \in H$ met $\text{LM}(h) \mid \text{LM}(g)$. Andersom is er een $f \in G$ met $\text{LM}(f) \mid \text{LM}(h)$. Maar dan geldt $\text{LM}(f) \mid \text{LM}(g)$ en volgt $f = g$, want anders geeft $(\text{LM}(G \setminus \{g\})) = (\text{LM}(G))$ een tegenspraak met de minimaliteit van G. In het bijzonder geldt $\text{LM}(g) = \text{LM}(h) \in \text{LM}(H)$. □

1.3 Buchbergers algoritme

Het probleem rest om uit gegeven voortbrengers van een ideaal een Gröbnerbasis te vinden. Daarvoor gebruiken we een eigenschap die equivalent is met de definitie van een Gröbnerbasis.

Definitie 1.11. Laat $g, h \in R$ twee niet-nul polynomen. Het *S-polynoom* van g en h is

$$S(g,h) = \frac{\text{kgv}(\text{LM}(g), \text{LM}(h))}{\text{LT}(g)} \cdot g - \frac{\text{kgv}(\text{LM}(g), \text{LM}(h))}{\text{LT}(h)} \cdot h.$$

Het S-polynoom is dus het verschil van veelvouden van g en h zodanig dat de leidende termen precies tegen elkaar wegvallen.

Stelling 1.12 (Buchbergers criterium). Zij $I \subset R$ een ideaal en $G \subset I$ een eindige deelverzameling. Rust G uit met een willekeurige ordening op de elementen. Dan is G een Gröbnerbasis voor I dan en slechts dan als geldt $I = (G)$ en $\text{nf}_G(S(g,h)) = 0$ voor alle $g, h \in G \setminus \{0\}$.

Bewijs. Zie [11, §2.6, Theorem 6]. □

Buchbergers criterium geeft een eenvoudige methode om te testen of G een Gröbnerbasis is. Ook kunnen we er een algoritme uit afleiden om Gröbnerbases te berekenen: als $\text{nf}_G(S(g,h)) \neq 0$, voeg dan $\text{nf}_G(S(g,h))$ toe aan G, en herhaal dit tot alle S-polynomen rest 0 geven bij deling door G.

Algoritme 1.13 (Buchbergers algoritme).
Invoer: eindige deelverzameling $G = \{g_1, \ldots, g_s\} \subset R \setminus \{0\}$.
Uitvoer: Gröbnerbasis voor (G).

$B := \{(g_i, g_j) : 1 \leq i < j \leq s\}$;
while $B \neq \varnothing$ **do**
  kies $(g,h) \in B$;
  $B := B \setminus \{(g,h)\}$;
  $q := \text{nf}_G(S(g,h))$; // met G op een of andere manier geordend
  if $q \neq 0$ **then**
    $B := B \cup \{(p,q) : p \in G\}$;
    $G := G \cup \{q\}$;
return G;

Stelling 1.14. Buchbergers algoritme termineert en is correct.

Bewijs. Definieer vooraf $I = (G)$. De gelijkheid $I = (G)$ geldt dan tijdens de hele executie. De polynomen die aan G worden toegevoegd zijn immers gereduceerde S-polynomen van polynomen in I, en liggen dus zelf in I. De verzameling B houdt bij welke S-polynomen nog niet zijn uitgerekend. Als het algoritme stopt, geldt voor alle verschillende polynomen g, h in de uitvoer dat tijdens de executie $\text{nf}_G(S(g,h))$ of $\text{nf}_G(S(h,g)) = -\text{nf}_G(S(g,h))$ is uitgerekend. Indien dat niet naar 0 reduceerde is er direct een polynoom aan G toegevoegd waardoor dat daarna wel het geval is. Volgens Buchbergers criterium 1.12 hoeven we dus alleen nog te bewijzen dat het algoritme termineert.

Noem de aan G toegevoegde polynomen $g_{s+1}, g_{s+2}, \ldots$, en schrijf $G_i = \{g_1, \ldots, g_i\}$. We gaan bewijzen dat voor $i > s$ geldt

$$(\text{LM}(G_{i-1})) \subsetneq (\text{LM}(G_i)). \tag{1}$$

De inclusie volgt direct uit $G_{i-1} \subset G_i$. Verder hebben we $g_i \neq 0$ en $\text{LM}(g_i) \in (\text{LM}(G_i))$. Omdat g_i de rest is bij deling van een polynoom door G_{i-1}, is geen term van g_i deelbaar door een term $\text{LT}(g_j)$ met $1 \leq j < i$. In het bijzonder geldt, wegens propositie 1.7, dat $\text{LM}(g_i) \notin (\text{LM}(G_{i-1}))$. De inclusie in (1) is dus strikt. Maar R is noethers, dus iedere keten van strikte ideaalinclusies is eindig. We concluderen dat het aantal toegevoegde polynomen eindig is. Op ieder moment is B eindig, en kunnen er hoogstens $\#B$ iteraties volgen zonder dat er een polynoom aan G wordt toegevoegd. Het aantal iteraties is dus ook eindig. □

Zoeken we de gereduceerde Gröbnerbasis voor I, dan passen we eerst Buchbergers algoritme toe. Daarna maken we alle polynomen monisch en reduceren herhaald alle $g \in G$ ten opzichte van $G \setminus \{g\}$, waarbij we nullen uit G verwijderen. Merk op dat deze constructie de existentie in propositie 1.9 bewijst.

1.4 Complexiteit

Met Buchbergers algoritme kunnen we altijd een Gröbnerbasis van een ideaal uitrekenen. Een belangrijke vraag is vervolgens wat de *complexiteit* van dit algoritme is. Om in de praktijk nuttig te zijn moet het binnen redelijke tijd een Gröbnerbasis vinden. Vragen die betrekking hebben op de complexiteit van Buchbergers algoritme zijn bijvoorbeeld:

- Hoeveel iteraties voert Buchbergers algoritme uit?
- Hoeveel polynomen voegt het algoritme toe aan het oorspronkelijke stel voortbrengers?
- Hoe groot is de graad van de polynomen in de uitvoer?
- Hoe groot wordt de graad van polynomen in de berekeningen van het algoritme?

Zowel bovengrenzen als ondergrenzen voor het slechtste geval zijn relevant. Deze grenzen drukken we meestal uit in het aantal variabelen in de polynoomring en de maximale graad van de polynomen in de invoer. Merk op dat de laatste twee vragen echt verschillend zijn. Het kan gebeuren dat tijdens het reduceren van een S-polynoom een tussenresultaat ontstaat met graad veel groter dan de graden van polynomen in de uitvoer. De eerste twee vragen liggen wel heel dicht bij elkaar.

Propositie 1.15. Stel dat Buchbergers algoritme t polynomen als uitvoer geeft, dan voert het algoritme precies $\binom{t}{2}$ iteraties uit.

Bewijs. In iedere iteratie wordt een S-polynoom van twee polynomen in de uitvoer berekend, en van ieder ongeordend tweetal polynomen in de uitvoer wordt het S-polynoom precies eenmaal berekend. Het aantal iteraties is dus gelijk aan het aantal paren polynomen in de uitvoer, oftewel $\binom{t}{2}$. □

Vaak wordt een versie van Buchbergers algoritme gebruikt die direct de gereduceerde Gröbnerbasis bepaalt. Daarin worden de elementen van G steeds ten opzichte van elkaar gereduceerd nadat een polynoom aan G is toegevoegd. Dat kan nuttig zijn omdat het aantal polynomen in G dan mogelijk kleiner wordt. Voor deze versie geldt propositie 1.15 niet: door het reduceren kan het aantal polynomen in de uitvoer kleiner zijn dan het aantal dat gedurende het algoritme aan G is toegevoegd. De graad van polynomen in een Gröbnerbasis kan door reduceren zowel kleiner als groter worden. Tussen aantal en graad bestaat in het algemeen bij minimale Gröbnerbases echter het volgende verband.

Propositie 1.16. Laat $I \subset R$ een ideaal zijn en G een minimale Gröbnerbasis voor I. Als alle monomen in $\text{LM}(G)$ graad hoogstens d hebben, dan bevat G niet meer dan $\binom{d+n-1}{n-1}$ polynomen.

Bewijs. Geen van de leidende monomen in $\text{LM}(G)$ is een deler van een ander wegens minimaliteit. Schrijven we zo'n monoom als $x_1^{d_1} \cdots x_n^{d_n}$, dan zijn er bij vaste $d_1, \ldots, d_{n-1}$ geen twee monomen waarin de variabelen $x_1, \ldots, x_{n-1}$ deze exponenten hebben: een daarvan zou immers de ander delen. Het aantal leidende monomen, dus het aantal polynomen in G, is daarom begrensd door het aantal manieren om $d_1 + \ldots + d_{n-1} \leq d$ te schrijven met $d_i \geq 0$ geheel. Dat aantal is $\binom{d+n-1}{n-1}$. □

Deze grens is strikt: de verzameling van de $\binom{d+n-1}{n-1}$ monomen van graad d is een gereduceerde, dus minimale Gröbnerbasis voor het ideaal dat het voortbrengt.

Voor alle bovengenoemde vragen zijn er nog geen vergelijkbare onder- en bovengrenzen bekend. De moeilijkheid in het vinden van bovengrenzen zien we wanneer we kijken naar het bewijs van stelling 1.14. Het termineren van Buchbergers algoritme is gebaseerd op het noethers zijn van R en wordt daarmee niet constructief bewezen. Uit het bewijs kan dus niet direct een bovengrens voor de looptijd worden geconcludeerd.

1.5 Een voorbeeld

In deze paragraaf illustreren we de voorgaande theorie aan de hand van een voorbeeld. We werken in de polynoomring $R = \mathbb{Q}[x, y, z]$ en gebruiken lex ordening met $x \succ y \succ z$. Laat

$$g_1 = x^2y - xyz^2, \qquad g_2 = xz + 2y^2.$$

We hebben $\text{LM}(g_1) = x^2y$ en $\text{LM}(g_2) = xz$. Het doel is om te bepalen of een derde polynoom

$$f = 2x^2y^3z + x^2yz^4$$

bevat is in het ideaal $I = (g_1, g_2)$. We proberen eerst naief f te delen door g_1 en g_2:

$$\begin{aligned} f &= 2y^2z \cdot g_1 + x^2yz^4 + 2xy^3z^3 = (2y^2z + z^4)g_1 + 2xy^3z^3 + xyz^6 \\ &= (2y^2z + z^4)g_1 + 2y^3z^2 \cdot g_2 + xyz^6 - 4y^5z^2 = (2y^2z + z^4)g_1 + (2y^3z^2 + yz^5)g_2 - 4y^5z^2 - 2y^3z^5 \end{aligned}$$

en nu kunnen we niet verder delen. Merk op dat de graad tijdens het delen is toegenomen. We hadden ook anders kunnen beginnen:

$$\begin{aligned} f &= 2xy^3 \cdot g_2 + x^2yz^4 - 4xy^5 = (2xy^3 + xyz^3)g_2 - 4xy^5 - 2xy^3z^3 \\ &= (2xy^3 + xyz^3 - 2y^3z^2)g_2 - 4xy^5 + 4y^5z^2. \end{aligned} \tag{2}$$

Dit geeft een andere rest, maar weer niet 0. Toch ligt f in I, want er geldt

$$f = x^2yz \cdot g_2 - xz^2 \cdot g_1.$$

Dit is dus een situatie waar voor een polynoom $f \in I$ geldt $\text{nf}_{\{g_1,g_2\}}(f) \neq 0$. Deze ongewenste eigenschap lossen we op door een Gröbnerbasis voor I te bepalen met Buchbergers algoritme. We hebben

$$S(g_1, g_2) = z \cdot g_1 - xy \cdot g_2 = -2xy^3 - xyz^3 = -yz^2 \cdot g_2 - 2xy^3 + 2y^3z^2.$$

We voegen dus $g_3 = xy^3 - y^3z^2$ als voortbrenger toe. Dan is

$$\begin{aligned} S(g_1, g_3) &= y^2 \cdot g_1 - x \cdot g_3 = 0, \\ S(g_2, g_3) &= y^3 \cdot g_2 - z \cdot g_3 = 2y^5 + y^3z^3, \end{aligned}$$

wat direct gereduceerd is. We voegen $g_4 = 2y^5 + y^3z^3$ toe. Het is eenvoudig te controleren dat nu alle S-polynomen naar 0 reduceren. Het volgt dat $G = \{g_1, g_2, g_3, g_4\}$ een Gröbnerbasis voor I is. Inderdaad zien we dat bijvoorbeeld de deling in (2) is voort te zetten als

$$f = (2xy^3 + xyz^3 - 2y^3z^2)g_2 - 4y^2 \cdot g_3.$$

Nu is de rest bij deling wel 0.

Merk op dat G wel minimaal maar niet gereduceerd is. Er geldt namelijk

$$g_1 = -yz \cdot g_2 + x^2y + 2y^3z.$$

Verder zijn alle polynomen wel gereduceerd, dus na ze monisch te maken volgt dat

$$\{x^2y + 2y^3z,\ xz + 2y^2,\ xy^3 - y^3z^2,\ y^5 + \tfrac{1}{2}y^3z^3\}$$

de gereduceerde Gröbnerbasis voor I is.

2 Dubbelexponentiële ondergrenzen

Bij het bestuderen van de complexiteit van een algoritme is het altijd belangrijk om niet alleen te kijken naar bovengrenzen, maar ook invoerinstanties te zoeken waarop het algoritme slecht presteert. Voor Buchbergers algoritme komt dat neer op het vinden van instanties waar de uitvoer in aantal of graad heel groot is (we gaan immers uit van een versie van het algoritme waarin niet gereduceerd wordt). De beste ondergrenzen gaan terug op een constructie van Mayr en Meyer [32, §6]. Zij geven voorbeelden waar de uitvoer in graad dubbelexponentieel groeit in het aantal variabelen. We zullen een vereenvoudigde versie van deze constructie geven, afkomstig van Bayer en Stillman [3, §2]. Vervolgens geven we een nieuwe vereenvoudiging van een constructie van Huynh [23]. Hieruit volgt ook een dubbelexponentiële ondergrens voor het aantal polynomen in de uitvoer.

2.1 Commutatieve Thuesystemen

De idealen in de constructies zullen allemaal *binoomidealen* zijn. Dat wil zeggen dat ze kunnen worden voortgebracht door *binomen*, polynomen die het verschil tussen twee monomen zijn. We gebruiken deze idealen omdat congruentie modulo het ideaal dan een equivalentierelatie op monomen geeft die we ook via zogenaamde commutatieve Thuesystemen kunnen beschrijven. Bovendien houden Gröbnerbases deze vorm intact. Stel immers dat de invoer van Buchbergers algoritme bestaat uit binomen. Er geldt

$$S(M_1 - N_1, M_2 - N_2) = P_1(M_1 - N_1) - P_2(M_2 - N_2) = P_2N_2 - P_1N_1$$

voor zekere monomen P_1 en P_2. Tijdens het reduceren blijft deze vorm behouden, aangezien de polynomen waardoor wordt gedeeld ook binomen zijn. Zo volgt meteen het volgende lemma.

Lemma 2.1. Zij $I \subset R$ een binoomideaal. Dan zijn de elementen van de gereduceerde Gröbnerbasis voor I ook binomen. □

Om commutatieve Thuesystemen te bestuderen voeren we nu eerst enkele begrippen in.

Definitie 2.2. Een *monoïde* is een verzameling X met een associatieve bewerking $\cdot : X \times X \to X$, zodanig dat er een eenheidselement $1 \in X$ is met $1 \cdot x = x \cdot 1 = x$ voor alle $x \in X$.

Definitie 2.3. De *vrije abelse monoïde* over een verzameling X is de monoïde met als elementen eindige associatieve en commutatieve producten van nul of meer elementen van X. De bewerking is de natuurlijke vermenigvuldiging hierop.

Een monoïde voldoet dus aan alle groepsaxioma's, behalve het bestaan van inversen. In de vrije abelse groep over X is de vrije abelse monoïde over X het deel dat bestaat uit elementen van de vorm $x_1 \cdots x_r$, met $x_1, \ldots, x_r \in X$. Dit worden ook wel de *effectieve* elementen genoemd. Merk op dat de vrije abelse monoïde over X precies de verzameling monomen over X is.

Definitie 2.4. Laat $\mathcal{M}$ de vrije abels monoïde over X zijn. Een *Thuesysteem* over X is een eindige deelverzameling $T \subset \mathcal{M} \times \mathcal{M}$. Als voor elke $(a, b) \in T$ ook geldt dat $(b, a) \in T$, dan heet T *commutatief*.

De elementen van T noemen we *producties*. Voor $v, w \in \mathcal{M}$ schrijven we $v \to w$ als er een $z \in \mathcal{M}$ en een $(a, b) \in T$ zijn met $v = az$ en $w = bz$. Een rijtje $v = v_0 \to v_1 \to \ldots \to v_s = w$ heet een *afleiding* van w uit v. Als zo'n afleiding bestaat is w *afleidbaar* uit v. Wanneer T commutatief is, is afleidbaarheid een equivalentierelatie, die we noteren met $v \equiv_T w$.

Bij een commutatief Thuesysteem T over X construeren we een binoomideaal $I_T \subset K[X]$, waar $K[X]$ de polynoomring over K is met de elementen van X als variabelen. Hiervoor vatten we iedere $(a, b) \in T$ op als het polynoom $a - b \in K[X]$, en laten I_T het ideaal voortgebracht door deze polynomen zijn. Congruentie en equivalentie van monomen is nu hetzelfde.

Propositie 2.5. Laat $\mathcal{M}$ de vrije abelse monoïde over X zijn en T een commutatief Thuesysteem over X. Voor monomen $v, w \in \mathcal{M}$ geldt $v \equiv_T w$ dan en slechts dan als $v - w \in I_T$.

Bewijs. Als geldt $v \equiv_T w$, dan schrijven we $v = v_0 \to v_1 \to \ldots \to v_s = w$. Neem $(a_i, b_i) \in T$ en $z_i \in \mathcal{M}$ voor $1 \leq i \leq s$ met steeds $v_{i-1} = a_i z_i$ en $v_i = b_i z_i$. Dan geldt dat $v - w = \sum_{i=1}^{s} z_i(a_i - b_i) \in I_T$. Stel nu andersom dat $v - w \in I_T$. Voor $v = w$ is de propositie triviaal dus neem aan dat geldt $v \neq w$. Schrijf $v - w = \sum_{i=1}^{s} c_i z_i (a_i - b_i)$ met steeds $c_i \in K$, $z_i \in \mathcal{M}$ en $(a_i, b_i) \in T$. Beschouw de graaf met als knopen monomen en voor $1 \leq i \leq s$ een gerichte pijl van $a_i z_i$ naar $b_i z_i$ met gewicht c_i. Noem het gewicht van een knoop de som van de gewichten van de uitgaande pijlen min de som van de gewichten van de ingaande pijlen. Dan heeft v gewicht 1, w gewicht -1 en alle andere monomen hebben gewicht 0. Bovendien is in iedere ongerichte samenhangscomponent het totale gewicht 0, dus v en w liggen in dezelfde component. Er is een ongericht pad $v = v_0, v_1, \ldots, v_s = w$ van v naar w. Nu geldt de afleiding $v_0 \to v_1 \to \ldots \to v_s$ dus er volgt $v \equiv_T w$. □

Kies een monoomordening $\succ$ op X. Voor iedere $v \in \mathcal{M}$ heeft de equivalentieklasse van v een kleinste element. Laat A_T de verzameling monomen zijn die niet het kleinste element van hun equivalentieklasse zijn. Deze kunnen dus nog 'gereduceerd' worden. Uit A_T nemen we vervolgens de deelverzameling M_T van minimale elementen ten opzichte van deling: dit zijn de elementen van A_T die geen echte delers in A_T hebben, dus de 'kleinste reduceerbare' elementen. De verzameling M_T heeft een bijzonder verband met Gröbnerbases.

Lemma 2.6. Laat T een commutatief Thuesysteem over X zijn en G een Gröbnerbasis voor het corresponderende ideaal $I_T \subset K[X]$. Dan geldt $M_T \subset \text{LM}(G)$.

Bewijs. Na propositie 1.10 is het genoeg om het lemma te bewijzen als G gereduceerd is. Kies $v \in M_T$ en neem een monoom $w \prec v$ met $w \equiv_T v$. Per definitie van M_T is dat mogelijk. Volgens propositie 2.5 geldt dat $v - w \in I_T$. Dan is er een $g \in G$ met $\text{LM}(g) \mid \text{LM}(v - w) = v$. Lemma 2.1 geeft dat $g = y - z$ voor zekere monomen y en z. Uit $y - z \in I_T$ volgt dat $y \equiv_T z$. Bovendien geldt $y \succ z$ dus $y \in A_T$. Maar y is een deler van v, die geen echte delers in A_T heeft. Er volgt dat $v = y = \text{LM}(g) \in \text{LM}(G)$. □

We hebben dit bewijs sterk vereenvoudigd ten opzichte van dat in [23, Lemma 2.8]. Daar wordt een omweg gemaakt via zogenaamde *Church-Rosser* Thuesystemen, die het equivalent van Gröbnerbases zijn voor commutatieve Thuesystemen.

2.2 De constructie

Een commutatief Thuesysteem T waarvoor M_T groot is in aantal of graad van de elementen geeft vanwege lemma 2.6 direct een instantie van Buchbergers algoritme met een minstens zo grote uitvoer. Hier geven we een constructie die op deze manier de volgende stelling bewijst.

Stelling 2.7. Voor $d \geq 2$ en $n \geq 0$ is er een verzameling G van $40n + 20$ polynomen in $40n + 37$ variabelen, elk polynoom van graad hoogstens $\max(d+2, 5)$, zodanig dat met elke graadrespecterende monoomordening iedere Gröbnerbasis voor (G) meer dan d^{2^n} polynomen van graad groter dan d^{2^n} bevat.

We beginnen met de constructie van Bayer en Stillman [3, §2]. Kies $d \geq 2$ vast en neem

$$V_n = \{s_n, t_n, c_{n1}, \ldots, c_{n4}, x_{n1}, \ldots, x_{n4}\}$$

voor $n \geq 0$. Definieer $X_n = V_0 \cup \ldots \cup V_n$. We maken inductief een commutatief Thuesysteem T_n over X_n. Definieer eerst T_0 door de producties $(s_0 c_{0i},\ t_0 c_{0i} x_{0i}^d)$ voor $1 \leq i \leq 4$. Gegeven T_n nemen we in T_{n+1} alle producties uit T_n en bovendien

$$\begin{array}{lll} (s_{n+1},\ s_n c_{n1}), & (t_n c_{n1},\ s_n c_{n2}), & (t_n c_{n2} x_{n1},\ t_n c_{n3} x_{n4}), \\ (s_n c_{n2},\ s_n c_{n3}), & (s_n c_{n3},\ t_n c_{n4}), & (s_n c_{n4},\ t_{n+1}), \end{array}$$

$$(t_n c_{n2} x_{n2} c_{n+1,i},\ t_n c_{n2} x_{n3} c_{n+1,i} x_{n+1,i}) \quad \text{voor } 1 \leq i \leq 4.$$

Steeds als we een productie (v, w) opnemen, nemen we ook (w, v) voor commutativiteit. Het bewijs van het volgende lemma is lang maar niet moeilijk.

Lemma 2.8. In T_n gelden de equivalenties $s_n c_{ni} \equiv_{T_n} t_n c_{ni} x_{ni}^{d^{2^n}}$ voor $1 \leq i \leq 4$. Een monoom $v \equiv_{T_n} s_n c_{ni}$ met een factor s_n of t_n kan alleen $v = s_n c_{ni}$ of $v = t_n c_{ni} x_{ni}^{d^{2^n}}$ zijn. Voor $e < d^{2^n}$ is uit $t_n c_{ni} x_{ni}^e$ geen monoom afleidbaar dat een factor s_n of t_n heeft, behalve $t_n c_{ni} x_{ni}^e$ zelf.

Bewijs. Zie [3, Lemma 2.2]. □

Het nagaan van de afleidingen bij deze equivalenties is een eenvoudige manier om de werking van T_n te bestuderen. Uit het lemma kunnen we instanties van Buchbergers algoritme construeren waarvoor de uitvoer polynomen van graad groter dan d^{2^n} bevat. In plaats daarvan geven we een nieuwe constructie om een vergelijkbare ondergrens voor het aantal polynomen te vinden. Deze constructie hebben we gebaseerd op die in [23], maar is eenvoudiger. We maken een commutatief Thuesysteem T met onder andere variabelen $s_1, \ldots, s_5, t, c, a, x, y, \bar{x}, \bar{y}, z$. Merk op dat dit nieuwe variabelen zijn en niet die van hierboven. Gebruik viermaal bovenstaande constructie als deelconstructie om equivalenties

$$s_1 c \equiv s_2 c a^{d^{2^n}}, \qquad s_2 c \equiv s_3 c x^{d^{2^n}}, \qquad s_4 c \equiv s_3 c a^{d^{2^n}}, \qquad s_5 c \equiv s_4 c z^{d^{2^n}}$$

te krijgen. Hier en later noteren we kortweg $\equiv$ voor $\equiv_T$. De hulpvariabelen die we voor deze equivalenties nodig hebben kiezen we steeds verschillend. Verder nemen we in T nog de producties

$$(s_4 x,\ s_4 \bar{x} z), \quad (s_4 y,\ s_4 \bar{y} z), \quad (s_5 \bar{x},\ s_5 \bar{y}), \quad (s_4 c,\ t),$$

waarbij we weer voor iedere productie (v, w) ook (w, v) in T nemen. Eerst merken we op dat de equivalentie $s_1 c \equiv t x^e y^f$ geldt voor alle $e, f \geq 0$ met $e + f = d^{2^n}$. De afleiding is

$$\begin{aligned} s_1 c &\equiv s_2 c a^{d^{2^n}} \equiv s_3 c a^{d^{2^n}} x^{d^{2^n}} \equiv s_4 c x^{d^{2^n}} \equiv s_4 c \bar{x}^{d^{2^n}} z^{d^{2^n}} \\ &\equiv s_5 c \bar{x}^{d^{2^n}} \equiv s_5 c \bar{x}^e \bar{y}^f \equiv s_4 c \bar{x}^e \bar{y}^f z^{d^{2^n}} \equiv s_4 c x^e y^f \equiv t x^e y^f. \end{aligned}$$

Gebruiken we een graadrespecterende monoomordening, dan geldt $s_1 c \prec t x^e y^f$ dus $t x^e y^f \in A_T$. Stel nu dat v een echte deler van $t x^e y^f$ is. We bewijzen dat $v \notin A_T$. Als v geen factor t bevat zijn er geen producties toepasbaar op v en volgt meteen dat $v \notin A_T$. Anders heeft v de vorm $v = t x^p y^q \equiv s_4 c x^p y^q$ met $p + q < d^{2^n}$. Op $s_4 c x^p y^q$ kunnen we, naast de zinloze productie $(s_4 c,\ t)$, alleen de producties $(s_4 x,\ s_4 \bar{x} z)$ en $(s_4 y,\ s_4 \bar{y} z)$ toepassen, en producties uit de equivalenties $s_4 c \equiv s_3 c a^{d^{2^n}}$ en $s_4 c z^{d^{2^n}} \equiv s_5 c$. Door producties $(s_4 x,\ s_4 \bar{x} z)$ en $(s_4 y,\ s_4 \bar{y} z)$ neemt het aantal factoren x en y af en krijgen we hoogstens $p + q < d^{2^n}$ factoren z. Schrijf het resultaat als $s_4 c w$ met w een monoom over $\{x, y, \bar{x}, \bar{y}, z\}$. Nu zijn er twee mogelijkheden.

- We passen producties van de equivalentie $s_4 c \equiv s_3 c a^{d^{2^n}}$ toe. Andere producties zijn pas weer toepasbaar als het resultaat een factor s_4 of s_3 bevat, dus $s_3 c a^{d^{2^n}} w$ is volgens lemma 2.8. Daarop zijn verder alleen producties van de equivalentie $s_3 c x^{d^{2^n}} \equiv s_2 c$ van toepassing. Wegens $p < d^{2^n}$ geeft lemma 2.8 dat we geen monoom dat s_2 bevat kunnen afleiden. Bovendien is $s_4 c w$ zelf het enige afleidbare element dat een factor s_4 bevat.
- We passen producties van de equivalentie $s_4 c z^{d^{2^n}} \equiv s_5 c$ toe. Het aantal factoren z in w is kleiner dan d^{2^n}, dus geen monoom dat s_5 bevat is afleidbaar. Het enige afleidbare monoom dat s_4 bevat is weer $s_4 c w$ zelf.

Nalopen van deze mogelijkheden laat zien dat alle monomen die we wel kunnen afleiden grotere graad hebben dan $v = t x^p y^q$. Het volgt dat met een graadrespecterende monoomordening v het kleinste element van zijn equivalentieklasse is, zodat v niet in A_T zit. Dit geldt voor elke echte deler v van $t x^e y^f$, waar $e + f = d^{2^n}$. We concluderen dat niet alleen $t x^e y^f \in A_T$ maar zelfs $t x^e y^f \in M_T$ geldt. Dan bevat M_T meer dan d^{2^n} elementen van graad groter dan d^{2^n}. Tellen van de gebruikte variabelen en toepassing van lemma 2.6 voltooit het bewijs van stelling 2.7.

Dit resultaat geeft direct een ondergrens voor de looptijd en uitvoer van Buchbergers algoritme. Het is niet de beste grens: Yap [41] geeft bijvoorbeeld een constructie met slechts $2n + O(\sqrt{n})$ variabelen waar iedere Gröbnerbasis een element van graad groter dan d^{2^n} bevat. Deze grens is scherper, maar heeft wel dezelfde orde van grootte. Essentieel betere constructies zijn er niet: met n variabelen en voortbrengers van graad hoogstens d is er altijd een Gröbnerbasis is waarvan de elementen in graad begrensd zijn door $2(\frac{1}{2}d^2 + d)^{2^{n-1}}$. Een vergelijkbare bovengrens geldt ook voor het aantal. In het volgende hoofdstuk gaan we hier verder op in.

3 De bovengrens van Dubé

Voor de complexiteit van Buchbergers algoritme is van belang hoe groot in het algemeen een Gröbnerbasis kan zijn. We hebben al ondergrenzen gezien die dubbelexponentieel groeien in het aantal variabelen. Een belangrijke stelling van Dubé [12] geeft een vergelijkbare bovengrens: voor elk ideaal $I \subset R$ is er een Gröbnerbasis waarvan de elementen graad hoogstens $2(\frac{1}{2}d^2 + d)^{2^{n-1}}$ hebben, met d de maximale graad van voortbrengers van I en n het aantal variabelen. In dit hoofdstuk geven we een overzichtelijk bewijs van deze stelling. Op enkele punten vereenvoudigen we het bewijs van Dubé.

3.1 Homogeniteit

We beginnen met een nuttige constructie.

Definitie 3.1. Voor een ideaal $I \subset R$ en $f \in R$ heet $I : f = \{g \in R : fg \in I\}$ een *quotiëntideaal*.

Het is triviaal dat $I : f$ een ideaal is. Stel dat I wordt voortgebracht door monomen $M_1, \ldots, M_s$. Laat $x \in X$ een variabele zijn. Definieer $N_i = M_i/x$ als x een deler van M_i is, en anders $N_i = M_i$. Het is duidelijk dat $N_1, \ldots, N_s \in I : x$. Andersom geldt voor $P \in I : x$ dat xP door een M_i deelbaar is wegens propositie 1.7. Dan is P deelbaar door N_i. Er volgt $I : x = (N_1, \ldots, N_s)$. Door dit te herhalen vinden we met de regel $I : fg = (I : f) : g$ voortbrengers van $I : M$, waar M een monoom is.

Een polynoom $f \in R$ is *homogeen* als alle monomen in f dezelfde graad hebben. Elke f kunnen we schrijven als een som van homogene polynomen. Het deel van f met de termen van graad z heet de *homogene component van graad z* van f. Merk op dat f de som van zijn homogene componenten is.

Definitie 3.2. Een niet-lege deelverzameling $S \subset R$ heet *homogeen* als S een natuurlijk K-moduul is (dat wil zeggen, gesloten onder optelling en scalaire vermenigvuldiging) en voor iedere $f \in S$ ook alle homogene componenten van f in S liggen.

Van bijzonder belang zijn homogene idealen. Dit zijn precies de idealen die kunnen worden voortgebracht door homogene polynomen. Om fijne eigenschappen van homogene polynomen en idealen ook in het inhomogene geval toe te passen, gebruiken we *homogenisatie*. We voeren een extra variabele x_0 in, zodat we de polynoomring ${}^hR = K[x_0, \ldots, x_n]$ krijgen. Een polynoom $f = \sum_{i=1}^{r} a_i M_i$, met alle $a_i \in K$ en M_i monomen in R, homogeniseren we door

$$ {}^hf = \sum_{i=1}^{r} a_i x_0^{\deg(f)-\deg(M_i)} M_i. $$

Dit is een homogeen polynoom in ${}^hR$ van graad $\deg(f)$. Andersom wordt $g \in {}^hR$ gedehomogeniseerd door het polynoom ${}^ag \in R$ waarin x_0 gelijk aan 1 is gesteld. Een ideaal $I = (f_1, \ldots, f_s) \subset R$ homogeniseren we door ${}^hI = ({}^hf_1, \ldots, {}^hf_s) \subset {}^hR$. We benadrukken dat ${}^hI$ afhankelijk is van de gekozen voortbrengers: voor alle $g \in {}^hI$ geldt ${}^ag \in I$, maar voor $f \in I$ geldt alleen $x_0^k \cdot {}^hf \in {}^hI$ voor k groot genoeg, afhankelijk van de voortbrengers. Dit kunnen we vermijden door ${}^hI$ te vervangen door ${}^hI : x_0^m$, wat voor m groot genoeg het ideaal voortgebracht door $\{{}^hf : f \in I\}$ is. Hier hebben we aan ${}^hI$ genoeg.

Ten slotte homogeniseren we ook de monoomordening $\succ$. Voor monomen M en N in ${}^hR$ definiëren we $M \,{}^h\!\succ N$ als $\deg(M) > \deg(N)$, of als $\deg(M) = \deg(N)$ en ${}^aM \succ {}^aN$. Hiermee is ${}^h\!\succ$ graadrespecterend. Merk op dat geldt $\operatorname{LM}({}^hf) = x_0^k \operatorname{LM}(f)$ voor zekere $k \geq 0$.

Propositie 3.3. Zij $I = (f_1, \ldots, f_s) \subset R$ een ideaal en G een Gröbnerbasis voor ${}^hI \subset {}^hR$ ten opzichte van ${}^h\!\succ$, met alle $g \in G$ homogeen. Dan is $\{{}^ag : g \in G\}$ een Gröbnerbasis voor I ten opzichte van $\succ$.

Bewijs. Neem $f \in I$. Voor m groot genoeg geldt $x_0^m \cdot {}^hf \in {}^hI$. In het bijzonder is er een $k \geq 0$ met $x_0^k \operatorname{LM}(f) \in \operatorname{LM}({}^hI)$, dus er is een $g \in G$ met $\operatorname{LM}(g) \mid x_0^k \operatorname{LM}(f)$. Omdat g homogeen is geldt dan $\operatorname{LM}({}^ag) \mid \operatorname{LM}(f)$. Uit $\{{}^ag : g \in G\} \subset I$ volgt dat dit een Gröbnerbasis voor I is. □

Van een homogene deelverzameling $S \subset R$ kunnen we het deel $S_z \subset S$ nemen van homogene polynomen van graad z. Dan is S_z een eindigdimensionale K-vectorruimte.

Definitie 3.4. De *Hilbertfunctie* H_S van een homogene deelverzameling $S \subset R$ wordt gegeven door $H_S(z) = \dim(S_z)$.
Let op: voor homogene idealen $I \subset R$ wordt elders vaak $\dim((R/I)_z)$ in plaats van $\dim(I_z)$ gebruikt.

De Hilbertfunctie is een maat voor de grootte van S. Als $S = T_1 \oplus T_2$ een directe som van homogene verzamelingen is, dan geldt $H_S = H_{T_1} + H_{T_2}$. Een beroemde stelling zegt dat $H_I(z)$ een polynoom is voor z voldoende groot, waar $I \subset R$ een homogeen ideaal is [4, Theorem 9.27]. Dat gebeurt eveneens bij de homogene verzameling nf_I, de verzameling normaalvormen ten opzichte van een Gröbnerbasis voor I. Dit zijn precies de polynomen waarvan geen monoom in $(\textsc{lm}(I))$ ligt. Uit stelling 1.5 volgt direct $R = I \oplus \mathrm{nf}_I$. We zien eenvoudig dat nf_I een representantenstelsel voor de quotiëntring R/I is.

3.2 Kegeldecomposities

Homogene verzamelingen bestuderen we aan de hand van eenvoudige bouwstenen.

Definitie 3.5. Als $g \in R$ een homogeen polynoom is en $V \subset X = \{x_1, \ldots, x_n\}$ een deelverzameling, dan heet $c(g, V) = \{gh : h \in K[V]\}$ een *kegel*.

Merk op dat $c(g, V)$ een homogene deelverzameling van R is.

Definitie 3.6. Een *kegeldecompositie* van een homogene deelverzameling $S \subset R$ is een eindige verzameling Q van kegels, zodanig dat S de directe som van de kegels in Q is.

Met $\overline{Q}$ noteren we de deelverzameling van Q die bestaat uit de kegels $c(g, V) \in Q$ met $V \neq \varnothing$. Kegels met $V = \varnothing$ zijn zo klein dat ze vaak niet relevant zijn. We noemen twee soorten kegeldecomposities.

Definitie 3.7. Een kegeldecompositie Q met $\overline{Q} \neq \varnothing$ heet *d-standaard* als voor iedere kegel $c(g, V) \in \overline{Q}$ geldt dat $\deg(g) \geq d$ en, indien $\deg(g) > d$, er een $c(h, W) \in \overline{Q}$ is met $\deg(h) = \deg(g) - 1$ en $|W| \geq |V|$.
In het geval $\overline{Q} = \varnothing$ heet Q een 0-standaard kegeldecompositie.
We noemen Q verder *d-exact* als Q ten eerste d-standaard is en bovendien voor verschillende kegels $c(g, V)$ en $c(h, W)$ in $\overline{Q}$ altijd geldt $\deg(g) \neq \deg(h)$.
We merken op dat deze definities enigszins afwijken van die in [12]: daar is een kegeldecompositie Q met $\overline{Q}$ leeg d-standaard voor iedere $d \in \mathbb{N}$, en heet Q kortweg exact als deze d-exact is voor zekere d.

Als Q een d-standaard kegeldecompositie is en $\overline{Q}$ niet leeg, dan is d de kleinste graad van een polynoom g waarvoor er een kegel $c(g, V) \in \overline{Q}$ is. Er volgt dat d altijd uniek bepaald is.

Definitie 3.8. Laat Q een d-standaard kegeldecompositie zijn. Met Q associëren we een rij *Macaulay constanten* $b_0 \geq b_1 \geq \ldots \geq b_{n+1} = d$ gegeven door

$$b_i = \min\{e \geq d : \text{als } c(g, V) \in Q \text{ met } |V| \geq i, \text{ dan geldt } \deg(g) < e\}.$$

Bijvoorbeeld is $b_1 - 1$ de grootste graad van een polynoom $g \in R$ waarvoor er een $c(g, V) \in \overline{Q}$ is. Wanneer Q zelfs d-exact is, bevatten de Macaulay constanten $\overline{Q}$ veel informatie van Q.

Propositie 3.9. Zij Q een d-exacte kegeldecompositie met Macaulay constanten $b_0, \ldots, b_{n+1}$. Voor $i = 1, \ldots, n$ en $e \in \mathbb{N} = \mathbb{Z}_{\geq 0}$ met $b_{i+1} \leq e < b_i$ is er een unieke kegel $c(g, V) \in \overline{Q}$ met $\deg(g) = e$. Voor die kegel geldt bovendien $|V| = i$.

Bewijs. Neem $i \in \{1, \ldots, n\}$ en $e \in \mathbb{N}$ met $b_{i+1} \leq e < b_i$. Uit $b_{i+1} < b_i$ volgt dat er een kegel $c(h, W) \in \overline{Q}$ is met $\deg(h) = b_i - 1$ en $|W| = i$. Maar Q is d-standaard en er geldt $d \leq e \leq b_i - 1$, dus er is een kegel $c(g, V) \in \overline{Q}$ met $\deg(g) = e$ en $|V| \geq |W| = i$. Uniciteit geldt direct omdat Q exact is. Verder moet gelden dat $|V| = i$, want $|V| \geq i + 1$ zou betekenen dat $e < b_{i+1}$. □

Een van de doelen van deze paragraaf is om de volgende stelling te bewijzen. Deze stelling laat het verband tussen kegeldecomposities en Gröbnerbases zien.

Stelling 3.10. Zij $I \subset R$ een homogeen ideaal. Er is een 0-exacte kegeldecompositie van nf_I met Macaulay constanten $b_0, \ldots, b_{n+1}$, zodanig dat er een Gröbnerbasis voor I is waarvan de elementen graad hoogstens b_0 hebben.

We gaan dus zo'n kegeldecompositie van nf_I construeren. Het is voldoende om monoomidealen te beschouwen vanwege de triviale gelijkheid $\mathrm{nf}_I = \mathrm{nf}_{(\mathrm{LM}(I))}$. Het volgende algoritme is eenvoudiger dan dat in [12, §4], en we geven een nieuw terminatiebewijs.

Algoritme 3.11 (Decompositie).
Invoer: een eindige verzameling F van monomen, een monoom M en een deelverzameling $V \subset X$.
Uitvoer: kegeldecompositie Q van $\mathrm{nf}_{(F)} \cap c(M, V)$ die, indien $\overline{Q}$ niet leeg is, $\deg(M)$-standaard is.

$G :=$ `gereduceerde Gröbnerbasis voor` $(F) : M$`;`
`if` $1 \in G$ `then return` $\varnothing$`;`
`else if` $G \cap K[V] = \varnothing$ `then return` $\{c(M, V)\}$`;`
`else`
  `kies` $W \subset V$ `met` $|W|$ `maximaal zodanig dat` $G \cap K[W] = \varnothing$`;`
  `kies` $x \in V \setminus W$`;`
  $Q_1 :=$ `Decompositie(`F`,`M`,`$V \setminus \{x\}$`);`
  $Q_2 :=$ `Decompositie(`F`,`xM`,`V`);`
  `return` $Q_1 \cup Q_2$`;`

Stelling 3.12. Het decompositiealgoritme termineert en is correct.

Bewijs. We noteren $I = (F)$. In de eerste recursieve aanroep wordt $|V|$ kleiner. Bij de tweede aanroep wordt het ideaal $I : M$ groter. Immers, de keuze van W en x is dusdanig dat er een $g \in G$ is die deelbaar is door x. Nu geldt $g/x \in I : xM$ maar $g/x \notin I : M$ omdat G gereduceerd is. Er volgt $I : M \subsetneq I : xM$. Omdat R noethers is termineert het algoritme.

In het geval $1 \in G$ geldt $M \in I$ zodat $c(M, V)$ bevat is in I en $\mathrm{nf}_I \cap c(M, V)$ gelijk is aan $\{0\}$, wat de lege verzameling als kegeldecompositie heeft. Stel nu dat geldt $G \cap K[V] = \varnothing$. Neem $MN \in c(M, V)$ met $N \in K[V]$ een monoom, dan is N niet deelbaar door een element van G. Er volgt $N \notin I : M$ en $MN \notin I$, zodat geldt $MN \in \mathrm{nf}_I$. We concluderen dat $c(M, V) \subset \mathrm{nf}_I$ en dat $\{c(M, V)\}$ een $\deg(M)$-standaard kegeldecompositie van $\mathrm{nf}_I \cap c(M, V) = c(M, V)$ is (tenzij $V = \varnothing$).

Anders kunnen we met inductie naar de recursiediepte aannemen dat Q_1 en Q_2 respectievelijk $\deg(M)$- en $(\deg(M) + 1)$-standaard zijn (tenzij $\overline{Q}_1$ of $\overline{Q}_2$ leeg is). Uit $c(M, V) = c(M, V \setminus \{x\}) \oplus c(xM, V)$ volgt direct dat $Q_1 \cup Q_2$ een kegeldecompositie van $\mathrm{nf}_I \cap c(M, V)$ is. Merk nu op dat Q_1 niet leeg is. In de keten onderliggende 'Q_1-recursies' verandert namelijk M en dus G niet. Het geval $1 \in G$ kan niet optreden dus ooit wordt een kegel $c(M, Y)$ toegevoegd. Om te bewijzen dat $Q_1 \cup Q_2$ ook $\deg(M)$-standaard is, hoeven we daarom alleen nog te kijken naar kegels $c(N, Z) \in \overline{Q}_2$ waarvoor geldt $\deg(N) = \deg(M) + 1$. Die voldoen aan $c(N, Z) \subset \mathrm{nf}_I \cap c(M, V)$. Delers van monomen in nf_I liggen ook in nf_I, zodat volgt $c(M, Z) \subset \mathrm{nf}_I \cap c(M, V)$. Nu hebben we $Z \subset V$ en $G \cap K[Z] = \varnothing$. Immers, $P \in G \cap K[Z]$ zou voldoen aan $PM \in I$ en $PM \in c(M, Z) \subset \mathrm{nf}_I$, wat niet kan. De kegel $c(M, Y) \in Q_1$ van hierboven heeft $|Y| \geq |Z|$ omdat het algoritme $|W|$ steeds maximaal kiest. Dus $Q_1 \cup Q_2$ is $\deg(M)$-standaard. □

Hiermee vinden we altijd een 0-standaard kegeldecompositie van $\mathrm{nf}_I = \mathrm{nf}_I \cap c(1, X)$ aangezien de lege kegeldecompositie ook 0-standaard is. We hebben nog de volgende constructie nodig. Deze is intuïtiever dan de oorspronkelijke constructie in [12, §6].

Lemma 3.13. Laat $S \subset R$ een homogene deelverzameling. Als S een d-standaard kegeldecompositie heeft, dan heeft S ook een d-exacte kegeldecompositie.

Bewijs. Zij Q een d-standaard kegeldecompositie van S. Noem z de kleinste graad waarvoor er verschillende kegels $c(g, V)$ en $c(h, W)$ in $\overline{Q}$ zijn met $\deg(g) = \deg(h) = z$. Stapsgewijs verhogen we z. Kies daartoe een $c(h, W) \in \overline{Q}$ met $\deg(h) = z$ zodanig dat $|W|$ maximaal is. Voor elke kegel $c(g, V)$, waar we zonder verlies van algemeenheid $V = \{x_1, \ldots, x_i\}$ nemen, geldt de identiteit

$$c(g, V) = c(g, \varnothing) \oplus c(x_1 g, \{x_1, \ldots, x_i\}) \oplus c(x_2 g, \{x_2, \ldots, x_i\}) \oplus \ldots \oplus c(x_i g, \{x_i\}). \tag{3}$$

Vervang alle kegels $c(g, V) \in \overline{Q} \setminus \{c(h, W)\}$ met $\deg(g) = z$ door de kegels in het bijbehorende rechterlid. Vanwege de keuze van $c(h, W)$ is de resulterende kegeldecompositie weer d-standaard en $c(h, W)$ is de enige kegel in $\overline{Q}$ met $\deg(h) = z$. Dit herhalend kunnen we z steeds groter maken.

We bewijzen dat dit proces stopt. Laat $b_0, \ldots, b_{n+1}$ de Macaulay constanten van de oorspronkelijke kegeldecompositie zijn en herhaal de constructie tot $z = b_1 - 1$. Noem op dat moment k het aantal kegels $c(g, V)$ met $\deg(g) = b_1 - 1$ waarvoor $|V|$ maximaal is. Laat t deze maximale waarde van $|V|$ zijn. Als we het proces weer een stap toepassen voegen we aan $\overline{Q}$ alleen kegels $c(h, W)$ toe met $\deg(h) = b_1$. Maar $\overline{Q}$ bevatte nog geen dergelijke kegels, dus $\overline{Q}$ bevat daarna precies $k - 1$ kegels $c(h, W)$ met $\deg(h) = b_1$ en $|W| = t$. Na k iteraties zijn er geen kegels $c(h, W)$ meer met $\deg(h) = b_1 + k - 1$ en $|W| = t$. Evenzo zijn er na eindig veel iteraties geen kegels meer met $|W| = t - 1$. Dit voortzettend concluderen we dat de constructie termineert. □

Bewijs stelling 3.10. Laat Q de 0-standaard kegeldecompositie van $\mathrm{nf}_I = \mathrm{nf}_{(\mathrm{LM}(I))}$ zijn die het decompositiealgoritme geeft wanneer toegepast op $(\mathrm{LM}(I))$. Noteer met $a_0, \ldots, a_{n+1}$ de Macaulay constanten van Q. Zij H een minimale Gröbnerbasis voor I bestaande uit homogene polynomen. We bewijzen dat $\deg(g) \leq a_0$ geldt voor alle $g \in H$. Laat daartoe $N \in \mathrm{LM}(H)$. We doorlopen de recursieve aanroepen van het algoritme zodanig dat steeds geldt $N \in c(M, V)$, in de notatie van het algoritme. Dit kan, want uit $N \in c(M, V)$ volgt $N \in c(M, V \setminus \{x\})$ of $N \in c(xM, V)$. Deze keten aanroepen stopt op een gegeven moment met een aanroep `Decompositie(`F`,`M`,`V`)`. Dan geldt de conditie $1 \in G$ of $G \cap K[V] = \varnothing$. Dat laatste kan niet: als in het bewijs van stelling 3.12 geldt dan $c(M, V) \subset \mathrm{nf}_I$, maar dat is in tegenspraak met $N \in c(M, V) \cap (\mathrm{LM}(I))$. Dus we hebben $1 \in G$, zodat geldt $c(M, V) \subset (\mathrm{LM}(I))$. De minimaliteit van H impliceert dat geen deler van N bevat is in $(\mathrm{LM}(I))$, dus er volgt $M = N$.

We beschouwen de aanroep `Decompositie(`F`,`M`,`V`)`. Wanneer geldt $M = 1$ en $V = X$, dan hebben we $N = 1$ dus $I = R$. De claim dat voor alle $g \in H$ geldt $\deg(g) \leq a_0$ is dan triviaal. Anders moet dit een 'Q_2-aanroep' zijn (of de conditie $1 \in G$ zou al eerder hebben gegolden). De corresponderende 'Q_1-aanroep' is `Decompositie(`F`,`M/x`,`$V \setminus \{x\}$`)` voor een zekere variabele x. De uitvoer bevat dus een kegel $c(M/x, W)$. In het bijzonder geldt $a_0 \geq \deg(M/x) + 1 = \deg(N)$. De elementen van $\mathrm{LM}(H)$ zijn dus in graad begrensd door a_0 en wegens homogeniteit de elementen van H ook.

Construeer als in lemma 3.13 uit Q een 0-exacte kegeldecompositie van nf_I. Uit het bewijs zien we direct dat de Macaulay constanten $b_0, \ldots, b_{n+1}$ van deze nieuwe kegeldecompositie voldoen aan $b_i \geq a_i$. De elementen van H hebben dus graad hoogstens b_0. □

Ten slotte geven we ook een kegeldecompositie van homogene idealen.

Lemma 3.14. Zij $I \subset R$ een niet-nul ideaal met homogene voortbrengers van graad hoogstens d. Dan is er een d-exacte kegeldecompositie van I.

Bewijs. Laat $f_1, \ldots, f_s$ de voortbrengers zijn. Definieer $J = (f_2, \ldots, f_s) : f_1$ en $S = \{gf_1 : g \in \mathrm{nf}_J\}$. We bewijzen dat geldt $I = S \oplus (f_2, \ldots, f_s)$. Het is duidelijk dat S en $(f_2, \ldots, f_s)$ deelverzamelingen van I zijn. Voor $f \in I$ kunnen we altijd $f = gf_1 + h$ schrijven met $h \in (f_2, \ldots, f_s)$. Neem een Gröbnerbasis G voor J. Dan geldt $g - \mathrm{nf}_G(g) \in J$ en dus $(g - \mathrm{nf}_G(g))f_1 \in (f_2, \ldots, f_s)$. Nu hebben we

$$\mathrm{nf}_G(g)f_1 \in S \qquad \text{en} \qquad f - \mathrm{nf}_G(g)f_1 = (g - \mathrm{nf}_G(g))f_1 + h \in (f_2, \ldots, f_s).$$

Daarmee ligt f in $S + (f_2, \ldots, f_s)$ en het resteert te bewijzen dat $S \cap (f_2, \ldots, f_s) = \{0\}$. Maar een element $gf_1 \in S$, met $g \in \mathrm{nf}_J$, ligt in $(f_2, \ldots, f_s)$ precies wanneer $g \in J$. Uit $J \cap \mathrm{nf}_J = \{0\}$ concluderen we dat inderdaad geldt $I = S \oplus (f_2, \ldots, f_s)$.

Met het decompositiealgoritme vinden we een 0-standaard kegeldecompositie P van nf_J. We zien meteen dat $\{c(gf_1, V) : c(g, V) \in P\}$ een $\deg(f_1)$-standaard kegeldecompositie van $S = \mathrm{nf}_J \cdot f_1$ is (tenzij $\overline{P} = \varnothing$). Deze constructie herhalend schrijven we $I = S_1 \oplus \ldots \oplus S_{s-1} \oplus (f_s)$. Voor iedere S_i bestaat een $\deg(f_i)$-standaard kegeldecompositie P_i en voor (f_s) nemen we de $\deg(f_s)$-standaard kegeldecompositie $\{c(f_s, X)\}$. Met de uitdrukking in (3) kunnen we een e-standaard kegeldecompositie eenvoudig omzetten in een $(e+1)$-standaard kegeldecompositie. Het volgt dat $S_1, \ldots, S_{s-1}$ en (f_s) ook een d-standaard kegeldecompositie hebben. De vereniging Q hiervan is een d-standaard kegeldecompositie van I. Merk hier op dat sommige $\overline{P_i}$ leeg kunnen zijn, maar $\overline{Q}$ niet omdat $I \neq \{0\}$. Uit lemma 3.13 volgt ten slotte dat S een d-exacte kegeldecompositie heeft. □

3.3 Een grens voor de Macaulay constanten

De Hilbertfunctie van een kegel $c(g, V)$ met $V \neq \varnothing$ is de binomiaalcoëfficiënt

$$H_{c(g,V)}(z) = \binom{z - \deg(g) + |V| - 1}{|V| - 1}$$

voor $z \geq \deg(g)$: de elementen gM, waarbij M een monoom in $K[V]$ is van graad $z - \deg(g)$, vormen immers een K-basis voor $c(g, V)_z$, en dit is het aantal dergelijke monomen. In het geval $V = \varnothing$ geldt $H_{c(g,V)}(z) = 1$ voor $z = \deg(g)$ en anders 0. Als Q een d-exacte kegeldecompositie van S is met Macaulay constanten $b_0, \ldots, b_{n+1}$ dan volgt uit propositie 3.9 dat S Hilbertfunctie

$$H_S(z) = \sum_{i=1}^{n} \sum_{e=b_{i+1}}^{b_i - 1} \binom{z - e + i - 1}{i - 1}$$

heeft voor $z \geq b_0$. Merk op dat dit een polynoom in z is. Stel nu dat $I \subset R$ een niet-nul ideaal is met homogene voortbrengers van graad hoogstens d. Neem een d-exacte kegeldecompositie P van I en de 0-exacte kegeldecompositie Q van nf_I uit stelling 3.10. Noteer met $a_0, \ldots, a_{n+1}$ de Macaulay constanten van P en met $b_0, \ldots, b_{n+1}$ die van Q. Uit $R = I \oplus \mathrm{nf}_I$ volgt $H_I + H_{\mathrm{nf}_I} = H_R$ oftewel

$$\sum_{i=1}^{n} \sum_{e=a_{i+1}}^{a_i - 1} \binom{z - e + i - 1}{i - 1} + \sum_{i=1}^{n} \sum_{e=b_{i+1}}^{b_i - 1} \binom{z - e + i - 1}{i - 1} = \binom{z + n - 1}{n - 1} \tag{4}$$

voor $z \geq \max(a_0, b_0)$. Maar dan kunnen de Macaulay constanten niet te groot zijn, aangezien $a_{n+1} = d$ en $b_{n+1} = 0$ vastliggen. Het bewijs van de volgende grens is lang maar oninteressant.

Lemma 3.15. Voor $d \geq 1$ geldt $a_1 + b_1 \leq 2(\frac{1}{2}d^2 + d)^{2^{n-2}}$.

Bewijs. Dit volgt uit (4), zie [12, Lemma 8.1]. Daar wordt het alleen voor $n \geq 3$ bewezen, maar voor $n < 3$ is het triviaal. □

Merk op dat (4) een polynoomgelijkheid is voor $z \geq \max(a_1, b_1)$. Als Q een kegel $c(g, \varnothing)$ bevat met $\deg(g) \geq \max(a_1, b_1)$, dan zou $H_{\mathrm{nf}_I}(\deg(g))$ groter zijn dan de tweede term in uitdrukking (4). Maar ook is $H_I(\deg(g))$ minstens zo groot als de eerste term in uitdrukking (4), en we krijgen

$$H_I(\deg(g)) + H_{\mathrm{nf}_I}(\deg(g)) > \binom{\deg(g) + n - 1}{n - 1} = H_R(\deg(g)) = H_I(\deg(g)) + H_{\mathrm{nf}_I}(\deg(g)).$$

Uit deze tegenspraak volgt de bovengrens $b_0 \leq \max(a_1, b_1) \leq a_1 + b_1$. Volgens stelling 3.10 hebben we daarmee een grens voor de graden van polynomen die nodig zijn in een Gröbnerbasis voor I. Dit geldt alleen voor homogene idealen, maar via homogenisatie en propositie 3.3 vinden we ook een grens voor het inhomogene geval.

Stelling 3.16 (Dubé). Zij $I \subset R$ een ideaal met voortbrengers van graad hoogstens d. Dan is er een Gröbnerbasis voor I waarvan alle polynomen graad hoogstens $2(\frac{1}{2}d^2 + d)^{2^{n-1}}$ hebben. □

Een waarschuwing is hier op zijn plaats. Merk ten eerste op dat dit een existentiestelling is. In het bijzonder hoeft deze grens niet te gelden voor de uitvoer van Buchbergers algoritme. Verder beweert Dubé dat er een gereduceerde Gröbnerbasis voor I is met deze graadgrens. Maar zijn definitie van 'gereduceerd' verschilt van de gebruikelijke definitie 1.8 en komt overeen met wat wij minimaal noemen. Dit is verkeerd overgenomen in bijvoorbeeld [27, 31]. De toevoeging dat er een minimale Gröbnerbasis als in stelling 3.16 is, is een triviaal gevolg.

Uit stelling 3.16 kunnen we wel conclusies trekken over het aantal elementen van een minimale Gröbnerbasis en in het bijzonder van de gereduceerde. Dubé zelf doet dat opmerkelijk genoeg niet.

Gevolg 3.17. Zij $I \subset R$ een ideaal met voortbrengers van graad hoogstens d. Een minimale Gröbnerbasis voor I bestaat uit niet meer dan $\binom{e+n-1}{n-1}$ polynomen, met $e = 2(\frac{1}{2}d^2 + d)^{2^{n-1}}$.

Bewijs. Dit volgt direct uit propositie 1.10 en propositie 1.16. □

Merk op dat $\binom{e+n-1}{n-1}$ een polynoom in e is van graad $n - 1$. Dit geeft dus een bovengrens voor het aantal elementen van een minimale Gröbnerbasis die ook dubbelexponentieel groeit in n.

4 Een Ackermanngrens

Buchbergers algoritme voegt aan een stel voortbrengers G van een ideaal $I \subset R$ steeds meer polynomen toe. Zoals in het bewijs van stelling 1.14 ontstaan inclusies $G = G_0 \subsetneq G_1 \subsetneq \ldots$ en een keten

$$(\textsc{lm}(G_0)) \subsetneq (\textsc{lm}(G_1)) \subsetneq \ldots.$$

Omdat R noethers is, is deze keten eindig en termineert het algoritme. Een bovengrens voor de lengte van zo'n keten geeft ook een grens voor de complexiteit van Buchbergers algoritme. De lengte van deze ketens en de toepassing op Buchbergers algoritme zijn onderzocht in onder andere [35, 36, 30, 16]. Perdry leidt in zijn proefschrift [37, §I.5] een expliciete complexiteitsgrens af, in het geval van een graadrespecterende monoomordening. Deze grens is in termen van de Ackermannfunctie. Met slechts combinatorische argumenten zullen we een kleine verbetering van deze grens geven. Verder zullen we een nieuwe grens afleiden, ook uitgedrukt in de Ackermannfunctie, die geldt voor iedere monoomordening. Dit resultaat geldt geheel algemeen.

4.1 Mo

We beginnen met het bestuderen van een eenpersoonsspel, dat we *Mo* dopen. Later zullen we een keten monoomideaalinclusies reduceren tot zetten in Mo. We definiëren een *majorerende functie* als een strikt stijgende functie $\delta : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ met $\delta(d) > d$ voor alle $d \in \mathbb{Z}_{\geq 1}$. Voor een verzameling X noteren we met $X^\diamond$ de verzameling formele eindige associatieve en commutatieve sommen $m_1 \diamond \ldots \diamond m_r$ met $m_1, \ldots, m_r \in X$, inclusief de lege som. Er is een natuurlijke optelling $\diamond$ op $X^\diamond$. Hiermee is $X^\diamond$ dus de vrije abelse monoïde over X. Ook noteren we voor $k \in \mathbb{N} = \mathbb{Z}_{\geq 0}$ en $m \in X$ met $k \star m$ de som $m \diamond \ldots \diamond m$ van k kopieën van m.

Definitie 4.1. Kies een majorerende functie δ. Een *positie* in het spel Mo_δ is een paar (v, d) met $v \in \mathbb{N}^\diamond$ en $d \in \mathbb{Z}_{\geq 1}$. De positie (v, d) is een *eindpositie* als v de lege som is. Als (v, d) geen eindpositie is bestaat een *zet* uit de volgende stappen:
· kies $m \in \mathbb{N}$ en $w \in \mathbb{N}^\diamond$ met $v = m \diamond w$;
· vervang v door $k \star (m-1) \diamond w$ met $0 \leq k \leq d$ als $m > 0$, en vervang v door w als $m = 0$;
· vervang d door $\delta(d)$.

Lemma 4.2. Vanuit iedere positie in Mo_δ is er een eindige langste zettenreeks.

Bewijs. Laat (v, d) een positie zijn met $v = m_1 \diamond \ldots \diamond m_r$, waar $m_1 \geq \ldots \geq m_r$. We kennen aan deze positie het ordinaalgetal $\omega^{m_1} + \ldots + \omega^{m_r}$ toe. Het is duidelijk dat na een zet het ordinaalgetal corresponderend met de positie kleiner wordt. De ordinaalgetallen zijn welgeordend dus iedere zettenreeks is eindig. Verder zijn er in iedere positie slechts eindig veel keuzemogelijkheden voor een zet. Het lemma van König [26, §VI.2, Satz 6] geeft dat er, vanuit een gegeven positie, geen willekeurig lange zettenreeksen zijn. Dan is er vanuit elke positie een eindige langste zettenreeks. □

We kunnen dus met $L_\delta(v, d)$ de lengte van een langste Mo_δ-zettenreeks vanuit (v, d) noteren. De volgende propositie is dan triviaal.

Propositie 4.3. Voor $d, e \in \mathbb{Z}_{\geq 1}$ met $d \geq e$ geldt $L_\delta(v, d) \geq L_\delta(v, e)$. □

Zo'n langste zettenreeks kunnen we precies beschrijven. We schrijven $\alpha \to \beta$ als de posities α en β via een zet in elkaar overgaan, en $\alpha \to^* \beta$ als ze via een aantal (mogelijk nul) zetten in elkaar overgaan.

Lemma 4.4. In elke langste zettenreeks voor Mo_δ kiezen we in een positie (v, d) steeds $m \in \mathbb{N}$ en $w \in \mathbb{N}^\diamond$ met $v = m \diamond w$ zodanig dat m minimaal is. Als $m > 0$, dan vervangen we v door $d \star (m-1) \diamond w$.

Bewijs. De tweede bewering is triviaal. Neem voor de eerste een positie (v, d) en een langste zettenreeks uit (v, d) die in een zet (we mogen aannemen de eerste) m niet minimaal kiest. Schrijf $v = m \diamond w$. Laat $l < m$ een andere mogelijke keuze zijn, en neem $z \in \mathbb{N}^\diamond$ waarvoor geldt $v = m \diamond l \diamond z$. De gekozen langste zettenreeks begint met $(v, d) \to (d \star (m-1) \diamond l \diamond z,\ \delta(d))$ en heeft daarom lengte

$1 + L_\delta(d \star (m-1) \diamond l \diamond z,\ \delta(d))$. Maar omdat geldt $l \leq m-1$ kunnen we in nul of meer zetten een term $m-1$ in de formele som door l vervangen. Er volgt dat voor zekere $k \geq 2$ ook

$$(v, d) \to (m \diamond z,\ \delta(d)) \to ((d+1) \star (m-1) \diamond z,\ \delta^2(d)) \to^* (d \star (m-1) \diamond l \diamond z,\ \delta^k(d))$$

een zettenreeks is, van lengte k. Merk daarbij op dat $\delta(d) \geq d+1$. Deze reeks is te vervolgen tot lengte

$$k + L_\delta(d \star (m-1) \diamond l \diamond z,\ \delta^k(d)) \geq 2 + L_\delta(d \star (m-1) \diamond l \diamond z,\ \delta(d))$$

volgens propositie 4.3. Dat is groter dan de lengte van de langste zettenreeks, tegenspraak. □

Uit deze strategie leiden we een uitdrukking voor $L_\delta(m, d)$ af met $m \in \mathbb{N}$ en $d \in \mathbb{Z}_{\geq 1}$. Noteer daartoe

$$P_m(d) = L_\delta(m, d).$$

We zien meteen $P_0(d) = 1$. Voor $m > 0$ passen we bovenstaand lemma toe om in te zien dat de langste zettenreeks uit (m, d) er, voor geschikte $e_0, \ldots, e_d \in \mathbb{Z}_{\geq 1}$, uitziet als

$$(m, d) \to (d \star (m-1),\ e_0) \to^* ((d-1) \star (m-1),\ e_1) \to^* ((d-2) \star (m-1),\ e_2) \to^* \ldots \to^* (0 \star (m-1),\ e_d).$$

We definiëren $p_m(d, i)$ voor $0 \leq i \leq d$ als het aantal zetten van (m, d) tot $((d-i) \star (m-1),\ e_i)$. Er geldt meteen $e_i = \delta^{p_m(d,i)}(d)$. Ook is duidelijk dat geldt $p_m(d, 0) = 1$ en $p_m(d, d) = P_m(d)$. Recursief weten we dat tussen $((d-i+1) \star (m-1),\ e_{i-1})$ en $((d-i) \star (m-1),\ e_i)$ precies $P_{m-1}(e_{i-1})$ zetten liggen. We vinden dus de volgende uitdrukking voor $L_\delta(m, d)$.

Stelling 4.5. Er geldt $P_0(d) = 1$ en $P_m(d) = p_m(d, d)$ voor $m, d \in \mathbb{Z}_{\geq 1}$. Bovendien geldt

$$p_m(d, i) = \begin{cases} 1 & \text{als } i = 0, \\ k + P_{m-1}(\delta^k(d)) \quad \text{met} \quad k = p_m(d, i-1) & \text{als } 0 < i \leq d \end{cases}$$

voor alle $m, d \in \mathbb{Z}_{\geq 1}$ en $0 \leq i \leq d$. □

Bijvoorbeeld hebben we

$$L_\delta(1, d) = P_1(d) = d + 1. \tag{5}$$

Bovengrenzen voor $P_m(d)$ kunnen we nu met inductie afleiden, aangezien $k + P_{m-1}(\delta^k(d))$ stijgend is in k. Hiervoor gebruiken we het volgende.

Gevolg 4.6. Neem $m > 0$ vast en functies $Q_{m-1}(d)$ en $q_m(d, i)$ met $Q_{m-1}(d) \geq P_{m-1}(d)$ en

$$q_m(d, i) > \begin{cases} 1 & \text{als } i = 0, \\ k + Q_{m-1}(\delta^k(d)) \quad \text{met} \quad k = q_m(d, i-1) & \text{als } 0 < i \leq d \end{cases}$$

voor alle $d \in \mathbb{Z}_{\geq 1}$ en $0 \leq i \leq d$. Dan geldt $q_m(d, d) > P_m(d)$ voor $d \in \mathbb{Z}_{\geq 1}$. □

We leggen nu het verband met ketens monoomideaalinclusies. Monomen kunnen we opvatten als elementen van $\mathbb{N}^n$ via $x_1^{d_1} \cdots x_n^{d_n} \leftrightarrow (d_1, \ldots, d_n)$. De monomen die deelbaar zijn door een monoom $M = x_1^{d_1} \cdots x_n^{d_n}$ corresponderen dan precies met de punten in $\mathbb{N}^n$ waarvan alle coördinaten minstens zo groot als die van M zijn. Het complement hiervan is de vereniging over de $\deg(M)$ hypervlakken gegeven door $x_i = e$, voor $0 \leq e < d_i$. Zo vinden we de volgende grens.

Lemma 4.7. Laat δ een majorerende functie zijn en $d \in \mathbb{Z}_{\geq 1}$. Stel dat $M_0, \ldots, M_t \in R$ een rij monomen is waarin M_i geen deler van M_j is voor $0 \leq i < j \leq t$ en bovendien geldt $\deg(M_i) \leq \delta^i(d)$. Dan geldt $t < L_\delta(n, d)$.

Bewijs. We definiëren een *m-dimensionale deelruimte* van $\mathbb{N}^n$ als een deelverzameling waarin $n-m$ coördinaten vast liggen en de andere coördinaten door heel $\mathbb{N}$ lopen. Voor $i = 0, \ldots, t+1$ construeren we inductief een verzameling A_i van deelruimten van $\mathbb{N}^n$ met de eigenschap dat $\{M_i, \ldots, M_t\}$ bevat is in $\bigcup A_i = \bigcup_{S \in A_i} S$. We beginnen met $A_0 = \{\mathbb{N}^n\}$, wat zeker deze eigenschap heeft. Voor $0 \leq i \leq t$ maken we A_{i+1} als volgt uit A_i. Neem $S \in A_i$ met $M_i \in S$. Dat kan wegens $M_i \in \bigcup A_i$. Als $\dim(S) = 0$, dan geldt $S = \{M_i\}$ en voldoet $A_{i+1} = A_i \setminus \{S\}$. Anders schrijven we de verzameling monomen in S die niet deelbaar zijn door M_i als de vereniging over hoogstens $\deg(M_i) \leq \delta^i(d)$ hypervlakken in S. Deze hypervlakken zijn deelruimten van $\mathbb{N}^n$ van dimensie $\dim(S) - 1$. Laat B de verzameling van deze

hypervlakken zijn en neem $A_{i+1} = (A_i \cup B) \setminus \{S\}$. Dan geldt $\{M_{i+1}, \ldots, M_t\} \subset \bigcup A_{i+1}$. Immers, alle $M_j \in S$ met $j > i$ zijn niet deelbaar door M_i en dus bevat in een element van B.

Bij $A_i = \{S_1, \ldots, S_r\}$ nemen we $v_i = \dim(S_1) \diamond \ldots \diamond \dim(S_r) \in \mathbb{N}^\diamond$. We krijgen A_{i+1} uit A_i door een deelruimte S uit A_i te verwijderen en er hoogstens $\delta^i(d)$ van dimensie $\dim(S) - 1$ toe te voegen, zodat

$$(v_0,\ d) \to (v_1,\ \delta(d)) \to (v_2,\ \delta^2(d)) \to \ldots \to (v_{t+1},\ \delta^{t+1}(d))$$

een Mo_δ-zettenreeks vanuit $(v_0, d) = (n, d)$ is met $t + 1$ zetten. Er volgt dat $t < L_\delta(n, d)$. □

Met $I_i = (M_0, \ldots, M_i)$ is $\{0\} \subsetneq I_0 \subsetneq I_1 \subsetneq \ldots \subsetneq I_t$ een keten strikte ideaalinclusies volgens propositie 1.7. Het is niet moeilijk in te zien dat de ketens die we op deze manier uit een rij monomen construeren zelfs de langst mogelijke ketens ideaalinclusies zijn: onder alle ketens ideaalinclusies met de eigenschap dat het i^{de} ideaal I_i kan worden voortgebracht door polynomen van graad hoogstens $\delta^i(d)$ zijn deze ketens het langst [36, §3]. Dit lemma geeft dus in het algemeen een bovengrens voor de lengte van een keten ideaalinclusies.

4.2 Graadrespecterende monoomordeningen

We geven eerst een grens voor de uitvoer van Buchbergers algoritme in het eenvoudigere geval dat de monoomordening $\succ$ graadrespecterend is. Via propositie 1.15 geeft dat ook een grens op de looptijd. Neem polynomen $f_1, \ldots, f_s \in R$ van graad hoogstens d als invoer en stel dat hieraan tijdens de executie $g_1, \ldots, g_t$ worden toegevoegd. Elke g_i is een gereduceerd S-polynoom van eerdere polynomen. Dit S-polynoom heeft graad hooguit tweemaal de graad van $f_1, \ldots, f_s, g_1, \ldots, g_{i-1}$. Tijdens het reduceren wordt het leidende monoom alleen kleiner ten opzichte van $\succ$ en dus, omdat $\succ$ graadrespecterend is, niet groter in graad. We concluderen dat g_i graad hoogstens $2^i d$ heeft. Laten we nu $M_i = \mathrm{LM}(g_i)$ zijn voor $1 \leq i \leq t$ en bovendien $M_0 = \mathrm{LM}(f_1)$, dan geldt ook $\deg(M_i) \leq 2^i d$. Merk op dat het geen zin heeft om de leidende monomen van $f_2, \ldots, f_s$ in deze rij op te nemen aangezien we daartussen geen relaties voor graad en deelbaarheid kennen. Daarentegen is elke g_i gereduceerd ten opzichte van $f_1, g_1, \ldots, g_{i-1}$, zodat M_i niet deelbaar is door een eerder monoom uit de rij. Met de majorerende functie $\delta(d) = 2d$ kunnen we dus lemma 4.7 toepassen om t te begrenzen.

Eerst voeren we *Knuth pijlnotatie* in om grote getallen te noteren. De Knuthpijl is een ternaire operator $a \uparrow^m b$ voor $a, b \in \mathbb{N}$ en $m \geq -2$ die recursief gedefinieerd wordt door

$$a \uparrow^m b = \begin{cases} b + 1 & \text{als } m = -2, \\ a & \text{als } m = -1 \text{ en } b = 0, \\ 0 & \text{als } m = 0 \text{ en } b = 0, \\ 1 & \text{als } m > 0 \text{ en } b = 0, \\ a \uparrow^{m-1} (a \uparrow^m (b - 1)) & \text{anders.} \end{cases}$$

We spreken af dat de Knuthpijl rechtsassociatief werkt, dan geldt voor $m \geq 0$ ook

$$a \uparrow^m b = \underbrace{a \uparrow^{m-1} a \uparrow^{m-1} \cdots \uparrow^{m-1} a}_{b \text{ maal } a}.$$

Bij vaste a en m kunnen we $a \uparrow^m$ opvatten als operator op b. Intuïtief is $a \uparrow^m b$ dus de $(b-1)$-voudige toepassing van $a \uparrow^{m-1}$ op a. Herhaalde toepassing van deze operator noteren we voor het gemak als

$$a \uparrow_i^m b = \underbrace{a \uparrow^m a \uparrow^m \cdots a \uparrow^m}_{i \text{ maal } a \uparrow^m} b.$$

Enkele kleine gevallen zijn $a \uparrow^{-2} b = b + 1$, $a \uparrow^{-1} b = a + b$, $a \uparrow^0 b = ab$, $a \uparrow b = a \uparrow^1 b = a^b$ en $a \uparrow\uparrow b = a \uparrow^2 b = a^{a^{\cdots^a}}$, waar het aantal a's gelijk is aan b. Merk op dat we voor kleine m soms m pijlen noteren in plaats van $\uparrow^m$. Verder spreken we af dat in het evalueren van uitdrukkingen de Knuthpijl lagere prioriteit heeft dan vermenigvuldiging, maar hogere dan optelling. Er geldt dus $a \uparrow^m b \cdot c + k = (a \uparrow^m (b \cdot c)) + k$.

Sterk gerelateerd aan de Knuthpijl is de *Ackermannfunctie*. Meestal wordt deze gegeven door

$$A(m,b) = \begin{cases} b+1 & \text{als } m = 0, \\ A(m-1,1) & \text{als } m > 0 \text{ en } b = 0, \\ A(m-1, A(m,b-1)) & \text{anders} \end{cases}$$

voor $m, b \in \mathbb{N}$. De Ackermannfunctie is het standaardvoorbeeld van een recursieve functie die niet primitief recursief is [1, §3]. Met inductie bewijzen we zonder moeite dat ook geldt

$$A(m,b) = 2 \uparrow^{m-2} (b+3) - 3.$$

We geven nu zonder bewijs enkele eenvoudige afschattingen die we veel zullen gebruiken.

Lemma 4.8. De volgende ongelijkheden gelden.
(a) Voor $k \leq m$ en $b \geq 2$ geldt $2 \uparrow^k b \leq 2 \uparrow^m b$.
(b) Voor $k \leq m$ en $b \geq 0$ geldt $2 \uparrow^k 2 \uparrow^m b \leq 2 \uparrow^m 2 \uparrow^k b$.
(c) Voor $m \geq 1$ en $b \geq 0$ geldt $b+1 \leq 2 \uparrow^m b$, en voor $b \geq 2$ geldt $b+2 \leq 2 \uparrow^m b$.
(d) Voor $m \geq 1$ en $b \leq c$ geldt $2 \uparrow^m b + 2 \uparrow^m c \leq 2 \uparrow^m (c+1)$.
(e) Voor $m \geq 1$ en $b, c \geq 0$ geldt $(2 \uparrow^m b)(2 \uparrow^m c) \leq 2 \uparrow^m (b+c)$.
(f) Voor $m \geq -2$, $i \geq 0$ en $b \leq 2 \uparrow^{m+1} c$ geldt $2 \uparrow_i^m b \leq 2 \uparrow^{m+1} (c+i)$. In het bijzonder geldt voor $m \geq 0$, $i \geq 0$ en $b \geq 0$ dat $2 \uparrow_i^m 4b \leq 2 \uparrow^{m+1} (b+i+1)$ en $2 \uparrow_i^m 8b \leq 2 \uparrow^{m+1} (b+i+2)$. □

In de bewijzen van stellingen 4.9, 4.10 en 4.11 verwijzen we met (a)–(f) naar deze regels. Een typische afschatting is $b+2 \uparrow^m b \leq 2 \uparrow^m (b-1) + 2 \uparrow^m b \leq 2 \uparrow^m (b+1)$ wegens (c) en (d). De tussenstap schrijven we meestal niet op.

Stelling 4.9. Laat de invoer van Buchbergers algoritme bestaan uit polynomen in $R = K[x_1, \ldots, x_n]$ van graad hoogstens $d \geq 1$ en gebruik een graadrespecterende monoomordening. Dan voegt het algoritme hieraan minder dan $A(n+2, 2d-1)$ polynomen toe, elk van graad kleiner dan $2^{A(n+2,2d-1)}$.

Bewijs. We hoeven alleen nog te bewijzen dat geldt $P_n(d) < Q_n(d)$, met $\delta(d) = 2d$ en

$$Q_n(d) = 2 \uparrow^n (2d+2) - 2 - d = A(n+2, 2d-1) + 1 - d.$$

De grens op het aantal volgt dan direct en via (c) zijn de graden kleiner dan $2^{Q_n(d)} d \leq 2^{A(n+2,2d-1)}$. De ongelijkheid $P_n(d) < Q_n(d)$ is duidelijk voor $n \leq 1$. Bij $n = 2$ laten we $Q_1'(d) = d+1$ en $q_2(d,i) = 2 \uparrow_i 5d - 2 - d$. We zien dat $q_2(d,0) = 4d - 2 > 1$ en verder

$$\begin{aligned} q_2(d, i-1) + Q_1'(2^{q_2(d,i-1)} d) &\overset{\text{(c)}}{\leq} (2 \uparrow_{i-1} 5d+1) + 2^{2 \uparrow_{i-1} 5d-3} - 2 - d \\ &\overset{\text{(c)}}{<} 2^{2 \uparrow_{i-1} 5d-1} + 2^{2 \uparrow_{i-1} 5d-3} - 2 - d \overset{\text{(d)}}{<} 2^{2 \uparrow_{i-1} 5d} - 2 - d = 2 \uparrow_i 5d - 2 - d = q_2(d,i) \end{aligned}$$

voor $i > 0$. Volgens (5) geldt $Q_1'(d) = P_1(d)$, zodat uit gevolg 4.6 volgt dat

$$P_2(d) < q_2(d,d) = 2 \uparrow_d 5d - 2 - d \overset{\text{(f)}}{<} 2 \uparrow\uparrow (2d+2) - 2 - d = Q_2(d).$$

Voor $n > 2$ bewijzen we nu met inductie dat $P_n(d) < Q_n(d)$. Laat $q_n(d,i) = 2 \uparrow_i^{n-1} (5d+i) - 2 - d$ zijn. Weer geldt er $q_n(d,0) = 4d - 2 > 1$. Voor $i > 0$ en $k = q_n(d, i-1)$ hebben we

$$\begin{aligned} k + Q_{n-1}(2^k d) &\overset{\text{(c)}}{\leq} k + 2 \uparrow^{n-1} (2^{k+d} + 2) - 2 - d \overset{\text{(c),(d)}}{<} 2 \uparrow^{n-1} (2^{k+d} + 3) - 2 - d \\ &= 2 \uparrow^{n-1} (2^{2 \uparrow_{i-1}^{n-1} (5d+i-1) - 2} + 3) - 2 - d < 2 \uparrow^{n-1} 2^{2 \uparrow_{i-1}^{n-1} (5d+i-1)} - 2 - d \\ &\overset{\text{(a),(f)}}{\leq} 2 \uparrow^{n-1} 2 \uparrow_{i-1}^{n-1} (5d+i) - 2 - d = 2 \uparrow_i^{n-1} (5d+i) - 2 - d = q_n(d,i). \end{aligned}$$

Ten slotte merken we op dat geldt

$$q_n(d,d) = 2 \uparrow_d^{n-1} 6d - 2 - d \overset{\text{(f)}}{<} 2 \uparrow^n (2d+2) - 2 - d = Q_n(d).$$

Met gevolg 4.6 en inductie volgt de stelling. □

Deze stelling is een verscherping van het resultaat van Perdry [37, §I.5, Proposition 60]. Hij vindt een bovengrens $A(n+2, \lambda_n d)$ voor het aantal toegevoegde polynomen, waar λ_n een constante is die alleen van n afhangt. Hier zien we dat $\lambda_n = 2$ in feite voldoende is. Met een analoog bewijs krijgen we voor $k \in \mathbb{Z}_{\geq 1}$ en $\varepsilon = \frac{1}{k}$ de iets scherpere grens $A(n+2, \lfloor (1+\varepsilon)d \rfloor + k - 2)$. Zelfs $\lambda_n = \frac{3}{2}$ is dus genoeg.

4.3 Het algemene geval

Het argument in de vorige paragraaf berust op het feit dat de toegevoegde polynomen in graad steeds niet meer dan verdubbelen. Bij willekeurige monoomordeningen hoeft dit niet het geval te zijn. Toch kunnen we ook dan een dergelijke grens vinden. Beschouw een polynoom $f \in R$ van graad hoogstens d en polynomen $g_1, \ldots, g_s \in R \setminus \{0\}$ van graad hoogstens e. Bij de deling van f door $g_1, \ldots, g_s$ vinden we deelresultaten $f = f_0, f_1, \ldots, f_t$ overeenkomstig de iteraties van algoritme 1.3. Elke stap is een delingsstap, waarin de graad met maximaal e toeneemt, of een reststap, waarin de graad niet groter wordt. Met $M_i = \text{LM}(f_i)$ en $\delta(d) = d + e$ volgt dat $\deg(M_i) \leq \delta^i(d)$. Bovendien geldt voor $i < j$ dat $M_i \succ M_j$ dus kan M_i geen deler zijn van M_j. We passen weer lemma 4.7 toe.

Stelling 4.10. Met $f \in R = K[x_1, \ldots, x_n]$ van graad hoogstens d en $g_1, \ldots, g_s \in R \setminus \{0\}$ van graad hoogstens e als invoer voert het delingsalgoritme 1.3 minder dan $2 \uparrow^{n-1} (d+1)(e+1)$ iteraties uit.

Bewijs. De gevallen $d = 0$ en $e = 0$ zijn triviaal. Laat anders $\delta(d) = d + e$ en

$$Q_n(d) = 2 \uparrow^{n-1} (d+1)(e+1).$$

Het is voldoende te bewijzen dat $P_n(d) < Q_n(d)$. Voor $n \leq 1$ is dit duidelijk. Bij $n = 2$ bewijzen we met inductie de uitdrukking $p_2(d,i) = (e+1)^i + (d+1)\sum_{j=0}^{i-1}(e+1)^j$. Uit stelling 4.5 volgt dan dat

$$P_2(d) = p_2(d,d) = (e+1)^d + (d+1)\sum_{j=0}^{d-1}(e+1)^j = (e+1)^d + (d+1)\frac{(e+1)^d - 1}{e}$$

$$< (d+2)(e+1)^d \overset{\text{(c)}}{\leq} 2^{d+1}(2^e)^d < 2^{(d+1)(e+1)} = Q_2(d).$$

Voor $n > 2$ nemen we $q_n(d,i) = 2 \uparrow_{i+1}^{n-2} (d+3i)e$. Merk op dat geldt $q_n(d,0) = 2 \uparrow^{n-2} de > 1$ volgens (c). Bovendien geldt voor $i > 0$ en $k = q_n(d, i-1)$ de afschatting

$$\begin{aligned} k + Q_{n-1}(d+ke) &= k + 2 \uparrow^{n-2} (d+ke+1)(e+1) \overset{\text{(c),(d)}}{<} 2 \uparrow^{n-2} (d+ke)(e+2) \\ &\overset{\text{(c),(e)}}{\leq} 2 \uparrow^{n-2} (d + 2 \uparrow_i^{n-2} [(d+3i-2)e - 1])(e+2) \overset{\text{(c),(d)}}{<} 2 \uparrow^{n-2} (2 \uparrow_i^{n-2} (d+3i-2)e)(e+2) \\ &\overset{\text{(c),(e)}}{\leq} 2 \uparrow^{n-2} 2 \uparrow_i^{n-2} (d+3i)e = 2 \uparrow_{i+1}^{n-2} (d+3i)e = q_n(d,i). \end{aligned}$$

Aangezien ook geldt

$$q_n(d,d) = 2 \uparrow_{d+1}^{n-2} 4de \overset{\text{(f)}}{\leq} 2 \uparrow^{n-1} (de + d + 2) \leq 2 \uparrow^{n-1} (d+1)(e+1) = Q_n(d)$$

concluderen we met gevolg 4.6 en inductie dat de stelling klopt. □

In het geval van Buchbergers algoritme heeft het te reduceren S-polynoom graad hoogstens $2d$, met d de graad van alle eerdere polynomen. Het reduceren kost dus minder dan $2 \uparrow^{n-1} 6d^2$ iteraties. De graad van het gereduceerde S-polynoom is kleiner dan

$$2d + d(2 \uparrow^{n-1} 6d^2) \overset{\text{(c),(e)}}{\leq} 2d + 2 \uparrow^{n-1} (6d^2 + d - 1) \overset{\text{(c),(d)}}{<} 2 \uparrow^{n-1} (6d^2 + d) \leq 2 \uparrow^{n-1} 7d^2.$$

Deze afschatting werkt alleen voor $n \geq 2$, maar anders is de enige monoomordening graadrespecterend en geldt de grens zeker. Nu zijn we weer in dezelfde situatie als in de vorige paragraaf.

Stelling 4.11. Laat de invoer van Buchbergers algoritme (met een willekeurige monoomordening) bestaan uit polynomen in $R = K[x_1, \ldots, x_n]$ van graad hoogstens $d \geq 1$. Dan voegt het algoritme hieraan minder dan $A(2n+1, 2d-1)$ polynomen toe, elk van graad kleiner dan $A(2n+2, d+1)$.

Bewijs. Voor $n \leq 1$ is het triviaal. Laat anders $\delta(d) = 2 \uparrow^{n-1} 7d^2$ en

$$Q_m(d) = 2 \uparrow^{m+n-1} (2d+2) - 3 = A(m+n+1, 2d-1).$$

We bewijzen dat geldt $P_m(d) < Q_m(d)$. Dit is duidelijk voor $m \leq 1$. Met inductie bewijzen we eenvoudig dat de afschatting $\delta^k(d) < 2 \uparrow^n 2(d+k)$ geldt. Bij $m = 2$ nemen we $Q_1'(d) = d + 1$ en

$q_2(d,i) = 2 \uparrow_{i+1}^n 2(d+i) - 3$. Dan hebben we $q_2(d,0) = 2 \uparrow^n 2d - 3 \geq 2d - 1 \geq 1$ via (c). Voor $i > 0$ en $k = q_2(d, i-1)$ geldt

$$\begin{aligned} k + Q_1'(\delta^k(d)) &< (k+4) + 2 \uparrow^n 2(d+k) - 3 \overset{\text{(c),(d)}}{<} 2 \uparrow^n 2(d+k+1) - 3 \\ &< 2 \uparrow^n 2(d + 2 \uparrow_i^n 2(d+i-1)) - 3 \overset{\text{(c),(d)}}{<} 2 \uparrow^n 2(2 \uparrow_i^n (2d+2i-1)) - 3 \\ &\overset{\text{(c),(e)}}{<} 2 \uparrow^n 2 \uparrow_i^n 2(d+i) - 3 = 2 \uparrow_{i+1}^n 2(d+i) - 3 = q_n(d,i). \end{aligned}$$

Uit (5) volgt dat $Q_1'(d) = P_1(d)$, en wegens gevolg 4.6 geldt

$$P_2(d) < q_2(d,d) = 2 \uparrow_{d+1}^n 4d - 3 \overset{\text{(f)}}{\leq} 2 \uparrow^{n+1} (2d+2) - 3 = Q_2(d).$$

Voor $m > 2$ noteren we $l = m + n - 1$. Neem $q_m(d,i) = 2 \uparrow_i^{l-1} 2 \uparrow_{i+1}^n 2(d+i) - 3$. Merk op dat geldt $q_m(d,0) = 2 \uparrow^n 2d - 3 \geq 2d - 1 \geq 1$, wederom volgens (c). Voor $i > 0$ en $k = q_m(d, i-1)$ geldt

$$\begin{aligned} k + Q_{m-1}(\delta^k(d)) &< k + 2 \uparrow^{l-1} (2(2 \uparrow^n 2(d+k)) + 2) - 3 \overset{\text{(c),(e)}}{<} k + 2 \uparrow^{l-1} (2 \uparrow^n 2(d+k+1) + 2) - 3 \\ &\overset{\text{(c),(d)}}{<} k + 2 \uparrow^{l-1} 2 \uparrow^n 2(d+k+2) - 3 \overset{\text{(c),(d)}}{<} 2 \uparrow^{l-1} 2 \uparrow^n 2(d+k+3) - 3 \\ &= 2 \uparrow^{l-1} 2 \uparrow^n 2(d + 2 \uparrow_{i-1}^{l-1} 2 \uparrow_i^n 2(d+i-1)) - 3 \overset{\text{(c),(d)}}{<} 2 \uparrow^{l-1} 2 \uparrow^n 2(2 \uparrow_{i-1}^{l-1} \uparrow_i^n (2d+2i-1)) - 3 \\ &\overset{\text{(c),(e)}}{<} 2 \uparrow^{l-1} 2 \uparrow^n 2 \uparrow_{i-1}^{l-1} \uparrow_i^n 2(d+i) - 3 \overset{\text{(b)}}{\leq} 2 \uparrow_i^{l-1} 2 \uparrow_{i+1}^n 2(d+i) - 3 = q_m(d,i). \end{aligned}$$

Verder geldt er wegens $l - 1 \geq n + 1$ dat

$$\begin{aligned} q_m(d,d) &= 2 \uparrow_d^{l-1} 2 \uparrow_{d+1}^n 4d - 3 \overset{\text{(f)}}{\leq} 2 \uparrow_d^{l-1} 2 \uparrow^{n+1} (2d+2) - 3 \\ &\overset{\text{(a)}}{\leq} 2 \uparrow_{d+1}^{l-1} (2d+2) - 3 \leq 2 \uparrow_{d+1}^{l-1} 4d - 3 \overset{\text{(f)}}{\leq} 2 \uparrow^l (2d+2) - 3 = Q_m(d). \end{aligned}$$

Met gevolg 4.6 en inductie is de ongelijkheid $P_m(d) < Q_m(d)$ dus bewezen. De bewering over het aantal volgt met $m = n$. Bovendien zijn de graden kleiner dan

$$\begin{aligned} \delta^{Q_n(d)}(d) &< 2 \uparrow^n 2(d + Q_n(d)) \overset{\text{(c),(d)}}{<} 2 \uparrow^n 2(d + 2 \uparrow^{2n-1} (2d+2)) - 3 \\ &\overset{\text{(c),(d),(e)}}{<} 2 \uparrow^n 2 \uparrow^{2n-1} (2d+4) - 3 \overset{\text{(a)}}{\leq} 2 \uparrow_2^{2n-1} 6d - 3 \overset{\text{(f)}}{<} 2 \uparrow^{2n} (d+4) - 3 = A(2n+2, d+1). \quad \square \end{aligned}$$

Ook hier kunnen we analoog iets scherpere grenzen bewijzen: voor $k \in \mathbb{Z}_{\geq 1}$ en $\varepsilon = \frac{1}{k}$ is het aantal polynomen begrensd door $A(2n+1, \lfloor (1+\varepsilon)d \rfloor + k - 2)$ en hun graad door $A(2n+2, \lfloor \varepsilon d \rfloor + k)$.

De grens is enorm groot en we benadrukken dat er geen redenen zijn om aan te nemen dat Buchbergers algoritme inderdaad soms zo traag is. De grootste ondergrenzen zijn 'slechts' dubbelexponentieel in n en velen denken dat er vergelijkbare bovengrenzen bestaan. Dit is bijvoorbeeld gebaseerd op de grens van Dubé uit het vorige hoofdstuk. Voor een dubbelexponentiële bovengrens op de complexiteit van Buchbergers algoritme is echter geen bewijs. Dergelijke betere grenzen, of zelfs primitief recursieve grenzen, kunnen we niet vinden met alleen de technieken die we hier toegepast hebben: Moreno Socías [35] bewijst dat zelfs met de 'kleinste' majorerende functie $\delta(d) = d + 1$ er voor alle $n, d \in \mathbb{Z}_{\geq 1}$ al rijen monomen als in lemma 4.7 zijn met lengte $A(n, d-1) - d$.

Zeer recent hebben we ontdekt dat de resultaten in dit hoofdstuk niet volledig nieuw zijn. Dubé, Mishra en Yap [13] geven vergelijkbare grenzen. In het graadrespecterende geval geven ze de bovengrens $A(n+1, cn)$ voor het aantal toegevoegde polynomen. Hier is c een constante die op een technische manier van de graad en andere eigenschappen van de invoer afhangt. Merk op dat dat iets scherper is dan stelling 4.9. Dubé, Mishra en Yap claimen bovendien dat er vergelijkbare grenzen in het algemene geval zijn, hoewel ze geen expliciete uitdrukking geven. De basis van hun argument is Robbiano's karakterisatie van monoomordeningen, zie propositie 5.7. Daaruit leiden ze af dat het delingsalgoritme op een polynoom f niet meer dan $O((r \deg(f))^n)$ iteraties uitvoert, met r afhankelijk van de monoomordening. Dit lijkt een sterke verbetering van stelling 4.10. Echter, r is in principe onbegrensd (over alle monoomordeningen genomen) dus dit voorziet niet in een algemene bovengrens voor de complexiteit van Buchbergers algoritme. De resultaten in dit hoofdstuk doen dat wel.

5 Overige resultaten

Dit laatste hoofdstuk is een inleiding in de literatuur omtrent Buchbergers algoritme en, meer in het algemeen, de complexiteit van het berekenen van Gröbnerbases. We benadrukken dat dit overzicht geenszins volledig is. In plaats daarvan hebben we enkele interessante onderwerpen geselecteerd, waarbij een combinatie is gemaakt tussen fundamentele resultaten en meer recent onderzoek. De meeste bewijzen geven we niet of alleen schetsmatig.

Uit ervaring willen we de lezer waarschuwen voor incorrecte referenties die we in de literatuur zijn tegengekomen. We noemen nogmaals de verkeerde interpretatie van de stelling van Dubé in [27, 31]. Het overigens goede boek van Cox, Little en O'Shea [11] verwijst naar de ondergrens uit hoofdstuk 2 als dubbelexponentieel in de graad van de invoerpolynomen, in plaats van in het aantal variabelen. Eisenbuds boek [14] geeft een bovengrens voor de graad van elementen van een Gröbnerbasis, afkomstig van Möller en Mora [33]. Dit is echter gebaseerd op een vermoeden in [29]. In de 2^{e} editie heeft Eisenbud deze grens inderdaad verwijderd. Ten slotte claimen Gritzmann en Sturmfels [21] de bovengrens d^{2^n} voor de graad van ieder polynoom dat in Buchbergers algoritme berekend wordt, maar geven daar geen geschikte referenties bij.

5.1 Selectiestrategieën en reductiecriteria

Het meest tijdrovende gedeelte van Buchbergers algoritme is het reduceren van polynomen tot hun normaalvorm. Deze reducties moeten zoveel mogelijk worden voorkomen. Dit kunnen we op twee manieren bereiken. Ten eerste heeft de volgorde waarin de S-polynomen worden berekend grote invloed op de complexiteit van het algoritme. We zoeken dus een *selectiestrategie* om deze keuze zo efficiënt mogelijk te maken. De tweede methode is het geven van *reductiecriteria* die van te voren bepalen of een reductie op 0 uitkomt en daarmee overbodig is. We noemen hier twee van deze criteria, afkomstig van Buchberger [5, 6, 8].

Propositie 5.1. Zij $g, h \in R \setminus \{0\}$ met $\text{LM}(g)$ en $\text{LM}(h)$ copriem. Dan geldt $\text{nf}_{\{g,h\}}(S(g,h)) = 0$.

Bewijs (schets). Uit [11, §2.9, Theorem 3] volgt dat het voldoende is als er een *representatie* van $S(g,h)$ is: dat wil zeggen, als er polynomen $p, q \in R$ zijn met $S(g,h) = pg + qh$ waarvoor bovendien geldt $\text{LM}(pg), \text{LM}(qh) \preceq \text{LM}(S(g,h))$. Maar er geldt

$$S(g,h) = \text{LT}(h)g - \text{LT}(g)h = (g - \text{LT}(g))h - (h - \text{LT}(h))g$$

dus neem $p = -(h - \text{LT}(h))$ en $q = g - \text{LT}(g)$. De monomen $\text{LM}(pg)$ en $\text{LM}(qh)$ zijn verschillend omdat $\text{LM}(g)$ en $\text{LM}(h)$ copriem zijn. Er volgt $\text{LM}(pg), \text{LM}(qh) \preceq \max(\text{LM}(pq), \text{LM}(qh)) = \text{LM}(S(g,h))$. □

Het S-polynoom van twee polynomen met onderling ondeelbare leidende monomen hoeft dus niet te worden uitgerekend. Het tweede, diepere criterium is een generalisatie van stelling 1.12.

Stelling 5.2. Zij $I \subset R$ een ideaal en $G \subset I$ een eindige deelverzameling. Rust G uit met een willekeurige ordening op de elementen. Dan is G een Gröbnerbasis voor I dan en slechts dan als $I = (G)$ en voor alle $g, h \in G \setminus \{0\}$ er een rij polynomen $g = g_1, \ldots, g_r = h$ in $G \setminus \{0\}$ is, zodanig dat $\text{LM}(g_i)$ steeds een deler van $\text{kgv}(\text{LM}(g), \text{LM}(h))$ is, en voor $1 \leq i < r$ geldt $\text{nf}_G(S(g_i, g_{i+1})) = 0$.

Bewijs. Zie [25, Theorem 1.5]. Een eenvoudiger bewijs voor $r = 3$ staat in [4, Proposition 5.70]. □

We gebruiken in Buchbergers algoritme deze sterkere stelling in plaats van criterium 1.12, wat het speciale geval $r = 2$ is. Dan hoeft $\text{nf}_G(S(g,h))$ alleen te worden berekend wanneer een rij als in stelling 5.2 niet bestaat. Dit is echter lastig algoritmisch te bepalen. Daarom wordt meestal beperkt tot het geval $r = 3$, wat bijna geen informatieverlies geeft [6, §5]. Dan wordt $\text{nf}_G(S(g,h))$ dus niet bepaald wanneer er een derde polynoom $p \in G$ is met $\text{LM}(p) \mid \text{kgv}(\text{LM}(g), \text{LM}(h))$ en waarvoor bovendien (g,p), (p,g), (h,p) en (p,h) niet in B liggen (met B als in algoritme 1.13). Als er niet zo'n p is en bovendien $\text{LM}(g)$ en $\text{LM}(h)$ niet copriem zijn, dan heet (g,h) een *essentieel* paar. Na het verwijderen van niet-essentiële paren uit B kunnen andere paren ook niet-essentieel blijken te zijn. Het loont dus deze paren zo vroeg mogelijk uit B te verwijderen. Dit is het idee achter de versie van Gebauer en Möller [17].

Volgens de criteria reduceert $S(g,h)$ naar 0 als (g,h) geen essentieel paar is. Hong en Perry [22] bewijzen dat deze criteria bijna altijd optimaal zijn in de volgende zin. Stel dat we uit alleen $\text{LM}(g)$, $\text{LM}(h)$, $\text{LM}(p)$ en het feit dat $S(g,p)$ en $S(p,h)$ naar 0 reduceren kunnen concluderen dat $S(g,h)$ ook naar 0 reduceert. Dan is (g,h) geen essentieel paar. De enige uitzondering is wanneer $|G| \leq 3$. In dat geval geeft [22] andere criteria, die voldoende en noodzakelijk zijn.

Uit het tweede criterium 5.2 volgt direct een heuristiek voor de volgorde van het berekenen van S-polynomen. Namelijk, bij paren (g,h) waarvoor $\text{kgv}(\text{LM}(g), \text{LM}(h))$ groot is, is het waarschijnlijk dat er ooit een $p \in G$ komt met $\text{LM}(p) \mid \text{kgv}(\text{LM}(g), \text{LM}(h))$. In dat geval hoeft $S(g,h)$ niet gereduceerd te worden. Daarom kunnen dergelijke paren het best zo laat mogelijk worden bekeken. De strategie is dus om steeds het paar (g,h) te kiezen waarvoor $\text{kgv}(\text{LM}(g), \text{LM}(h))$ zo klein mogelijk is ten opzichte van de monoomordening. Dit staat bekend als *normale selectiestrategie* [4, 6, 8]. Deze strategie werkt ook bijzonder goed in het homogene geval.

Propositie 5.3. Laat $\{g_1, \ldots, g_s\} \subset R$ bestaan uit homogene polynomen. Als $g_{s+1}, \ldots, g_t$ de polynomen zijn die Buchbergers algoritme hieraan toevoegt, met een graadrespecterende monoomordening en normale selectiestrategie, dan geldt $\deg(g_{s+1}) \leq \deg(g_{s+2}) \leq \ldots \leq \deg(g_t)$. Bovendien geldt voor $s < i \leq t$ dat g_i gereduceerd is ten opzichte van $\{g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_t\}$.

Bewijs. Voor $i > s$ geldt $g_i = \text{nf}_G(S(g_k, g_m))$ voor zekere $k, m < i$. Dit heeft graad

$$\deg(g_i) = \deg(S(g_k, g_m)) = \deg(\text{kgv}(\text{LM}(g_k), \text{LM}(g_m)))$$

wegens homogeniteit. Bij het toevoegen van g_i is deze graad minimaal gekozen vanwege de graadrespecterende monoomordening $\succ$ en normale selectiestrategie. In het geval $\deg(g_{i+1}) < \deg(g_i)$ moet dus gelden $g_{i+1} = \text{nf}_G(S(g_j, g_i))$ voor zekere $j < i$. Maar dan geldt

$$\deg(g_{i+1}) = \deg(\text{kgv}(\text{LM}(g_j), \text{LM}(g_i))) \geq \deg(\text{LM}(g_i)) = \deg(g_i),$$

tegenspraak. Voor de tweede bewering merken we op dat in feite geldt $\text{LM}(g_{s+1}) \prec \ldots \prec \text{LM}(g_t)$. Voor $s < i \leq t$ is g_i automatisch gereduceerd ten opzichte van $\{g_1, \ldots, g_{i-1}\}$. Voor $j > i$ kan $\text{LM}(g_j)$ geen term van g_i delen, want $\text{LM}(g_j)$ is groter dan elke term van g_i ten opzichte van $\succ$. □

Giovini e.a. [18] gebruiken een andere selectiestrategie, genaamd *suiker*, om deze fijne eigenschap ook in het inhomogene geval te benutten. Homogeniseren en toepassing van propositie 3.3 levert meestal een slechter algoritme, maar selectie kan wel op homogenisatie worden gebaseerd. Meer precies kennen we aan ieder polynoom g in Buchbergers algoritme een *fantoomgraad* of *suiker* $s(g)$ toe. Dit is de graad die het polynoom zou hebben 'wanneer we hadden gehomogeniseerd'. Voor de polynomen in de invoer nemen we $s(g) = \deg(g)$. Daarna stellen we

$$s(Mg) = \deg(M) + s(g) \qquad \text{en} \qquad s(g+h) = \max(s(g), s(h)),$$

waar g en h polynomen zijn en M een monoom. Door de laatste regel verschilt suiker van graad: als termen tegen elkaar wegvallen kan $\deg(g+h) < s(g+h)$ gelden. Bij homogene polynomen gebeurt dat niet. De selectiestrategie is nu om het paar (g,h) te kiezen waarvan $S(g,h)$ de kleinste suiker heeft. Experimenteel onderzoek toont aan dat suiker, in combinatie met bovengenoemde reductiecriteria, de beste resultaten geeft van alle varianten in deze paragraaf [18, §3].

5.2 Twee of drie variabelen

Hoewel de algemene complexiteit van Buchbergers algoritme nog onduidelijk is, is de complexiteit van sommige deelproblemen wel bekend. Als we het aantal variabelen beperken kan dat de complexiteitsanalyse aanzienlijk vereenvoudigen. Met name bij $n \leq 3$ zijn er goede grenzen bekend. Voor $n = 1$ specialiseert Buchbergers algoritme tot het algoritme van Euclides en wordt het aantal toegevoegde polynomen begrensd door d, de grootste graad van polynomen in de invoer. In het geval $n = 2$ noemen we enkele resultaten van Buchberger [6, 7] en Lazard [29].

Stelling 5.4. Gebruik Buchbergers algoritme met een graadrespecterende monoomordening en behandel alleen essentiële paren. Als de invoer bestaat uit polynomen in $K[x,y]$ van graad hoogstens d, dan hebben tijdens de executie alle berekende polynomen graad hoogstens $2d$.

Bewijs (schets). Zij G de invoer. Laat $m(G)$ de grootste graad van een term $\mathrm{kgv}(\mathrm{LM}(g), \mathrm{LM}(h))$ zijn, waar (g, h) een essentieel paar in G is. Laat verder $w(G) = e_x + e_y$ zijn, met $e_x, e_y \in \mathbb{N}$ de kleinste exponenten waarvoor er termen $x^{e_x}y^b \in \mathrm{LM}(G)$ respectievelijk $x^a y^{e_y} \in \mathrm{LM}(G)$ zijn. Het eerste toegevoegde polynoom heeft graad hoogstens $m(G)$, en $w(G)$ is een maat voor het aantal monomen niet in $(\mathrm{LM}(G))$. Men kan bewijzen dat $m(G) + w(G)$ tijdens de executie niet groter wordt, een grens voor de graad van ieder berekend polynoom is en dat geldt $m(G) + w(G) \leq 2d$. Zie [6, §6] en [7, Theorem 1] voor de details. Daar wordt de stelling alleen geclaimd voor deglex, maar het bewijs geldt voor iedere graadrespecterende monoomordening. □

In het bijzonder geldt deze grens voor de uitvoer. Lazard [29, Theorem 3] geeft voor de uitvoer zelfs de grens $2d - 1$, maar zijn bewijs geldt niet voor de tussenliggende berekeningen. Uit propositie 1.10 en het gebruik van een graadrespecterende monoomordening volgt dat de bovengrens $2d - 1$ geldt voor de graden in iedere minimale Gröbnerbasis. Deze grens is bovendien strikt: met deglex ordening en invoer $\{x^d,\ x^{d-1}y - y^d\}$, $d \geq 3$, vinden we de gereduceerde Gröbnerbasis $\{x^d,\ x^{d-1}y - y^d,\ xy^d,\ y^{2d-1}\}$. Niet bij alle monoomordeningen is de groei slechts lineair. Als we lex ordening gebruiken met $x \succ y$, dan geeft de invoer $\{x^d - y,\ x - y^d\}$ namelijk de gereduceerde Gröbnerbasis $\{x - y^d,\ y^{d^2} - y\}$. Schaller [39, §4.5] geeft een vergelijkbare bovengrens: bij lex ordening zijn alle polynomen tijdens de executie van Buchbergers algoritme begrensd door $2d^2$. In het bivariate geval geven we ten slotte nog de volgende grens van Buchberger [7, Theorem 2] voor het aantal polynomen.

Stelling 5.5. Zij $I = (g_1, \ldots, g_s) \subset K[x, y]$ een ideaal en $e = \min\{\deg(\mathrm{LM}(g_i)) : 1 \leq i \leq s\}$, met een willekeurige monoomordening. Elke minimale Gröbnerbasis G voor I voldoet aan $|G| \leq e + 1$.

Bewijs. Neem $g \in \{g_1, \ldots, g_s\}$ met $\deg(\mathrm{LM}(g)) = e$. Er is een $h \in G$ met $\mathrm{LM}(h) \mid \mathrm{LM}(g)$. In het bijzonder geldt $\deg(\mathrm{LM}(h)) \leq e$. Schrijf $\mathrm{LM}(h) = x^a y^b$. De andere elementen $x^p y^q \in \mathrm{LM}(G)$ hebben wegens minimaliteit $p < a$ of $q < b$. Bovendien zijn er bij vaste p geen verschillende monomen $x^p y^{q_1}$ en $x^p y^{q_2}$ in $\mathrm{LM}(G)$. Hetzelfde geldt voor q. We concluderen $|G| = |\,\mathrm{LM}(G)| \leq a + b + 1 \leq e + 1$. □

Let op dat e hier de kleinste graad is. Deze grens is optimaal, want de $e+1$ monomen $x^e, x^{e-1}y, \ldots, y^e$ van graad e vormen een gereduceerde Gröbnerbasis.

Het bewijs van stelling 5.4 berust sterk op $n = 2$ en wordt lastig gegeneraliseerd, maar voor $n = 3$ geeft Winkler [40] met vergelijkbare technieken nog de volgende stelling.

Stelling 5.6. Gebruik Buchbergers algoritme met deglex ordening en behandel alleen essentiële paren. Als $\{g_1, \ldots, g_s\} \subset K[x, y, z]$ de invoer is met d en e de grootste respectievelijk kleinste graad van de g_i, dan hebben tijdens de executie alle berekende polynomen graad hoogstens $(8d + 1)2^e$.

Bewijs. Zie [40, Corollary to Theorem 4.1]. □

Hoewel deze grens exponentieel groeit, is deze groei in de kleinste graad van een voortbrenger. Tijdens de executie van het algoritme zal e vaak kleiner worden, zodat we een steeds betere grens vinden.

5.3 Monoomordeningen

Sommige monoomordeningen geven kleinere Gröbnerbases dan andere. Vaak doen graadrespecterende ordeningen het beter, zoals we bijvoorbeeld in de vorige paragraaf zagen. Veel toepassingen van Gröbnerbases hangen niet af van een specifieke monoomordening. In zekere zin is de *omgekeerd graadlexicografische ordening*, of *degrevlex*, dan optimaal qua complexiteit. Voor $M = x_1^{d_1} \cdots x_n^{d_n}$ en $N = x_1^{e_1} \cdots x_n^{e_n}$ geldt in deze ordening $M \succ N$ dan en slechts dan als $\deg(M) > \deg(N)$, of als $\deg(M) = \deg(N)$ en $d_i < e_i$ voor de grootste i met $d_i \neq e_i$. Merk op dat dit verschilt van deglex: in beide monoomordeningen geldt $x_1 \succ \ldots \succ x_n$, maar voor deglex geldt $x_1 x_3 \succ x_2^2$ en voor degrevlex geldt $x_1 x_3 \prec x_2^2$. Bayer en Stillman [2] bewijzen voor homogene idealen $I \subset R$ in karakteristiek 0 dat voortbrengers van het ideaal $(\mathrm{LM}_\succ(I))$ 'meestal' (namelijk *in generieke coördinaten*) de kleinste graad hebben als $\succ$ de degrevlex ordening is. Hier en in de rest van deze paragraaf geven we de monoomordening expliciet aan. De elementen van minimale Gröbnerbases hebben bij degrevlex dus vaak de kleinste graad. Dit komt overeen met experimentele waarnemingen, ook bij inhomogene idealen.

Maar ook degrevlex ordening levert niet altijd de kortste berekening op. Er is winst te behalen door flexibeler met monoomordeningen om te gaan. Daarvoor geven we eerst de volgende karakterisatie van Robbiano [38]. Zij $\omega = (v_1, \ldots, v_n) \in \mathbb{R}^n$ een vector. We definiëren de *ω-graad* van een monoom door

$$\deg_\omega(x_1^{d_1} \cdots x_n^{d_n}) = v_1 d_1 + \ldots + v_n d_n.$$

Een polynoom $f \in R$ heet *ω-homogeen* als alle monomen in f dezelfde ω-graad hebben. We rusten $\mathbb{R}^r$ uit met de lexicografische ordening $>$. Hierin geldt $(a_1, \ldots, a_r) > (b_1, \ldots, b_r)$ als de eerste niet-nul coördinaat van $(a_1 - b_1, \ldots, a_r - b_r)$ positief is.

Propositie 5.7. Laat $\succ$ een monoomordening zijn. Er zijn lineair onafhankelijke vectoren $\omega_1, \ldots, \omega_r$ in $\mathbb{R}^n$ met $1 \leq r \leq n$, zodanig dat voor alle monomen M en N geldt

$$M \succ N \quad \Leftrightarrow \quad (\deg_{\omega_1}(M), \ldots, \deg_{\omega_r}(M)) > (\deg_{\omega_1}(N), \ldots, \deg_{\omega_r}(N)).$$

Bovendien geldt $\omega_1 \in \mathbb{R}^n_{\geq 0}$, en ω_1 is uniek op vermenigvuldiging met een scalar in $\mathbb{R}_{>0}$ na.

Bewijs. Zie [38, Theorem 4] voor de existentie. Als de i^{de} coördinaat van ω_1 negatief is, dan geldt $\deg_{\omega_1}(x_i) < 0 = \deg_{\omega_1}(1)$, maar $x_i \succ 1$. Er volgt $\omega_1 \in \mathbb{R}^n_{\geq 0}$. Stel dat $\sigma_1, \ldots, \sigma_t \in \mathbb{R}^n$ een ander dergelijk rijtje is met $\sigma_1 \neq \lambda\omega_1$ voor alle $\lambda \in \mathbb{R}$. Dan kunnen we eenvoudig monomen M en N vinden waarvoor geldt $\deg_{\omega_1}(M) > \deg_{\omega_1}(N)$ maar $\deg_{\sigma_1}(M) < \deg_{\sigma_1}(N)$, tegenspraak. Omdat geldt $\omega_1 \in \mathbb{R}^n_{\geq 0}$ en ω_1 onderdeel van een lineair onafhankelijk stelsel is, volgt dat λ positief is. □

Met lex ordening correspondeert bijvoorbeeld het rijtje standaardeenheidsvectoren $e_1, \ldots, e_n \in \mathbb{R}^n$. De vector ω_1 heet een *weegvector* van $\succ$. Voor een niet-nul vector $\omega \in \mathbb{R}^n_{\geq 0}$ construeren we als volgt een monoomordening met weegvector ω: neem $\succ$ willekeurig, en definieer $\succ_\omega$ door

$$M \succ_\omega N \quad \Leftrightarrow \quad \deg_\omega(M) > \deg_\omega(N), \text{ of } \deg_\omega(M) = \deg_\omega(N) \text{ en } M \succ N.$$

Dan is $\succ_\omega$ een monoomordening met weegvector ω.

Nu beschrijven we een *dynamische* versie van Buchbergers algoritme, naar Gritzmann en Sturmfels [21]. Hierin is de monoomordening niet vast. Steeds nadat een polynoom aan G is toegevoegd mag een nieuwe monoomordening worden gekozen (met notatie uit algoritme 1.13). De verzameling B moet daarna wel geherinitialiseerd worden met alle paren van polynomen in G, omdat reduceren afhankelijk is van de gekozen monoomordening. Wanneer B leeg is hebben we een Gröbnerbasis ten opzichte van de monoomordening die op dat moment gebruikt wordt. Terminatie van dit dynamische algoritme is niet direct duidelijk. Het oorspronkelijke bewijs [21, Theorem 3.1.3] bevat een fout. Golubitsky [20] toont dit aan en geeft een verbeterd bewijs door middel van convergentie van rijen monoomordeningen.

Stelling 5.8. De dynamische versie van Buchbergers algoritme termineert en is correct.

Bewijs (schets). Noem een rij monoomordeningen $\succ_1, \succ_2, \ldots$ *convergent* als er voor alle monomen $M \neq N$ een $k \in \mathbb{N}$ is, zodanig dat $M \succ_i N$ geldt voor alle $i \geq k$, of $M \prec_i N$ voor alle $i \geq k$. De natuurlijke *limiet* van deze rij is weer een monoomordening. Noem de tijdens de executie toegevoegde polynomen $g_1, g_2, \ldots$ en schrijf $G_i = \{g_1, \ldots, g_i\}$. Laat $\succ_1, \succ_2, \ldots$ de gebruikte monoomordeningen zijn, zodat elke g_i gereduceerd is ten opzichte van G_{i-1} en $\succ_i$. Als het algoritme niet termineert, zijn deze rijen oneindig. Men kan bewijzen dat $\succ_1, \succ_2, \ldots$ een convergente deelrij heeft. Noem de limiet $\succ$. Nu kunnen we indices $k_1, k_2, \ldots$ vinden waarvoor geldt

$$(\text{LM}_\succ(G_{k_1})) \subsetneq (\text{LM}_\succ(G_{k_2})) \subsetneq \ldots.$$

Omdat R noethers is, is deze rij eindig, tegenspraak. Na terminatie volgt correctheid direct uit het bewijs van stelling 1.14. Zie [20, Lemma 1, Theorem 1 en Theorem 2] voor de details. □

Om profijt te hebben van het dynamische algoritme moeten we steeds een slimme keuze voor de monoomordening maken. Noteer voor een vector $\omega \in \mathbb{R}^n$ en een polynoom $f \in R \setminus \{0\}$ met $\text{LT}_\omega(f)$ het deel van f bestaande uit de termen met de grootste ω-graad.

Lemma 5.9. Laat $g_1, \ldots, g_s \in R \setminus \{0\}$ polynomen zijn en M_i een monoom dat in g_i voorkomt voor alle $1 \leq i \leq s$. Er is een monoomordening $\succ$ met $\text{LM}_\succ(g_i) = M_i$ voor alle $1 \leq i \leq s$ dan en slechts dan als er vector $\omega \in \mathbb{R}^n_{\geq 0}$ is waarvoor geldt $\text{LT}_\omega(g_i) = c_i M_i$ voor alle $1 \leq i \leq s$, met zekere $c_i \in K$.

Bewijs. Gegeven $\succ$ kiezen we vectoren $\omega_1, \ldots, \omega_r \in \mathbb{R}^n$ als in propositie 5.7. Het is duidelijk dat de vector $\omega = \omega_1 + \varepsilon\omega_2 + \varepsilon^2\omega_3 + \ldots + \varepsilon^{r-1}\omega_r$ voldoet voor $\varepsilon > 0$ klein genoeg. We kunnen ω in $\mathbb{R}^n_{\geq 0}$ nemen door aan $g_1, \ldots, g_s$ de polynomen $x_i - 1$ toe te voegen voor $1 \leq i \leq n$. Andersom, gegeven $\omega \in \mathbb{R}^n_{\geq 0}$ zien we direct dat $\succ = \sqsupset_\omega$ voldoet, waarbij $\sqsupset$ een willekeurig monoomordening is. $\square$

Het bestaan van zo'n monoomordening is dus equivalent aan het bestaan van een oplossing van een stelsel lineaire ongelijkheden. Dit stelsel kan bijvoorbeeld worden opgelost met de simplex methode. Op deze manier bepalen we welke mogelijkheden er zijn voor $(\text{LM}_\succ(G))$ bij de verschillende keuzes voor $\succ$. Merk op dat dit eindig veel mogelijkheden zijn, want iedere $g \in G$ heeft maar eindig veel kandidaten voor leidende monomen. De heuristiek voor het kiezen van $\succ$ is nu om $(\text{LM}_\succ(G))$ zo groot mogelijk te maken. De reden voor deze keuze is dat Buchbergers algoritme herhaald $(\text{LM}_\succ(G))$ groter maakt, totdat G een Gröbnerbasis is en er geldt $(\text{LM}_\succ(G)) = (\text{LM}_\succ(I))$. Als $(\text{LM}_\succ(G))$ groot is, zijn we dus mogelijk dichtbij een Gröbnerbasis. We benadrukken dat ook $(\text{LM}_\succ(I))$ afhankelijk is van $\succ$, zodat dit slechts een heuristiek is en niet noodzakelijk de optimale strategie.

In de praktijk wordt niet $(\text{LM}_\succ(G))$ maar de Hilbertfunctie $H_{(\text{LM}_\succ(G))}(z)$ zo groot mogelijk gekozen. Voor z voldoende groot is dat een polynoom in z dat effectief bepaald kan worden [9, §2]. Twee polynomen vergelijken we door te zeggen dat $a_n z^n + \ldots + a_0$ groter is dan $b_n z^n + \ldots + b_0$ als $a_i > b_i$ geldt voor de grootste i met $a_i \neq b_i$.

Caboara [9] gebruikt een beperkte variant van dit algoritme. Daarin moet de nieuwe monoomordening dusdanig worden gekozen dat de leidende monomen van alle eerdere polynomen niet veranderen. Zo blijven alle eerdere berekeningen geldig. De verzameling B hoeft in deze versie dan ook niet steeds te worden geherinitialiseerd. Dat scheelt veel extra werk. Experimenten tonen aan dat deze versie vaak veel sneller is dan Buchbergers algoritme als in 1.13. Golubitsky [20, §5] geeft voorbeelden waar het algemene dynamische algoritme sneller is dan de beperkte versie van Caboara.

Soms willen we wel een specifieke monoomordening gebruiken. Zo is in eliminatietheorie lex ordening essentieel, zie [11, §3.1]. Buchbergers algoritme presteert echter vaak slecht met lex ordening. Daarom kan het lonen om de Gröbnerbasis voor een andere monoomordening te berekenen, en die vervolgens te transformeren naar een Gröbnerbasis voor lex ordening. De *Gröbnerwandeling* is een algoritme dat deze transformatie uitvoert. Wij beschrijven de versie van Collart, Kalkbrener en Mall [10]. Het volgende begrip staat hierin centraal. Definieer $\text{LT}_\omega(S) = \{\text{LT}_\omega(h) : h \in S \setminus \{0\}\}$ voor een vector $\omega \in \mathbb{R}^n_{\geq 0}$ en een deelverzameling $S \subset R$.

Definitie 5.10. Voor een monoomordening $\succ$ en een ideaal $I \subset R$ is

$$D_\succ(I) = \overline{\{\omega \in \mathbb{R}^n_{\geq 0} : (\text{LT}_\omega(I)) = (\text{LM}_\succ(I))\}}$$

de *Gröbnerkegel* van I ten opzichte van $\succ$. Hier is $\overline{A}$ de topologische afsluiting van A in $\mathbb{R}^n$. De verzameling $G(I) = \{D_\succ(I) : \succ \text{ monoomordening}\}$ heet de *Gröbnerwaaier* van I.

Een uitvoerige beschrijving van de Gröbnerwaaier is gegeven door Mora en Robbiano [34]. Zij laten zien dat de kegels in een Gröbnerwaaier een eindige, 'bijna disjuncte' overdekking van $\mathbb{R}^n_{\geq 0}$ vormen en geven een eenvoudige test om de elementen van een Gröbnerkegel te bepalen.

Stelling 5.11. Er geldt $\omega \in D_\succ(I)$ dan en slechts dan als $\text{LM}_\succ(g) = \text{LM}_\succ(\text{LT}_\omega(g))$ voor alle polynomen g in de gereduceerde Gröbnerbasis voor I ten opzichte van $\succ$. Voor een weegvector ω van $\succ$ geldt $\omega \in D_\succ(I)$. Elke Gröbnerkegel is convex en heeft een niet-leeg inwendige. Twee Gröbnerkegels zijn gelijk of snijden elkaar alleen in hun rand. Er geldt $D_{\succ_1}(I) = D_{\succ_2}(I)$ dan en slechts dan als geldt $(\text{LM}_{\succ_1}(I)) = (\text{LM}_{\succ_2}(I))$, en dan en slechts dan als I dezelfde gereduceerde Gröbnerbasis heeft ten opzichte van $\succ_1$ en $\succ_2$. De Gröbnerwaaier $G(I)$ is een eindige verzameling met vereniging $\mathbb{R}^n_{\geq 0}$.

Bewijs (schets). Er geldt $(\text{LT}_\omega(I)) = (\text{LM}_\succ(I))$ dan en slechts dan als $\text{LT}_\omega(g) = \text{LM}_\succ(g)$ voor alle polynomen g in de gereduceerde Gröbnerbasis voor I ten opzichte van $\succ$. Hieruit volgt het grootste deel van de stelling. Zie [14, Propositie 15.16] en [34, Lemma 2.6 en Theorem 2.7] voor de details. Om te bewijzen dat $G(I)$ eindig is beschouwen we een versie van Buchbergers algoritme die de gereduceerde Gröbnerbasis bepaalt. De enige invloed die de monoomordening heeft is het aanwijzen van leidende monomen. Steeds zijn daarvoor slechts eindig veel mogelijkheden, en het algoritme termineert bij

elke monoomordening. Volgens het lemma van König [26, §VI.2, Satz 6] is het aantal gereduceerde Gröbnerbases, dus het aantal Gröbnerkegels eindig. □

Laat $\succ_1$ en $\succ_2$ twee monoomordeningen zijn met weegvectoren σ respectievelijk τ. Stel dat de gereduceerde Gröbnerbasis G voor een ideaal $I \subset R$ ten opzichte van $\succ_1$ gegeven is. De Gröbnerwandeling berekent hieruit de gereduceerde Gröbnerbasis voor I ten opzichte van $\succ_2$. In feite lopen we over het lijnstuk $\omega(t) = (1-t)\sigma + t\tau$ van σ naar τ. Wanneer we daarbij een nieuwe Gröbnerkegel binnenkomen, werken we G op geschikte manier bij, totdat we in τ zijn aangekomen.

Eerst bepalen we de maximale $t_0 \in [0,1]$ met $\omega(t_0) \in D_{\succ_1}(I)$. Er geldt $\omega(t) \in D_{\succ_1}(I)$ dan en slechts dan als $\mathrm{LM}_{\succ_1}(g) = \mathrm{LM}_{\succ_1}(\mathrm{LT}_{\omega(t)}(g))$ voor alle $g \in G$, dus dit komt neer op het maximaliseren van t onder een stelsel lineaire ongelijkheden. De vector $\omega = \omega(t_0)$ ligt op de rand van $D_{\succ_1}(I)$. Definieer $\succ = (\succ_2)_\omega$, dan geldt ook $\omega \in D_\succ(I)$.

We construeren nu de gereduceerde Gröbnerbasis voor I ten opzichte van $\succ$. Zij $\sqsupset = (\succ_1)_\omega$. We zien dat G de gereduceerde Gröbnerbasis voor I ten opzichte van $\sqsupset$ is, omdat voor alle $g \in G$ geldt $\mathrm{LM}_\sqsupset(g) = \mathrm{LM}_{\succ_1}(\mathrm{LT}_\omega(g)) = \mathrm{LM}_{\succ_1}(g)$. Er volgt

$$(\mathrm{LM}_\sqsupset(\mathrm{LT}_\omega(I))) = (\mathrm{LM}_\sqsupset(I)) = (\mathrm{LM}_\sqsupset(G)) = (\mathrm{LM}_\sqsupset(\mathrm{LT}_\omega(G)))$$

dus $\mathrm{LT}_\omega(G)$ is een Gröbnerbasis voor $(\mathrm{LT}_\omega(I))$ ten opzichte van $\sqsupset$. Uit $\mathrm{LT}_\omega(G)$ berekenen we een ω-homogene Gröbnerbasis H voor $(\mathrm{LT}_\omega(I))$ ten opzichte van $\succ$. Dit doen we met Buchbergers algoritme. Wegens propositie 5.3, die algemener geldt met steeds graad vervangen door ω-graad en homogeen door ω-homogeen, geeft dit een niet al te ingewikkelde berekening. Bovendien hebben de elementen van $\mathrm{LT}_\omega(G)$ relatief weinig termen, wat de complexiteit sterk verlaagt. Voor $h \in H$ en $g \in G$ bepalen we ω-homogene polynomen $p_{h,g}$ waarvoor geldt

$$h = \sum_{g \in G} p_{h,g}\, \mathrm{LT}_\omega(g) \qquad \text{en} \qquad \deg_\omega(p_{h,g}\, \mathrm{LT}_\omega(g)) = \deg_\omega(h).$$

Dit kan eenvoudig wegens ω-homogeniteit (of de polynomen $p_{h,g}$ kunnen worden bijgehouden tijdens Buchbergers algoritme). We 'liften' deze uitdrukkingen naar

$$f_h = \sum_{g \in G} p_{h,g} g.$$

De verzameling $\{f_h : h \in H\}$ is een Gröbnerbasis voor I ten opzichte van $\succ$. Door reduceren vinden we daaruit de gereduceerde Gröbnerbasis F voor I ten opzichte van $\succ$. We kunnen dus $\succ_1$ vervangen door $\succ$, σ door ω en G door F. Dit proces herhalen we. We bewijzen dat de Gröbnerwandeling termineert.

Lemma 5.12. Gebruik notatie van hierboven, en stel $\omega \neq \tau$. Dan is er een $t \in (t_0, 1]$ met $\omega(t) \in D_\succ(I)$.

Bewijs. Neem $f \in F$ en schrijf $f = \mathrm{LT}_\omega(f) + g$. Er is een $t \in (t_0, 1]$ waarvoor de monomen in $\mathrm{LT}_\omega(f)$ allemaal een grotere $\omega(t)$-graad hebben dan de monomen in g. Omdat F eindig is kunnen we t zodanig kiezen dat dit voor alle $f \in F$ geldt. Voor $f \in F$ en een monoom M in $\mathrm{LT}_\omega(f)$ zien we dat nu geldt $\deg_\omega(M) = \deg_\omega(\mathrm{LM}_\succ(f))$ en $\deg_\tau(M) \leq \deg_\tau(\mathrm{LM}_\succ(f))$. Er volgt $\deg_{\omega(t)}(M) \leq \deg_{\omega(t)}(\mathrm{LM}_\succ(f))$, en deze laatste ongelijkheid geldt zelfs voor alle monomen M in f wegens de keuze van t. We concluderen dat geldt $\mathrm{LM}_\succ(f) = \mathrm{LM}_\succ(\mathrm{LT}_{\omega(t)}(f))$ voor alle $f \in F$, dus $\omega(t) \in D_\succ(I)$. □

Het volgt dat in elke iteratie, afgezien van mogelijk de eerste, geldt $t_0 > 0$. Omdat de Gröbnerwaaier $G(I)$ eindig is en elke Gröbnerkegel convex is hebben we op een gegeven moment $\sigma = \tau$. Merk op dat dan geldt $\succ_2 = (\succ_2)_\sigma$. Door bovenstaande constructie nog eenmaal toe te passen krijgen we de gereduceerde Gröbnerbasis voor I ten opzichte van $\succ_2$.

Voor de Gröbnerwandeling is het eigenlijk niet nodig dat σ en τ weegvectoren van $\succ_1$ en $\succ_2$ zijn. Het is voldoende als geldt $\sigma \in D_{\succ_1}(I)$ en $\tau \in D_{\succ_2}(I)$. Door σ en τ enigszins te verschuiven kan de Gröbnerwandeling veel efficiënter worden. Wanneer de doorsnijding $D_{\succ_1}(I) \cap D_\succ(I)$ hoge dimensie heeft, bestaat $\mathrm{LT}_\omega(G)$ uit bijna alleen monomen en kost de Gröbnerbasistransformatie vrijwel geen moeite. Dit is het idee achter de versie van de Gröbnerwandeling van Fukuda e.a. [15]. Experimenten laten zien dat gebruik van de Gröbnerwandeling vaak veel sneller is dan het direct toepassen van Buchbergers algoritme met de gewenste monoomordening.

Literatuur

[1] W. Ackermann. *Zum Hilbertschen Aufbau der Reellen Zahlen.* Mathematische Annalen **99**, 118–133. Springer, Berlin–Heidelberg, 1928.

[2] D. Bayer, M. Stillman. *A Criterion for Detecting m-Regularity.* Inventiones Mathematicae **87**, 1–11. Springer, Berlin–Heidelberg, 1987.

[3] D. Bayer, M. Stillman. *On the Complexity of Computing Syzygies.* Journal of Symbolic Computation **6**, 135–147, 1988.

[4] T. Becker, V. Weispfenning. *Gröbner Bases. A Computational Approach to Commutative Algebra.* Springer, New York, 1993.

[5] B. Buchberger. *Ein Algorithmisches Kriterium für die Lösbarkeit eines Algebraischen Gleichungssystems.* Aequationes Mathematicae **4** nr. 3, 374–383, 1970.

[6] B. Buchberger. *A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases.* In E.W. Ng (redactie), Symbolic and Algebraic Computation, EUROSAM 1979. Lecture Notes in Computer Science **72**, 3–21. Springer, Berlin–Heidelberg, 1979.

[7] B. Buchberger. *A Note on the Complexity of Constructing Gröbner-Bases.* In J.A. van Hulzen (redactie), Computer Algebra, EUROCAL 83. Lecture Notes in Computer Science **162**, 137–145. Springer, Berlin–Heidelberg, 1983.

[8] B. Buchberger. *Gröbner Bases. An Algorithmic Method in Polynomial Ideal Theory.* In N.K. Bose (redactie), Multidimensional Systems Theory, Progress, Directions and Open Problems in Multidimensional Systems, 184–232. D. Reidel Publishing Company, Dordrecht, 1985.

[9] M. Caboara. *A Dynamic Algorithm for Gröbner Basis Computation.* In M. Bronstein (redactie), ISSAC 1993, Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, 275–283. ACM Press, New York, 1993.

[10] S. Collart, M. Kalkbrener, D. Mall. *Converting Bases with the Gröbner Walk.* Journal of Symbolic Computation **24**, 465–469, 1997.

[11] D.A. Cox, J.B. Little, D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer, New York, 3^{e} editie, 2007.

[12] T.W. Dubé. *The Structure of Polynomial Ideals and Gröbner Bases.* SIAM Journal on Computing **19** nr. 4, 750–773, 1990.

[13] T.W. Dubé, B. Mishra, C.K. Yap. *Complexity of Buchberger's Algorithm for Gröbner Bases.* Technisch Rapport, Courant Institute of Mathematical Sciences, New York University, 1995.

[14] D. Eisenbud. *Commutative Algebra, with a View Toward Algebraic Geometry.* Springer, New York, 1^{e} editie, 1995.

[15] K. Fukuda, A.N. Jensen, N. Lauritzen, R. Thomas. *The Generic Gröbner Walk.* Journal of Symbolic Computation **42**, 298–312, 2007.

[16] G. Gallo, B. Mishra. *A Solution to Kronecker's Problem.* Applicable Algebra in Engineering, Communication and Computing **5** nr. 6, 343–370. Springer, Berlin–Heidelberg, 1994.

[17] R. Gebauer, H.M. Möller. *On an Installation of Buchberger's Algorithm.* Journal of Symbolic Computation **6**, 275–286, 1988.

[18] A. Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso. *"One Sugar Cube, Please" or Selection Strategies in the Buchberger Algorithm.* In S. Watt (redactie), ISSAC 1991, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, 49–54. ACM Press, New York, 1991.

[19] M. Giusti. *Some Effectivity Problems in Polynomial Ideal Theory.* In B.F. Caviness (redactie), EUROCAL 85, European Conference on Computer Algebra. Lecture Notes in Computer Science **204**, 159–171. Springer, Berlin–Heidelberg, 1985.

[20] O. Golubitsky. *Converging Term Order Sequences and the Dynamic Buchberger Algorithm.* Preprint, 2006.

[21] P. Gritzmann, B. Sturmfels. *Minkowski Addition of Polytopes: Computational Complexity and Applications to Gröbner Bases.* SIAM Journal of Discrete Mathematics **6** nr. 2, 246–269, 1993.

[22] H. Hong, J. Perry. *Are Buchberger's Criteria Necessary for the Chain Condition?* Journal of Symbolic Computation **42**, 717–732, 2007.

[23] D.T. Huynh. *A Superexponential Lower Bound for Gröbner Bases and Church-Rosser Commutative Thue Systems.* Information and Control **68**, 196–206, 1986.

[24] D.T. Huynh. *The Complexity of the Membership Problem for Two Subclasses of Polynomial Ideals.* SIAM Journal on Computing **15** nr. 2, 581–594, 1986.

[25] C. Kollreider, B. Buchberger. *An Improved Algorithmic Construction of Gröbnerbases for Polynomial Ideals.* ACM SIGSAM Bulletin **12** nr. 2, 27–36, 1978.

[26] D. König. *Theorie der Endlichen und Unendlichen Graphen. Kombinatorische Topologie der Streckenkomplexe.* Chelsea Publishing Company, New York, 1950.

[27] U. Koppenhagen, E.W. Mayr. *Optimal Gröbner Base Algorithms for Binomial Ideals.* In F. Meyer auf der Heide, B. Monien (redactie), Automata, Languages and Programming, ICALP 96. Lecture Notes in Computer Science **1099**, 244–255. Springer, Berlin–Heidelberg, 1996.

[28] K. Kühnle, E.W. Mayr. *Exponential Space Computation of Gröbner Bases.* In Y.N. Lakshman (redactie), ISSAC 1996, Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, 63–71. ACM Press, New York, 1996.

[29] D. Lazard. *Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations.* In J.A. van Hulzen (redactie), Computer Algebra, EUROCAL 83. Lecture Notes in Computer Science **162**, 146–156. Springer, Berlin–Heidelberg, 1983.

[30] H. Lombardi, H. Perdry. *The Buchberger Algorithm as a Tool for Ideal Theory of Polynomial Rings in Constructive Mathematics.* In B. Buchberger, F. Winkler (redactie), Gröbner Bases and Applications. London Mathematical Society Lecture Note Series **251**, 393–407, 1998.

[31] E.W. Mayr. *Some Complexity Results for Polynomial Ideals.* Journal of Complexity **13** nr. 3, 303–325, 1997.

[32] E.W. Mayr, A.R. Meyer. *The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals.* Advances in Mathematics **46** nr. 3, 305–329, 1982.

[33] H.M. Möller, F. Mora. *Upper and Lower Bounds for the Degrees of Groebner Bases.* In J. Fitch (redactie), EUROSAM 84, International Symposium on Symbolic and Algebraic Computation. Lecture Notes in Computer Science **174**, 172–183. Springer, Berlin–Heidelberg, 1984.

[34] T. Mora, L. Robbiano. *The Gröbner Fan of an Ideal.* Journal of Symbolic Computation **6**, 183–208, 1988.

[35] G. Moreno Socías. *An Ackermannian Polynomial Ideal.* In H.F. Mattson, T. Mora, T.R.N. Rao (redactie), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Lecture Notes in Computer Science **539**, 269–280. Springer, Berlin–Heidelberg, 1991.

[36] G. Moreno Socías. *Length of Polynomial Ascending Chains and Primitive Recursiveness.* Mathematica Scandinavica **71**, 181–205, 1992.

[37] H. Perdry. *Aspects Constructifs de la Théorie des Corps Valués (précédée d'un chapitre sur la noetherianité constructive).* Ph.D. thesis, Université de Franche–Comté, 2001.

[38] L. Robbiano. *Term Orderings on the Polynomial Ring.* In B.F. Caviness (redactie), EUROCAL 85, European Conference on Computer Algebra. Lecture Notes in Computer Science **204**, 513–517. Springer, Berlin–Heidelberg, 1985.

[39] S.C. Schaller. *Algorithmic Aspects of Polynomial Residue Class Rings.* Ph.D. thesis, University of Wisconsin–Madison, 1979.

[40] F. Winkler. *On the Complexity of the Gröbner-Bases Algorithm over $K[x, y, z]$.* In J. Fitch (redactie), EUROSAM 84, International Symposium on Symbolic and Algebraic Computation. Lecture Notes in Computer Science **174**, 184–194. Springer, Berlin–Heidelberg, 1984.

[41] C.K. Yap. *A New Lower Bound Construction for Commutative Thue Systems with Applications.* Journal of Symbolic Computation **12** nr. 1, 1–27, 1991.