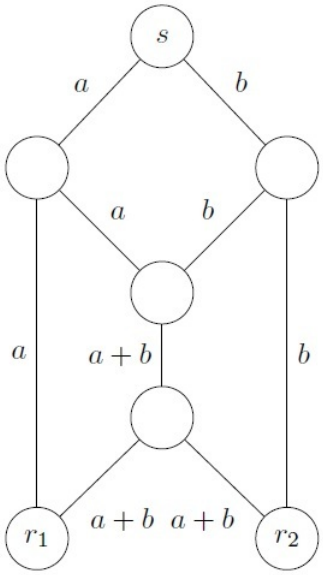
Lineær netværkskodning

Hvordan man løser et lineært netværkskodningsproblem med Gröbner-baser



Thomas Vestergaard

Specialeafhandling i Matematik

Vejleder: Diego Ruano

Aalborg Universitet

Institut for Matematiske Fag

Fredrik Bajers Vej 7 G • 9220 Aalborg Øst • Danmark

AALBORG UNIVERSITET

Institut for Matematiske Fag
Fredrik Bajers Vej 7G
9220 Aalborg Øst
Telefon 99 40 88 04
Fax 98 15 81 29
http://www.math.aau.dk

Titel: Lineær netværkskodning

Projektperiode: 1.sep. 2011-6.jan.2012

Projektgruppe: G4-103

Skrevet af:

Thomas Vestergaard

Vejleder: Diego Ruano

Oplagstal: 4

Sidetal: 79

Bilagsantal og –art: Ingen

Afsluttet: 6. jan. 2012.

Synopsis:

Formålet med denne specialeafhandling er at forstå og forklare artiklen *Aspects of random network coding* af Lektor ved Aalborg Universitet Olav Geil og tidligere Phd-studerende Casper Thomsen, og herunder Gröbnerbasisteori. Et af hovedresultaterne er Fodaftryksgrænsen, som er med til at give et kriterium for, hvornår et lineært netværkskodningsproblem er løseligt. For at bevise dette kriterium benyttes flere store sætninger fra Gröbnerbasisteorien, hvilket inkluderer resulater som Dicksons lemma, Hilberts basissætning, Buchbergers kriterium og Buchbergers algoritme. Til at eksemplificere resultater fra Gröbnerbasisteorien anvendes computerprogrammet Singular.

Efter at have opbygget en værkstøjskasse til forståelse af begrebet netværkskodning, beskrives først idéen med netværkskodning, hvorefter en mere teoretisk gennemgang følger. Det vil herefter blive vist, hvordan man sikrer en høj sandsynlighed for at alle modtagere i et netværk får al den ønskede information. I afsnittet der følger præsenteres endvidere en algoritme til bestemmelse af flows ud fra et givet flowsystem til et netværk. Som anvendelse og illustration af begreberne tages udgangspunkt i Butterfly-netværket.

Kapitel 1

Abstract

Network Coding Theory is one of the newest research areas within mathematics end engineering. For the last 20 years the research has been moving forward, and the idea is used many applications from the everyday life. One example is wireless cellphones. The cellphones are connected in a data transmitting network. The objective of this thesis is to understand and explain the article *Aspects of random network coding* by associate professor at Aalborg University H. Olav Geil and former Phd. student Casper Thomsen.

A network or more specifically a computer network is a collection of computers connected, so they can exchange data. Network coding is quite simply the transmission of data from a source to a certain amount of receivers, and transmission must be noiseless. That is, there can not be any data loss on the way through the network. Data transmitted over point-to-point distances in a network, is best illustrated by a directed graph $G(V, E)$. Here V is the nodes and E is the edges. By $S = \{s_1, \ldots, s_{|S|}\} \subseteq V$, we mean the senders and by $R = \{r_1, \ldots, r_{|R|}\} \subseteq V$, we mean the recievers of the network. One of the most simple network examples is shown on the frontpage of the report. It is called a Butterfly network because of its structure, which is similar to the body of a butterfly. The article *Aspects of random network coding* and therefore the report focuses on *linear* network coding. Network coding is linear, when the message sent takes values in a final field $\mathbb{F}_q$, and when the coding and decoding is done linearly over $\mathbb{F}_q$.

Now, a natural question to ask regarding a network is whether a given network actually works and transmits every piece of information to all recievers, and if the network does it effectively. Effectively refers to if the transmission of data is done within a standard time limit. To answer these questions we will turn to the theory of a Groebner basis. A Groebner basis G is a particular kind of generating subset of an ideal I in a polynomial ring $k[x_1, \ldots, x_n]$, and they have many applications. Groebnerbases was firstly introduced by professor of Computer Mathematics Bruno Buchberger, who named them after his advisor Wolfgang Groebner. The reason why they are such a powerful tool in both mathematics and engineering is, that they are relatively easy to understand. But most importantly they solve complicated problems regarding final fields.

The first three chapters of the thesis are the abstract, the preface, and the introduction, and their meaning is obvious. The first real chapter of the thesis is called Groebner basis theory, and it holds several key results. The first section of chapter 4 holds some general information on ideals in a polynomial ring $k[x_1, \ldots, x_n]$. We then proceed by exploring monomial orderings. Such

orderings are important for submitting the division algorithm on polynomials, and the division algorithm plays an important role in solving, what is known as the *ideal membership problem*: If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, how do we decide if a polynomial $f \in k[x_1, \ldots, x_n]$ is contained in the ideal $\langle f_1, \ldots, f_s \rangle$. The answer is stated in Buchbergers Criterion, section 4.5, which has to do with something called S-polynomials.

Another problem concerning polynomial ideals is the *ideal description problem*: Is it possible to write every polynomial ideal as $\langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. The answer to this is yes. In section 4.3 the first key result is presented. It is Dickson's Lemma, which solves the ideal description problem for a special kind of polynomial ideal. The lemma extends to The Hilbert Basis theorem, which solves the problem for all polynomial ideals. As a bonus The Hilbert Basis Theorem gives rise to Groebner bases. Section 4.5 and 4.6 explores the applications of Groebner bases and gives an algorithm for producing Groebner bases. Sections 4.7 and 4.8 explores the relationsship between ideals and varieties, while sections 4.9 and 4.10 involves functions between varieties. The goal of these sections are also to establish the Footprint Bound in the last section of this chapter. This specific bound holds the key to linear network coding and marks the end of the chapter.

Chapter 5 is all about linear network coding. The chapter begins with a short introduction to the topic, then a more theoretical approach follows. The section following shows how to ensure, that there is a high probability that all receivers in a network gets all information. Afterwards an algorithm for determining the flow from a given flow system is presented. Results will be illustrated through the Butterfly network. In the end we will see what else can be said about the probability of succes.

Kapitel 2

Forord

Dette er en specialeafhandling indenfor hovedretningen Diskret Matematik ved Institut for Matematiske Fag, Aalborg Universitet. Specialet er udarbejdet i perioden 1. sep. 2011 - 6. jan. 2012. Målet med specialet er at forstå og forklare artiklen [2010 Geil & Thomsen] og herunder at forstå og forklare Gröbnerbasisteori og netværkskodning. Der forudsættes et basalt kendskab til grafteori, abstrakt algebra og lineær algebra. Specialet er et forsøg på at kaste lys over netværkskodning for almindelige studerende og ikke-professorere.

I rapporten er vigtige begreber skrevet med kursiv første gang de nævnes. Litteraturhenvisninger angives som (udgivelsesår, Forfatter(e)) og litteraturlisten kan findes bagerst i rapporten. I starten af hvert afsnit anføres, hvilke kilder afsnittet er baseret på. Der gøres endvidere opmærksom på, at der ved nogle sætninger er udeladt beviser, og der vil istedet være en henvisning til stedet, hvor beviset kan findes. Henvisninger i parentes som (4.28) henviser til et ligningsnummer, mens sætninger mv. henvises til som f.eks. sætning 4.31. Til nogle eksempler er brugt computerprogrammet Singular og Singular-koden vil være inkluderet. For mere information om programmet henvises til http://www.singular.uni-kl.de. I nogle af eksemplerne vil Singular-koden være inkluderet.

Til slut vil jeg gerne takke min vejleder Diego Ruano for et stort engagement og faglig vejledning gennem hele processen. Endvidere skal der lyde en tak til Martin Steffano for kyndig vejledning indenfor særligt Gröbnerbasisteorien.

Thomas Vestergaard
Aalborg d. 6. jan. 2012

Indhold

Kapitel 3

Indledning

Netværkskodning er et af de nyere forskningsområder indenfor matematikken, og det er et område, hvor der er sket stor forskningsmæssig fremgang indenfor de sidste 10 til 20 år. Denne specialeafhandling vil beskæftige sig med emnet lineær netværkskodning, som er fokusområdet i artiklen [2010 Geil & Thomsen] af Lektor H. Olav Geil ved Aalborg Universitet og tidligere Phd.-studerende Casper Thomsen, og herunder Gröbnerbasisteori.

Et netværk eller rettere sagt et computernetværk er en samling computere forbundet af netværksudstyr, så de kan udveksle data. Netværkskodning drejer sig i al sin enkelthed om transmission af data fra en kilde til en bestemt mængde af modtagere, og transmissionen skal være støjfri. Det vil sige, der må ikke gå noget data tabt undervejs. Data transmitteres over punkt-til-punkt afstande i et netværk, hvilket bedst illustreres ved en orienteret graf. De fundamentale tanker bag netværkskodning blev første gang introduceret i forbindelse med kommunikation imellem satelitter i 1999 i skriftet *Distributed Source Coding for Satellite Communications* af R. W. Yeung and Z. Zhang. Idéerne blev senere videreudviklet i 2000 i skriftet *Network Information Flow* af R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Det var også først i år 2000, at begrebet netværkskodning første gang opstod.[2006 R. W. Yeung et al.]

Som før nævnt vil dette speciale være rettet mod lineær netværkskodning. Kodningen er lineær, såfremt at data består af værdier tilhørende et endeligt legeme $\mathbb{F}_q$, og hvis kodningen samt dekodningen udføres lineært over $\mathbb{F}_q$. Det store spørgsmål vedrørende lineær netværkskodning, og netværkskodning generelt, er, hvornår man kan være sikker på, at det virker og med hvor stor en hastighed netværket kan transmittere data. Det vil sige, hvor effektivt er netværket. Til at besvare denne problemstilling rettes opmærksomheden mod Gröbnerbasisteorien. Udover deres betydning for netværkskodning er Gröbnerbaser også interessante i sig selv. De er et meget kraftfuldt værktøj indenfor matematikken og ingeniørvidenskaben. Dette skyldes, at de er relativt lette at forstå, men vigtigst af alt så løser de komplicerede problemer, der har med endelige legemer at gøre. Derfor vil jeg i specialet gå i dybden med Gröbnerbasisteorien og også nå omkring flere emner, end hvad der er nødvendigt, for at godtgøre hvornår et lineært netværk virker efter hensigten.

De første tre kapitler i Specialet er forord, et engelsk resumé og indledningen, som anses som værende en naturlig del af en specialeafhandling. I Kapitel 4 findes Gröbnerbasisteorien. Dette kapitel indbefatter hovedresultater som Dicksons's Lemma, Buchbergers Basissætning, Buchbergers Algoritme og Fodaftryksgrænsen og beviserne herfor. Det første afsnit i kapitel 4 indeholder nogle

generelle oplysninger om idealer i et polynomium ring $k[x_1, \ldots, x_n]$. Efter dette følger et afsnit om monomiel ordning. Monomielle ordninger er især vigtige i forbindelse med division af polynomier i flere variable (Divisionsalgoritmen). Divisionsalgoritmen spiller en vigtig rolle i løsningen af *ideal membership problem*: Hvis $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, tilhører et polynomium $f \in k[x_1, \ldots, x_n]$ da idealet, frembragt af $f_1, \ldots, f_s$? Svaret er ikke altid ja, men det vil blive vist i Buchbergers Kriterium fra afsnit 4.5, at problemet kan løses.

Et andet problem vedrørende polynomielle idealer er *Ideal Description Problem*: Kan man udtrykke ethvert polynomielt ideal ved $\langle f_1, \ldots, f_s \rangle$ for nogle $f_1, \ldots, f_s \; ik[x_1, \; ldots, x_n]$. Svaret på dette er ja. I afsnit **??** præsenteres Dicksons lemma, der løser the ideal description problem for en særlig type af polynomielle idealer. Dickson's lemma udvides derefter til Hilbert Basis sætning, som løser problemet for alle polynomielle idealer. Som en sidegevinst i beviset for Hilberts Basissætning opstår de såkaldte Gröbnerbaser. I Afsnit 4.5 og 4.6 udforskes Gröbnerbasers egenskaber og en algoritme til at producere Groebnerbaser gives. Afsnit **??** og 4.8 udforsker forholdet mellem idealer og affine varieteter, mens afsnit **??** og 4.10 omhandler indbyrdes funktioner mellem affine varieteter. Målet med dette kapitel er også Fodaftryksgrænsen, som bevises sidst i kapitlet. Denne specifikke grænse er nøglen til at afgøre, hvornår et lineært netværkskodningsproblem har en løsning.

Resultater og generel viden om begreber diskuteret i Gröbnerbasisteorien vil blive sat i forbindelse med lineær netværkskodning i kapitel 5. Kapitel 5 omhandler således lineær netværkskodning og i særdeleshed, hvordan man sikrer, at et netværk virker. Kapitlet indeholder først en lille introduktion til emnet, hvorefter en mere teoretisk tilgang følger. Dernæst vises, hvordan man sikrer, at alle modtagere i et netværk får al information og en algoritme til bestemmelse af flows ud fra et givet flowsystem præsenteres. Til slut diskuteres sandsynligheden for, at et netværk virker, hvis kodningskoefficienterne til systemet er valgt vilkårligt.

Kapitel 4

Gröbnerbasisteori

Dette kapitel indeholder den mere teoretiske del af projektet. Som indikeret i indledningen er formålet med projektet at belyse evt. problemstillinger indenfor lineær netværkskodning. Der ønskes altså en værkstøjskasse med redskaber nok til at kunne forstå og anvende lineær netværkskodning. Indenfor netværkskodning arbejdes der med polynomier af flere variable. I kapitlet betragtes derfor polynomierne som ét hele ved at fokusere på de såkaldte polynomiumsidealer. Polynomiumsidealerne vil danne udgangspunktet, for til sidst i teorien at nå til Fodaftryksgrænsen i afsnit 4.11. Undervejs stiftes bekendtskab med de såkaldte Gröbnerbaser, som bl.a. gør det muligt at sammenligne polynomiumsidealer. Kapitlet bygger på teori fra [2008 Cox, Little & O´Shea] suppleret op med teori fra [2003 Lauritzen], [2000 Justesen & Høholdt] og [2008 Greuel & Pfister].

4.1 Idealer

I det følgende afsnit defineres polynomielle idealer og nogle vigtige egenskaber for disse. Det er målet at kunne opskrive en formel, som indeholder alle idealer. I beviset for dette opstår et såkaldt Groebner basis, som vi senere vil se er meget anvendelige i løsningen af netværksproblemer. Inden definitionen af idealer, er der et begreb, som først skal berøres, nemlig affine varianter.

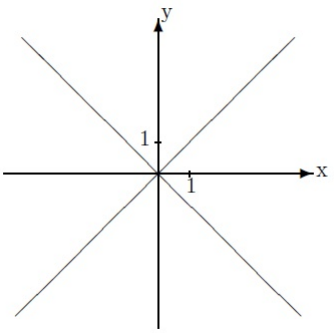
Definition 4.1 (Affine varieteter)**.** *Hvis k er et legeme og $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, så defineres en affin varietet som værende*

$$\boldsymbol{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n | f_i(a_1, \ldots, a_n) = 0 \quad \textit{for alle } i = 1, \ldots, s\}\,.$$

$\boldsymbol{V}(f_1, \ldots, f_s)$ siges da at være en affin varietet defineret ved polynomierne $f_1, \ldots, f_s$.

Det bemærkes, at en affin varietet faktisk er mængden af alle løsninger til $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$. For polynomier af en variabel er en affin varietet til dette polynomium lig hvad der på sædvanligvis kendes som rødderne eller nulpunkterne. Denne situation er nem at skitsere i et koordinatsystem. Det er også muligt at skitsere løsningerne for et polynomium af to variable. F.eks. kan de affine varieteter $\mathbf{V}(f)$ for $f = x^2 - y^2$ skitseres som på figur 4.1.

Det ses, at det ikke er helt så nemt at bestemme affine varieteter for polynomier af flere variabler



Figur 4.1: Figuren illusterer de affine varieteter for $f = x^2 - y^2$.

end to, men med indførslen af idealer kan dette problem omgås. Idealer sikrer altså en matematisk kontekst, som gør det muligt at regne med affine varieteter.

Definition 4.2. *En delmængde $I \subseteq k[x_1, \ldots, x_n]$ er et polynomielt ideal, såfremt I opfylder, at*

(i) $0 \in I$.

(ii) Hvis $f, g \in I$, *så* $f + g \in I$.

(iii) Hvis $f \in I$ *og* $h \in k[x_1, \ldots, x_n]$, *så* $hf \in I$.

Et eksempel på et ideal, som vi også senere vil benytte er illustreret i følgende definition. Senere vil det blive vist, at alle idealer kan udtrykkes på denne måde(se sætning 4.7).

Definition 4.3. *Lad $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Da sættes*

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{n} h_i f_i | h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\} \tag{4.1}$$

Først er vi dog nødt til at godtgøre, at $\langle f_1, \ldots, f_s \rangle$ er et ideal. Påstanden vises i nedenstående lemma.

Lemma 4.1. *Hvis $f_1 \ldots, f_s \in k[x_1, \ldots, x_n]$, da er $\langle f_1, \ldots, f_s \rangle$ et ideal i $k[x_1, \ldots, x_n]$. Herved siges $\langle f_1, \ldots, f_s \rangle$ at være idealet genereret ud fra $f_1 \ldots, f_s$.*

Bevis. Lad $f_1 \ldots, f_s \in k[x_1, \ldots, x_n]$. Hvis $\langle f_1, \ldots, f_s \rangle$ er et ideal, skal det opfylde de tre betingelser i definition 4.2. For det første så da $\sum_{i=1}^{s} 0 \cdot f_i = 0$, for $0 \in k[x_1, \ldots, x_n]$, da gælder, at $0 \in \langle f_1, \ldots, f_s \rangle$. Hermed er (i) opfyldt. Antag nu at $f = \sum_{i=1}^{s} p_i f_i$ og $g = \sum_{i=1}^{s} q_i f_i$. Herved ses, at

$$\begin{aligned} f + g &= p_1 f_1 + \cdots + p_s f_s + q_1 f_1 + \cdots + q_s f_s \\ &= (p_1 + q_1) f_1 + \cdots + (p_s + q_s) f_s = \sum_{i=1}^{s} (p_i + q_i) f_i \end{aligned}$$

Idet p_i'erne og q_i'erne ligger i $k[x_1, \ldots, x_n]$, så gør også $p_i + q_i$ for $i = 1, \ldots, s$. Ergo er også (ii) opfyldt. På samme vis ses, at for $h \in k[x_1, \ldots, x_n]$, så

$$\begin{aligned} hf &= h(p_1 f_1 + \cdots + p_s f_s) \\ &= hp_1 f_1 + \cdots + hp_s f_s = \sum_{i=1}^{n} (hp_i) f_i \end{aligned}$$

Som før ses det her, at $hp_i \in k[x_1, \ldots, x_n]$, hvorfor den tredie betingelse også er opfyldt. □

Der indføres følgende terminologi vedrørende idealet frembragt af polynomier fra $k[x_1, \ldots, x_n]$:

Definition 4.4. *Et ideal I siges at være endeligt genereret, hvis der findes polynomier $f_1 \ldots, f_s \in k[x_1, \ldots, x_n]$, sådan at $I = \langle f_1, \ldots, f_s \rangle$. Polynomierne $f_1, \ldots, f_s$ siges da at være et basis for I.*

Ikke alle idealer er endeligt genererede. Idealer, som er endeligt genererede, kaldes også for Nötherianske idealer. I den følgende følgende sætning vises, at den affine varietet kun afhænger af idealet frembragt eller genereret af de polynomier, som hører til varieteten. Bemærk, at et polynomielt ideal kan have mange forskellige baser, men i afsnit 4.4 vil et særligt anvendeligt basis (Gröbner-basis) blive præsenteret. Selvom to ens idealer har forskelligt basis, ændrer det dog ikke på de de tilhørende affine varieteter. Med andre ord så hvis to ens idealer har forskelligt basis, da er de fælles nulpunkter for hver af de to baser faktisk ens. Hvorfor er beskrevet i nedenstående sætning.

Sætning 4.1. *Hvis $f_1, \ldots, f_s$ og $g_1, \ldots, g_t$ er basis for det samme ideal i $k[x_1, \ldots, x_n]$, sådan at $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, da gælder, at $\boldsymbol{V}(f_1, \ldots, f_s) = \boldsymbol{V}(g_1, \ldots, g_t)$.*

Bevis. Det skal vises, at når $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, så

$$\mathbf{V}(f_1, \ldots, f_s) \subseteq \mathbf{V}(g_1, \ldots, g_t) \text{ og } \mathbf{V}(f_1, \ldots, f_s) \supseteq \mathbf{V}(g_1, \ldots, g_t).$$

Kun implikationen $\mathbf{V}(f_1, \ldots, f_s) \subseteq \mathbf{V}(g_1, \ldots, g_t)$ vises, da den anden implikation bevises similært. Tag $\overline{x} \in \mathbf{V}(f_1, \ldots, f_s)$, så betyder det jvf. definition 4.1, at $f_1(x) = 0, \ldots, f_s(x) = 0$. Pr. antagelse og ved brug af definition 4.3 haves, at

$$\begin{aligned} \langle g_1, \ldots, g_t \rangle &= \langle f_1, \ldots, f_s \rangle \\ &= \left\{ \sum_{i=1}^{n} h_i f_i \mid h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\} \end{aligned}$$

Det vil sige, at $g_i = \sum_{j=0}^{t} a_j f_j$. Indsættes x ses, at hvert led i linearkombinationen giver 0, hvorfor hele summen giver nul. Derfor gælder, at $x \in \mathbf{V}(g_1, \ldots, g_t)$. □

Sætning 4.1 giver en metode til at bestemme affine varieteter. Selvom basis for et ideal ændres, har det ikke nogen indvirkning på de affine varieteter. Det illustreres bedst i et eksempel med to forskellige basis for det samme ideal.

Eksempel 4.1. *Antag at man ønsker at finde $\boldsymbol{V}(x + xy, y + xy, x^2, y^2)$. Det kan vises, at*

$$\left\langle x + xy, y + xy, x^2, y^2 \right\rangle = \langle x, y \rangle ,$$

hvorfor sætning 4.1 kan anvendes. Ifølge denne gælder, at $\boldsymbol{V}(x + xy, y + xy, x^2, y^2) = \boldsymbol{V}(x, y)$, og dermed ses, at $\boldsymbol{V}(x + xy, y + xy, x^2, y^2) = \{0, 0\}$. Selvom det til at starte med ikke er trivielt at bestemme den affine varietet til et givent ideal, kan man gøre det nemmere for sig selv ved at udtrykke idealets basis på en simplere måde.

Indtil nu har vi beskæftiget os med affine varieteter som værende de punkter, hvor polynomier af flere variable har fælles nulpunkter. Givet en affin varietet V er spørgsmålet da, om der findes flere polynomier, som forsvinder i V. For at kunne afgøre det defineres en mængde, som indeholder alle de polynomier, som forsvinder i V.

Definition 4.5. *Lad $V \subseteq k^n$ være en affin varietet, hvor $k^n = \{(a_1, \ldots, a_n) | a_1, \ldots, a_n \in k\}$, ketlegeme. Mængden bestående af polynomier, som forsvinder i V, er da givet ved*

$$\boldsymbol{I}(V) = \{f \in k[x_1, \ldots, x_n] | f(a_1, \ldots, a_n) = 0 \text{ for alle } (a_1, \ldots, a_n) \in V\}.$$

Denne mængde har nogle særlig egenskaber. Faktisk er mængden et ideal, hvilket ses af det følgende lemma. Mængden vil blive refereret til som idealet for V.

Lemma 4.2. *$\boldsymbol{I}(V)$ er et ideal.*

Bevis. For at bevise lemmaet skal det vises, at $\mathbf{I}(V)$ opfylder alle tre betingelser i definition 4.2. For det første bemærkes det, at nulpolynomiet forsvinder på k^n og dermed på V, og da $\mathbf{I}(V)$ består af alle de polynomier, som forsvinder på V, så $f = 0 \in \mathbf{I}(V)$. For at bevise den anden betingelse i definitionen af et ideal, tag $f, g \in \mathbf{I}(V)$ og $a \in V$ Da gælder, at

$$(f + g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0.$$

Det vil sige, at $f + g$ også forsvinder på V, hvorfor $f + g \in I(V)$. På samme vis ses ved at tage $h \in k[x_1, \ldots, x_n]$, at

$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0,$$

hvorved $hf \in \mathbf{I}(V)$. □

Eksempel 4.2. *Følgende eksempel bliver genbrugt i beviset for lemma 4.3. Betragt affin varietet $\{(0,0)\}$. Idealet til $\{(0,0)\}$ består således af alle polynomier, som forsvinder i punktet $(0,0)$. Påstanden er da, at*

$$\boldsymbol{I}(\{(0,0)\}) = \langle x, y \rangle.$$

Påstanden er sand, hvis $\boldsymbol{I}(\{(0,0)\}) \subseteq \langle x, y \rangle$ og $\boldsymbol{I}(\{(0,0)\}) \supseteq \langle x, y \rangle$. Tag først $f \in \langle x, y \rangle$, da kan f udtrykkes ved $h_1 x + h_2 y$, hvor $h_1, h_2 \in k[x_1, x_2]$. Det ses klart, at f forsvinder, hvis $x = 0$ og $y = 0$, hvorfor $f \in \boldsymbol{I}(\{(0,0)\})$. Det vil sige, at $\boldsymbol{I}(\{(0,0)\}) \supseteq \langle x, y \rangle$.

Tag nu istedet $f = \sum_{i,j} a_{i,j} x^i y^j$ og antag, at f forsvinder i $(0,0)$. Det betyder, at

$$\begin{aligned} f(0,0) &= a_{0,0} x^0 y^0 \\ &= a_{0,0} = 0. \end{aligned}$$

Derfor ses, at

$$\begin{aligned} f = a_{0,0} + f &= \sum_{i,j \neq 0,0} a_{i,j} x^i y^j \\ &= 0 + \sum_{i>0,j} a_{i,j} x^i y^j + \sum_{i,j>0} a_{i,j} x^i y^j \\ &= \left(\sum_{i>0,j} a_{i,j} x^{i-1} y^j \right) x + \left(\sum_{i,j>0} a_{i,j} x^i y^{j-1} \right) y \in \langle x, y \rangle, \end{aligned}$$

hvorved også $\boldsymbol{I}(\{(0,0)\}) \subseteq \langle x, y \rangle$.

For at opsummere er det nu muligt, givet polynomier $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ først at bestemme punkterne, hvor alle polynomierne forsvinder, for dernæst at bestemme alle polynomier, som forsvinder i netop de punkter. Med andre ord går man fra at bestemme affine varieteter for givne polynomier $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ og videre til at bestemme idealet til de affine varieteter $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$. Det store spørgsmål er da, om idealet til de affine varieteter er lig idealet frembragt af polynomierne (se def. 4.3). Det er de ikke nødvendigvis, men det følgende lemma indikerer, at der i hvert fald er en sammenhæng.

Lemma 4.3. *Hvis $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, så gælder, at $\langle f_1, \ldots, f_s \rangle \subseteq \boldsymbol{I}(\boldsymbol{V}(f_1, \ldots, f_s))$. Der behøver ikke at være lighed.*

Bevis. For $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ tag da $f \in \langle f_1, \ldots, f_s \rangle$. Ifølge definition 4.3 så $f = \sum_{i=1}^{n} h_i f_i$, hvor $h_i \in k[x_1, \ldots, x_n]$. I og med at $f_1, \ldots, f_s$ forsvinder på $\mathbf{V}(f_1, \ldots, f_s)$, så må f, som jo er en linearkombination af f_i'er, også forsvinde på $\mathrm{V}(f_1, \ldots, f_s)$. Det vil sige, da $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ indeholder alle polynomier, som forsvinder på $\mathbf{V}(I)$, så må f være blandt disse, og dermed $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.

Ved at give et eksempel på en situation, hvor $\langle f_1, \ldots, f_s \rangle \subsetneq \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, vises den anden påstand i lemmaet. Lad $f_1 = x^2$ og $f_2 = y^2$. Det ses, at $\mathbf{V}(f_1, f_2) = \{(0,0)\}$, da $f_1(0) = 0^2 = 0$ og $f_2(0) = 0^2 = 0$. Ifølge eksempel 4.2 så $\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle$, hvorved at også $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) = \langle x, y \rangle$. Bemærk, at polynomier frembragt af x^2 og y^2 er udtrykt som $h_1(x,y)x^2 + h_2(x,y)y^2$. Monomier i den type af polynomier har grad mindst to. Ergo $x \notin \langle f_1, f_2 \rangle$ og dermed $\langle f_1, f_2 \rangle \subsetneq \mathbf{I}(\mathbf{V}(f_1, f_2))$. □

Forlader vi igen kort idéen om, at idealet til affine varieteter, som er defineret ud fra polynomier $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, skal kædes sammen med $\langle f_1, \ldots, f_s \rangle$ fra definition 4.3, så kan der istedet siges noget om de affine varieteter og de tilhørende idealer.

Sætning 4.2. *For affine varieteter $V, W \in k^n$, hvor k er et legeme gælder, at*

(i) $V \subseteq W \Leftrightarrow I(V) \supseteq I(W)$,

(ii) $V = W \Leftrightarrow I(V) = I(W)$.

Bevis. Først vises (i). Antag, at $V \subseteq W$. Derved indeholder V nogle eller alle vektorer fra W. Et polynomium forsvinder på W, hvis det for hver af vektorerne i W er lig 0. Da V består af nogle eller alle af vektorerne fra W, så forsvinder f også på V. Det vil sige, at alle polynomier, som forsvinder på W, også forsvinder på V. Heraf $\mathbf{I}(V) \supseteq \mathbf{I}(W)$.

Antag nu istedet, at $\mathbf{I}(V) \supseteq \mathbf{I}(W)$. varieteten W er pr. definition givet ud fra polynomier $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Idet at $I(W)$ består af alle polynomier, som forsvinder på W, så specielt $f_1, \ldots, f_s \in \mathbf{I}(W)$. Ifølge den første antagelse gælder også, at $f_1, \ldots, f_s \in \mathbf{I}(V)$. Herudaf ses, at $f_1, \ldots, f_s$ forsvinder på V. Husk, at W består af alle de vektorer, som indsat i $f_1, \ldots, f_s$ giver 0, og nu er det vist, at V indeholder i hvert fald nogle af dem, hvorved det ses, at $V \subseteq W$.

Beviset for (ii) følger af (i). Antag først at $V = W$. Polynomier, som forsvinder på V, forsvinder også på W, og $\mathbf{I}(V) = \mathbf{I}(W)$ er trivielt opfyldt.

Antag istedet, at $\mathbf{I}(V) = \mathbf{I}(W)$. Der gælder, at

$$\mathbf{I}(V) = \mathbf{I}(W) \Rightarrow \begin{cases} \mathbf{I}(V) \subseteq \mathbf{I}(W) \\ \mathbf{I}(V) \supseteq \mathbf{I}(W) \end{cases} \Leftrightarrow \begin{cases} V \subseteq W \\ V \supseteq W \end{cases}$$

Det sidste lighedstegn fås ved at benytte (i). Ovenstående betyder at hvis $\mathbf{I}(V) = \mathbf{I}(W)$, så hhv. $V \subseteq W$ og $V \supseteq W$, hvorved det ses, at $V = W$. □

Som det ses af ovenstående sætning er det derfor muligt at bestemme affine varieteter entydigt ud fra det tilhørende ideal. I det næste vil vi se nærmere på konstruktionen af de polynomier, som idealer og affine varieteter defineres ud fra. Vi ønsker at vise $f \in I$ hvis og kun hvis f kan skrives på formen som i definition 4.2. Med andre ord at alle elementer i et ideal kan udtrykkes som en linearkombination af polynomier. Sætningen er kendt som Hilberts Basissætning men først før denne kan bevises, indføres monomier og monomiel ordning.

4.2 Monomiel ordning

Dette afsnit er skrevet ud fra [2008 Cox, Little & O´Shea]. Monomiel ordning handler om i hvilken rækkefølge leddene i et polynomium rangordnes. Hvis f.eks. $f = -x^2 - 3 + 2x^5 + 5x + x^4$ ordnes efter potenserne, sådan at det led med højeste potens skrives først, fås da $f = 2x^5 + x^4 - x^2 + 5x - 3$. Polynomier er konstrueret ud fra monomier, og monomierne i f er x^5, x^4, x^2 og x. Mere præcist er et monomium defineret som følgende:

Definition 4.6. *Et monomium i $x_1, \ldots, x_n$ er et produkt udtrykt som*

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Som det ses, består et polynomium af en sum af monomier. Det vil sige, at leddet $x^2y^3z^4$ er et monomium i polynomiet $f = x^2y^3z^4 + 2x - y^2$. Som først indikeret ønskes derfor måder, hvorpå man kan rangordne monomierne. I praksis skal hvert monomium i et polynomium altså sammenlignes med de øvrige monomier. For monomier x^α, x^β, hvis en af følgende tre relationer af opfyldt, siges ordningen da at være total/lineær:

$$x^\alpha > x^\beta, \qquad x^\alpha = x^\beta \qquad \text{og} \qquad x^\alpha < x^\beta. \tag{4.2}$$

En eksempel på en ordning, som ej er lineær, er den naturlige ordning, hvor $x^a y^b < x^c y^d$, hvis $a < c$ og $b < d$. Det ses, at ingen af de ovenstående relationer behøver at være opfyldt for hvert par af monomier. Betragt f.eks. polynomiet $f = x^2y + xy^2$. Ifølge den naturlige ordning er hverken $x^2y < xy^2$, $x^2y = xy^2$ eller $x^2y > xy^2$. Problemet omgås med definitionen af en monomiel ordning, hvor rangordningen altså skal foregå lineært.

Definition 4.7. *En monomiel ordning $>$ på $k[x_1, \ldots, x_n]$ er en relation på mængden af monomier x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, som opfylder, at*

(i) Relationen $>$ er en lineær ordning på $\mathbb{Z}^n_{\geq 0}$.

(ii) Hvis $\alpha > \beta$ og $\gamma \in \mathbb{Z}^n_{\geq 0}$, så $\alpha + \gamma > \beta + \gamma$.

(iii) Alle ikke-tomme delmængder af $\mathbb{Z}^n_{\geq 0}$ har et mindste element, når de er underlagt $>$. Relationen siges da at være velordnet.

At en ordning er velordnet og har et mindste element kan også formuleres som i følgende lemma.

Lemma 4.4. *En ordning $>$ på $\mathbb{Z}^n_{\geq 0}$ er velordnet hvis og kun hvis enhver strengt aftagende følge i $\mathbb{Z}^n_{\geq 0}$,*

$$\alpha(1) > \alpha(2) > \cdots,$$

har en grænse.

Bevis. For at bevise ovenstående lemma, vil vi istedet verificere, at $>$ ikke er velordnet hvis og kun hvis der findes en uendeligt aftagende følge i $\mathbb{Z}^n_{\geq 0}$. Antag først at $>$ ikke er velordnet. Ifølge (iii) i definition 4.7 findes da en ikke-tom delmængde $S \subset \mathbb{Z}^n_{\geq 0}$, som ikke har et mindste element. Vælg nu $\alpha(1) \in S$, da vil $\alpha(1)$ ikke være mindste element i S. Derfor $\alpha(2) < \alpha(1)$ vælges.$\alpha(2)$ er ej heller mindste element, hvorfor vi igen kan vælge $\alpha(3) < \alpha(2)$. Fortsættes på samme vis haves en følge,

$$\alpha(1) > \alpha(2 > \cdots,$$

som er en uendeligt aftagende følge i $\mathbb{Z}^n_{\geq 0}$. Antag nu istedet at en uendeligt aftagende følge,

$$\alpha(1) > \alpha(2 > \cdots,$$

haves. Dermed vil mængden $\{\alpha(1), \alpha(2), \ldots\}$ være en ikke-tom delmængde af $\mathbb{Z}^n_{\geq 0}$, som samtidigt ikke har noget mindste element. □

En måde at arrangere monomier i et polynomium er ud fra monomiernes eksponenter. Det kan gøres på flere forskellige måder. Et eksempel på hvordan eksponenterne er markør for, hvordan monomierne i et polynomium arrangeres ses af følgende definition.

Definition 4.8 (Leksikografisk ordning)**.** *Lad $\alpha = (\alpha_1, \ldots, \alpha_n)$ og $\beta = (\beta_1, \ldots, \beta_n)$, hvor $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Der gælder, at $\alpha >_{lex} \beta$, med $x_1 > x_2 > \ldots > x_n$, hvis komponenten forskellig fra 0 og længst mod venstre i vektoren $\alpha - \beta \in \mathbb{Z}^n$ er positiv. Hvis $\alpha >_{lex} \beta$, så $x^\alpha >_{lex} x^\beta$.*

Eksempel 4.3. *Et eksempel på en leksikografisk ordning er, hvis man betragter polynomiet $f = 5x^4yz^3 - 3x^4y^2z + x$. Med leksikografisk ordning hvor $x > y > z$, vil leddene i polynomiet arrangeres sådan, at $f = -3x^4y^2z + 5x^4yz^3 + x$. Dette ses ved at lade α være potenserne for det første monomium, β det næste og γ det tredie. Dermed fås $\alpha = (4,1,3)$,$\beta = (4,2,1)$ og $\gamma = (1,0,0)$. Heraf ses, at da $\beta - \alpha = (0,1,-2)$ og $\alpha - \gamma = (3,1,3)$, så $x^\beta >_{lex} x^\alpha >_{lex} x^\gamma$.*

At den leksikografiske måde at ordne leddene i et polynomium på rent faktisk også opfylder betingelserne for en monomiel ordning ses af følgende sætning.

Sætning 4.3. *Den leksikografiske ordning på $\mathbb{Z}^n_{\geq 0}$ er en monomiel ordning.*

Bevis. Vi skal vise at den leksikografiske ordning overholder (i)-(iii) i definition 4.7. At $>_{lex}$ er en lineær ordning følger direkte af definition 4.8 og det, at potenserne tilhører $\mathbb{Z}^n_{\geq 0}$.

Lad nu $\alpha >_{lex} \beta$, så haves at værdien på positionen længst mod venstre i $\alpha - \beta$, er positiv. Tag $\gamma \in \mathbb{Z}^n_{\geq 0}$, hvorved det bemærkes, at $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ og $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Ved anvendelse af leksikografisk ordning får hermed, at $\alpha + \gamma - (\beta + \gamma) = \alpha - \beta$, som pr. antagelse er positiv. Dermed er (ii) opfyldt.

Den tredie betingelse vil blive vist ved en modstrid. Antag modsætningsvist at $>_{lex}$ ikke er velordnet. Jvf. lemma 4.4 findes en uendelig strengt aftagende følge

$$\alpha(1) >_{lex} \alpha(2) >_{lex} \cdots,$$

hvor $\alpha(i) \in \mathbb{Z}^n_{\geq 0}, i = 1, 2, \cdots$. Betragt nu de første indgange i vektorerne $\alpha(i)$. Da $\mathbb{Z}^n_{\geq 0}$ er velordnet, findes et k for hvilken den første indgang i $\alpha(k)$ vil være lig den første indgang i $\alpha(k+1)$. De første indgange siges da at være stabile. Det samme gentages nu for $\alpha(k)$ og fremefter indtil den anden indgang også har stabiliseret sig. Fortsættes på samme måde vil der til sidst være et l for hvilken vektorerne ikke længere er forskellige, altså hvor alle indgange i $\alpha(l), \alpha(l+1), \ldots$ er ens. Dette er i modstid med antagelsen om, at $\alpha(l) >_{lex} \alpha(l+1)$. Altså er den leksikografiske ordning også vel-ordnet. □

Et andet eksempel på, hvordan monomierne i et polynomium af flere variable kan arrangeres, er ved den graduerede leksikografiske ordning.

Definition 4.9 (Gradueret leksikografisk ordning)**.** *Lad $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Om α og β siges, at $\alpha >_{grlex} \beta$ med $x_1 > x_2 > \ldots > x_n$ såfremt, at*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

eller, at $|\alpha| = |\beta|$ og $\alpha >_{lex} \beta$.

Eksempel 4.4. *For $\alpha = (10, 1, 0)$ og $\beta = (3, 2, 1)$ ses, at $|\alpha| = 11 > |\beta| = 6$, hvorfor der i dette tilfælde gælder, at $\alpha >_{grlex} \beta$. En anden mulighed er, hvis $\alpha = (4, 2, 0)$ og $\beta = (3, 1, 2)$. I dette tilfælde giver summerne det samme, $|\alpha| = |\beta| = 6$, men det ses også, at $\alpha - \beta = (1, 1, -2)$, hvorfor der også her kan skrives, at $\alpha >_{grlex} \beta$.*

Beviset for at den graduerede leksikografiske ordning også er en monomiel ordning følger samme procedure som for den leksikografiske ordning. En anden meget anvendt ordning er den graduerede reverse leksikografiske ordning.

Definition 4.10 (Gradueret reverse leksikografisk ordning)**.** *Lad $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. Om α og β siges, at $\alpha >_{grevlex} \beta$ såfremt, at*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

eller, at $|\alpha| = |\beta|$ og hvis der for $\alpha - \beta \in \mathbb{Z}^n$ gælder, at den indgang, forskellig fra nul, længst mod højre er negativ.

Eksempel 4.5. *Betragt polynomiet $f = x^2y^3z - x^3z^3$. Vi vil anvende gradueret reverse leksikografisk ordning på monomierne i f. Her sættes $\alpha = (2, 3, 1)$ og $\beta = (3, 0, 3)$. Det ses, at totalgraderne er ens, og da $\alpha - \beta = (-1, 3, -2)$, hvor indgangen længst mod højre er negativ, så $\alpha >_{grevlex} \beta$. Hermed $x^2y^3z >_{grevlex} x^3z^3$.*

Der haves nu redskaber til at ordne polynomier, så det næste skridt må derfor være at klarlægge terminologien og reglerne for, hvordan man opererer med polynomier i flere variable. For bl.a. at undgå forvirring i forhold til sprogbrugen i arbejdet med polynomier, indføres følgende begreber:

Definition 4.11. *Lad $f = \sum_\alpha a_\alpha x^\alpha$ være et ikke-nul polynomium i $k[x_1, \ldots, x_n]$, og lad $>$ være en monomiel ordning.*

(i) Multigraden for f er defineret ved

$$multideg(f) = max\left\{\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0\right\}.$$

(ii) Den ledende koefficient for f er defineret ved

$$LC(f) = a_{multideg(f)} \in k$$

(iii) Det ledende monomium for f er defineret ved

$$LM(f) = x^{multideg(f)}$$

(iv) Det førende led for f er defineret ved

$$LT(f) = LC(f) \cdot LM(f)$$

Forkortelserne stammer fra de engelske udtryk multidegree, leading coefficient, leading monomial og leading term.

Eksempel 4.6. *Tag et polynomum $f = 3x^2z + 2y^3 - 2xyz - 10z$, og lad ordningen være den leksikografiske ordning med $x > y > z$ fra definition 4.8, da er multigraden for f givet ved multideg$(f) = (2, 0, 1)$. Ligeledes ses at den ledende koefficent er udtrykt som $LC(f) = 3$. Det ledende monomium er $LM(f) = x^2$ og det førende led, $LT(f)$, er $3x^2z$.*

Vi får brug for et par nyttige regneregler vedrørende ovenstående begreber.

Lemma 4.5. *Lad $f \in k[x_1, \ldots, x_n]$, og m være et monomium. Da gælder, at*

$$LT(mf) = m \cdot LT(f).$$

Bevis. Lad $\alpha = \text{multideg}(f)$, og $m = x^\beta$. Der gælder, at

$$\begin{aligned} LT(fm) = LT(f \cdot x^\beta) &= LC(f \cdot x^\beta) \cdot LM(f \cdot x^\beta) \\ &= LC(f) \cdot x^{\alpha+\beta} \\ &= LC(f) \cdot x^\alpha \cdot x^\beta \\ = LT(f) \cdot m, & \end{aligned}$$

og sætningen er bevist. □

En anden nyttig egenskab er illustreret i nedenstående lemma.

Lemma 4.6. *Lad $f, g \in k[x_1, \ldots, x_n]$ være polynomier forskellige fra nulpolynomiet. Da gælder, at*

(i) multideg(fg) = multideg(f) + multideg(g)

(ii) Hvis $f + g \neq 0$, så multideg$(f + g) \leq max($multideg$(f),$ multideg$(g))$. Lighed gælder, når multideg$(f) \neq$ multideg(g).

Eksempel 4.7. *Tag $f = 2x^2 - x^2y$ og $g = y^2 + x^2y$. Den leksikografiske ordning fra 4.8 anvendes med $x > y$. Det ses, at $fg = 2x^2y^2 + 2x^4y - x^2y^3 - x^4y^2$. Jvf. def. 4.11 fås, at*

$$\begin{aligned} multideg(fg) &= (4, 2) \\ multideg(f) + multideg(g) &= (2, 1) + (2, 1) = (4, 2). \end{aligned}$$

Derfor overholder f og g betingelsen (i) i lemmaet. Idet $f+g = 2x^2 - x^2y + y^2 + x^2y = 2x^2 + y^2$, så

$$\begin{aligned} multideg(f+g) &= (2,0) \\ max(multideg(f), multideg(g)) &= (2,1), \end{aligned}$$

hvorved også (ii) i lemmaet er opfyldt.

Hvordan man opererer med polynomier i flere variable, særligt hvordan man laver polynomiers division, er en anden sag. Processen minder meget om i det en-dimensionelle tilfælde, hvor målet er at slippe af med det førende led. Det antages, at læseren er bekendt med divisionsalgoritmen for polynomier i $k[x]$. Algoritmen er nyttig, hvis man skal afgøre om et givet polynomium f tilhører et givet ideal. Polynomiet ligger i idealet, såfremt at det kan udtrykkes som en linearkombination af frembringerne for idealet. Algoritmen er som følger:

Sætning 4.4 (Divisionsalgoritmen for polynomier i flere variable)**.** *Lad $>$ være en monomiel ordning på $\mathbb{Z}^n_{\geq 0}$ og lad $F = (f_1, \ldots, f_s)$ være en ordnet tuppel af polynomier i $k[x_1, \ldots, x_n]$. Ethvert $f \in k[x_1, \ldots, x_n]$ kan da skrives som*

$$f = a_1 f_1 + \cdots + a_s f_s + r, \tag{4.3}$$

hvor $a_i, r \in k[x_1, \ldots, x_n]$ og hvor r enten er lig 0 eller også gælder der, at r er en linearkombination af monomier med koefficienter i k, som ej er dividerbare med $LT(f_1), \ldots, LT(f_s)$. Polynomiet r siges at være resten ved division af f med F. Faktisk så gælder, at hvis $a_i, f_i \neq 0$, da

$$multideg(f) \geq multideg(a_i f_i).$$

Beviset for algoritmen overlades til læseren, men kan findes kap. 2, §3 i [2008 Cox, Little & O´Shea]. Istedet gives en strategi for beviset og sætningen forklares med et eksempel. Strategien i beviset er først definere en divisionsalgoritme, som ved input af en polynomiumstuppel $F = (f_1, \ldots, f_s)$ og et polynomium $f \in k[x_1, \ldots, x_n]$, konstruerer koefficienterne og resten i udtrykket fra (4.3). Hvis det kan vises, at denne algoritme slutter efter et endeligt antal trin, og at outputtet opfylder sætningen, da er sætning 4.4 bevist. Divisionsalgoritmen udtrykt i pseudokode defineres ved

Input: Polynomiumstuppel $F = (f_1, \ldots, f_s)$ og polynomium $f \in k[x_1, \ldots, x_n]$
Output: Koefficienter $a_1, \ldots, a_s$ og rest r
Sæt $a_1 := 0, \ldots, a_s := 0$ og $p := f$
While $p \neq 0$ **Do**
    $i := 1$
    division:=false
    While $i \leq s$ **And** division=false **Do**
        If $LT(f_i) | LT(p)$ **Then**
            $a_i := a_i + LT(p)/LT(f_i)$
            $p := p - (LT(p)/LT(f_i))f_i$
            division:=true
        Else $i := i + 1$
    If division=false **Then**
        $r := r + LT(p)$
        $p := p - LT(p)$

I While-løkken tjekkes hvert monomium i f om det er deleligt med en af $LT(f_i)$. Polynomiet p anvendes til at holde styr, hvor meget af f, der stadig mangler at blive skrevet på formen $f = a_1f_1 + \cdots + a_sf_s + r$. Hvis ingen $LT(f_i)$ går op i $LT(p)$, så tilføjes monomiet $LT(p)$ til resten. Algoritmen slutter, idet at $p = 0$. Fremgangsmåden, for at bevise at algoritmen terminerer og giver det rigtige output, er følgende:

(i) Vis først, at $f = a_1f_1 + \cdots + a_sf_s + r + p$ holder i alle trin i algoritmen. Når $p = 0$ og algoritmen slutter, da må udtrykket i (4.3) være opfyldt. Ved algoritmens begyndelse, hvor $a_1 = 0, \ldots, a_s = 0$ og $f = p$ er betingelsen trivielt opfyldt, og det er også mulig at vise at udtrykket gælder i både divisionstrinnet og rest-trinnet.

(ii) Kraveene til resten er opfyldt i og med at der kun tilføjes led til resten, når $LT(f_i)$ ikke går op i leddet.

(iii) Det ses, at multideg(p) er aftagende i alle trin. Endvidere er den valgte ordning pr. definition velordnet, hvorfor $p = 0$ må indtræffe efter et endeligt antal trin i algoritmen.

(iv) Til sidst skal det også vises, at multideg(f) $\geq$ multideg(a_if_i).

Eksempel 4.8. *Lad $f = x^5y - 3xy^2 + 5$, og antag at f skal divideres med $F = (f_1, f_2)$, hvor $f_1 = x^2y - 1$ og $f_2 = y^2$, og hvor $>_{grevlex}$ med $x > y$ anvendes som ordning. Det ses, at $LT(f) = x^5y$, $LT(f_1) = x^2y$ og $LT(f_2) = y^2$. Det bemærkes, at $LT(f_1)$ går op i $LT(f)$ og giver x^3. Ved at multiplicere x^3 med f_1 og subtrahere dette produkt fra f, fås*

$$x^3 - 3xy^2 + 5.$$

Det ses, at med $>_{grevlex}$ er x^3 nu det førende led, men hverken $LT(f_1)$ og $LT(f_2)$ går op i x^3. Dette monomium fjernes derfor fra ligningen og gemmes som en rest. Det ses nu, at $LT(f_2)$ går op i $-3xy^2$ med resultatet $-3x$. Ved at multiplicere $-3x$ med f_2 og subtrahere dette produkt fra f, fås

$$-3xy^2 + 5 - (-3xy^2) = 5.$$

Det vil sige, at vi kan opskrive f som en linearkombination af f_1 og f_2 med en rest r:

$$f = x^5y - 3xy^2 + 5 = x^3(x^2y - 1) + (-3x)(y^2) + x^3 + 5,$$

hvor ingen $LT(F)$ går op i monomier i r. Det ses også, at multideg(f) = multideg(x^3f_1) $\geq$ multideg($-3x \cdot f_2$). Sætning 4.4 er altså sand lige netop i vores tilfælde.

4.3 Monomielle idealer

I det følgende afsnit introduceres monomielle idealer, som er idealer frembragt af monomier. Afsnittet når sit højdepunkt med Dickson's lemma, hvor det vises, at alle *monomielle* idealer over $k[x_1, \ldots, x_n]$ har et endeligt basis. Dette resultat er en vigtig ingrediens i beviset for Hilberts basis sætning4.7, hvor det vises, at faktisk alle idealer over $k[x_1, \ldots, x_n]$ har et endeligt basis . I dette afsnit vil Dickson's lemma også blive anvendt til at give et kriterium for, hvornår en ordning (se definition 4.7) på $k[x_1, \ldots, x_n]$ er monomiel. Afsnittet initieres med en definition af monomielle idealer på $k[x_1, \ldots, x_n]$.

Definition 4.12. *Et ideal $I \subset k[x_1, \ldots, x_n]$ siges at være et monomielt ideal, hvis der findes en delmængde $A \subset \mathbb{Z}^n_{\geq 0}$ (muligvis uendelig), sådan at I består af alle de polynomier, som er endelige summer på formen $\sum_{\alpha \in A} h_\alpha x^\alpha$, hvor $h_\alpha \in k[x_1, \ldots, x_n]$. Hermed skrives $I = \langle x^\alpha | \alpha \in A \rangle$.*

Dette betyder, at hvis et ideal I er monomielt, så er alle elementer i I polynomier, som kan skrives som en endelig linearkombination af monomier. Definitionen indikerer, at ikke alle idealer er monomielle. I det følgende eksempel demonstreres først, hvordan et ideal kan være monomielt og derefter vises et eksempel på et ideal, der ej er monomielt.

Eksempel 4.9. *Lad $I = \langle x + y, y \rangle \subseteq k[x, y]$ være et ideal. Spørgsmålet er, om I er monomielt. Det skal vises, at I kan skrives på formen $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(n)} \right\rangle$, hvor $x^{\alpha(1)}, \ldots, x^{\alpha(n)} \in A$. Bemærk, at*

$$(x + y) - y = x \in I,$$

da både $x+y \in I$ og $y \in I$. Det vil sige, at $I = \langle x + y, y \rangle = \langle x, y \rangle$, hvoraf det ses, at I er monomielt.

Betragt nu istedet idealet $I = \langle 1 + x \rangle \subseteq k[x, y]$. Kan det også skrives på samme form som ovenstående? Svaret på det findes ved at tage $f \in I$, så $f = h(1 + x)$. Her ligger $1 + x$ i idealet, men det gør 1 og x hver for sig ikke. Fordi $1 + x$ ikke kan skrives på formen $\sum_{\alpha \in A} h_\alpha x^\alpha$, så er I ikke et monomielt ideal jvf. definition 4.12.

Monomier i et monomielt ideal har en særlig egenskab illustreret i nedenstående lemma. Lemmaet vil vise sig at være meget anvendeligt i forbindelse med flere af beviserne i afsnit 4.4.

Lemma 4.7. *Lad $I = \langle x^\alpha | \alpha \in A \rangle$ være et monomielt ideal. Et monomium x^β ligger i I, hvis og kun hvis der findes $\alpha \in A$, så x^α går op i x^β.*

Bevis. Først vises implikationen fra højre mod venstre. Antag at x^β er et multiplum af x^α, for $\alpha \in A$, sådan at $x^\beta = x^\alpha \cdot x^\gamma$ for et $\gamma \in \mathbb{Z}^n_{\geq 0}$. Da $x^\alpha \in I$ og x^γ, fås ifølge definition 4.2 (iii), at $x^\beta \in I$.

Antag nu istedet, at $x^\beta \in I$. Ifølge definition 4.12 kan monomiet skrives som $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, hvor $h_i \in k[x_1, \ldots, x_n]$ og $\alpha(i) \in A$. Det ses, at alle led på højre side af lighedstegnet er dividérbart med et $x^{\alpha(i)}$, hvorfor det samme må gælde for venstresiden af lighedstegnet, x^β. □

Det bemærkes, at hvis x^α går op i x^β, så må der findes et $\gamma \in \mathbb{Z}^n_{\geq 0}$, så $x^\beta = x^\alpha \cdot x^\gamma$. Ved almindelig potensregneregler ses, at dette er det samme som at skrive, at $\beta = \alpha + \gamma$. Mængden,

$$\alpha + \mathbb{Z}_{\geq 0} = \{\alpha + \gamma | \gamma \in \mathbb{Z}_{\geq 0}\},$$

udtrykker derfor alle mulige eksponenter til monomier, som går op i x^α. Givet et polynomium f, da er det muligt at afgøre om f ligger i et monomielt ideal blot ved at betragte monomierne for f. Dette illustreres af følgende lemma.

Lemma 4.8. *Lad I være et monomielt ideal og lad $f \in k[x_1, \ldots, x_n]$. Følgende udsagn er ækvivalente:*

(i) $f \in I$

(ii) Alle led i f ligger i I

(iii) Polynomiet f er en k-linearkombination af monomier i I.

Bevis. Først vises implikationerne (iii)⇒(ii)⇒(i). Hvis f er en k-linearkombination af monomier i I, så følger det af definitionen for et ideal, 4.2(iii), at alle led i f ligger i I. Hvis alle led i f ligger i I, så ligger f også i I jvf. det andet punkt i definitionen for et ideal.

Næst vises implikationerne (i)⇒(ii)⇒(iii). Antag at $f \in I$. Ifølge definition 4.12 kan polynomiet skrives som $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, hvor $h_i \in k[x_1, \ldots, x_n]$ og $\alpha(i) \in A$. Det ses ved at skrive linearkombinationen ud, at hvert led i f er dividérbart med et $x^{\alpha}(i)$. Ifølge lemma 4.7 betyder det, at hvert led også ligger i I. I og med at alle led i f er monomier i I og at der findes k af dem, er f en k-linearkombination af monomierne i I. □

Det tredie punkt i lemmaet indikerer, at det er nok at beskæftige sig med monomierne i et polynomium for for at afgøre om polynomiet tilhører et monomielt ideal. Sagt på en anden måde er et monomielt ideal entydigt bestemt ud fra monomierne tilhørende idealet.

Korollar 4.1. *To monomielle idealer er ens, hvis og kun hvis de indeholder de samme monomier.*

Afsnittets springpunkt er at vise, at alle monomielle idealer i $k[x_1, \ldots, x_n]$ er endeligt genereret(se definition 4.4). Det ses, at det monomielle ideal defineret ved 4.12 i princippet godt kan være uendeligt genereret. Senere i rapporten vil vi også se, at faktisk er det ikke kun de monomielle idealer, men derimod alle idealer i $k[x_1, \ldots, x_n]$, som er endeligt genererede, hvorved det polynomielle ideal fra definition 4.12 også er endeligt.

Sætning 4.5 (Dickson's lemma)**.** *Lad $I = \langle x^{\alpha} | \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$ være et monomielt ideal. Da gælder, at $I = \left\langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \right\rangle$, hvor $\alpha(1), \ldots, \alpha(s) \in A$. Specielt har I et endeligt basis.*

Bevis. Beviset er et induktionsbevis, og der induceres over antallet af variable. Basistrinnet kommer ret nemt, men til induktionstrinnet skitseres en strategi. I induktionstrinnet antages, at sætningen er sand for $n-1$, hvor $n > 1$, og det vises, at sætningen så også gælder for antallet af variable lig med n. Dette gøres ved at tage et monomielt ideal I og finde frembringere til I. Frembringerne findes ved at opslitte I i dele af monomielle idealer, og vælge monomier tilhørende hver af disse delidealer som generatorer for I.

Antag at $n = 1$, hvorved $I = \langle x_1^{\alpha} | \alpha \in A \rangle$, hvor $A \subset \mathbb{Z}_{\geq 0}$. Det vil sige, at I er frembragt af monomierne x_1^{α}. Lad β være det mindste element i $A \subset \mathbb{Z}_{\geq 0}$. Da må der gælde, at $\beta \leq \alpha$ for alle $\alpha \in A$. Det betyder, at x_1^{β} går op i x_1^{α} for alle $\alpha \in A$. Ifølge lemma 4.7 ses, at $x_1^{\beta} \in I$ og dermed også frembringer I, så $I = \left\langle x_1^{\beta} | \alpha \in A \right\rangle$, hvilket er et endeligt basis for I.

Antag nu, at sætningen er sand for $n-1$, hvor $n > 1$, vi vil da vise, at sætningen også er sand, hvis antallet af variable er lig n. De n variable benævnes $x_1, \ldots, x_{n-1}, y$. Monomierne tilhørende $k[x_1, \ldots, x_{n-1}, y]$ kan udtrykkes ved $x^{\alpha} y^m$, hvor $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$, og $m \in \mathbb{Z}_{\geq 0}$. Antag nu som i sætningen, at $I \subset k[x_1, \ldots, x_{n-1}, y]$ er et monomielt ideal. Vi ønsker da at finde frembringere for I. Frembringere til I findes ved at indføre $J \in k[x_1, \ldots, x_{n-1}]$ som værende idealet frembragt af monomierne x^{α}, hvorom der gælder, at $x^{\alpha} y^m \in I$ for et helt tal $m \geq 0$. Det ses jvf. definition 4.12, at J er et monomielt ideal i $k[x_1, \ldots, x_{n-1}]$. Da J er et monomielt ideal haves ifølge induktionsantagelsen at der findes endeligt mange x^{α}'er som frembringer J. Dette skrives som $J = \left\langle x^{\alpha(1)}, x^{\alpha(2)}, \ldots, x^{\alpha(s)} \right\rangle$.

Har altså nu konstrueret et monomielt ideal J ud fra elementer i I, hvorom Dickson's lemma pr. antagelse er sand. Bemærk, at for hvert $i = 1, \ldots, s$ haves, at $x^{\alpha(i)}y^{m_i} \in I$, hvor $m_i \geq 0$. Lad m være det største af m_i'erne. Betragt for hvert k mellem 0 og $m-1$ idealet $J_k \subset k[x_1, \ldots, x_{n-1}]$, som er genereret af monomierne x^β, hvorom der gælder, at $x^\beta y^k \in I$. Igen kan induktionsantagelsen anvendes, hvorved J_k har et endeligt basis og er frembragt af $x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)}$. Det hævdes nu, at frembringerne for I faktisk er monomier fra $J, J_0, J_1, \ldots, J_{m-1}$:

$$\begin{aligned} J &: x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m \\ J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)} \\ J_1 &: x^{\alpha_0(1)}y, \ldots, x^{\alpha_0(s_0)}y \\ &\vdots \\ J_{m-1} &: x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1} \end{aligned}$$

Hvis det kan vises, at alle monomier i I er et multiplum af ovenstående monomier, så haves ifølge lemma 4.7, at ovenstående monomier genererer et ideal indeholdende samme monomier som I. Ved at anvende korollar 4.1 ses, at I og idealet, frembragt af monomier fra $J, J_0, J_1, \ldots, J_{m-1}$, er ens. At alle monomier i I er et multiplum af monomier fra $J, J_0, J_1, \ldots, J_{m-1}$ ses ved at betragte $x^\alpha y^p \in I$. Hvis $p \geq m$, så findes et $x^{\alpha(i)}y^m$, som går op i $x^\alpha y^p$ pga. den måde, hvorpå J_p er konstrueret. Husk, at J_p er idealet genereret ud fra monomierne x^β, hvorom der gælder, at $x^\beta y^p \in I$. Hvis $p < m$ ses, at der findes et $x^{\alpha_p(j)}y^p$, som går op i $x^\alpha y^p \in I$.

Det eneste der mangler er at vise der findes et endeligt basis for I. Hvis variablerne igen noteres som $x_1, \ldots, x_n$, så er det monomielle ideal $I = \langle x^\alpha | \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$. Vi ved fra ovenstående diskussion at $I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ for monomier $x^{\beta(i)} \in I$. Lemma 4.7 giver, at hvert monomium $x^{\beta(i)}$ er dividérbart med $x^{\alpha(i)}$, for et $\alpha(i) \in A$. Heraf følger, at $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. □

Som indikeret i begyndelsen af dette afsnit har Dickson's lemma en særlig anvendelighed i forhold til monomielle ordninger på $k[x_1, \ldots, x_n]$. Lemmaet gør at det ikke er nogen sag at bevise følgende korollar.

Korollar 4.2. *Lad $>$ være en relation på $\mathbb{Z}^n_{\geq 0}$, som opfylder følgende to betingelser:*

(i) Relationen $>$ er en lineær ordning (se ligning 4.2).

(ii) Hvis $\alpha > \beta$ og $\gamma \in \mathbb{Z}^n_{\geq 0}$, så $\alpha + \gamma > \beta + \gamma$.

Da gælder, at relationen $>$ er velordnet hvis og kun hvis $\alpha \geq 0$ for alle $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Som der blev indikeret i indledningen til dette afsnit, giver Dickson's lemma en metode til at koble monomiel ordning

Bevis. Antag først, at $>$ er velordnet. Lad α_0 være det mindste element i $\mathbb{Z}^n_{\geq 0}$. At et sådant findes sikres af definition 4.7(iii), som siger at alle ikke-tomme delmængder af $\mathbb{Z}^n_{\geq 0}$ har et mindste element, når de er underlagt $>$. Det mindste af mindste elementer er α_0. Det skal vises, at $\alpha_0 \geq 0$, hvilket gøres per modstrid. Antag modsætningsvist at $\alpha_0 < 0$. Ifølge (ii) i korollaret så hvis $\alpha = 0$, $\beta = \alpha_0$ og $\gamma = \alpha_0$ opnås, at $\alpha_0 > 2\alpha_0$. Dette er i modstrid med, at α_0 var mindste element.

Antag nu istedet, at $\alpha \geq 0$ for alle $\alpha \in \mathbb{Z}^n_{\geq 0}$. Lad $A \subseteq \mathbb{Z}^n_{\geq 0}$ være en ikke-tom delmængde, da skal det vises, at A har et mindste element. Til at bevise dette anvendes Dickson's lemma, sætning 4.5. Betragtes det monomielle ideal $I = \langle x^\alpha | \alpha \in A \rangle$, findes der ifølge lemmaet $\alpha(1), \ldots, \alpha(s) \in A$, sådan at $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Antag uden tab af generalitet, at $\alpha(1) < \alpha(2) < \cdots < \alpha(s)$. Det kan vi gøre uden problemer, for hvis ikke rækkefølgen af potenserne passer, omarrangeres de og navngives efter α'erne. Tag nu $\alpha \in A$, så $x^\alpha \in I$. Ifølge Dickson må $x^\alpha \in \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Det betyder ifølge lemma 4.7, at et $x^{\alpha(i)}$, $i = 1, \ldots, s$, går op i x^α. Det betyder, at $\alpha = \alpha(i) + \gamma$ for et $\gamma \in \mathbb{Z}^n_{\geq 0}$. Hermed fås, da $\gamma \geq 0$, at

$$\begin{aligned} \alpha = \alpha(i) + \gamma &\geq \alpha(i) + 0 \\ &\geq \alpha(1) \end{aligned}$$

Den sidste ulighed følger af den måde vi arrangerede $\alpha(i)$'erne på. Hermed ses også, at $\alpha(1)$ er mindste element. □

Forståelsen af monomielle idealer og i særlig grad Dickson's Lemma gør, at det kan vises, at alle polynomielle idealer har et endeligt basis. I det følgende afsnit udtrykkes det hovedresultat i Hilbert's Basissætning og i den forbindelse stiftes der for første gang i denne specialeafhandling bekendtskab med Gröbnerbaser.

4.4 Hilberts Basissætning og Gröbnerbaser

Målet med dette afsnit er at verificere, at alle idealer i $k[x_1, \ldots, x_n]$ har et endeligt basis. Dickson's lemma gav, at alle monomielle idealer havde et endeligt basis, og at dette basis var bestemt ud fra monomier i $k[x_1, \ldots, x_n]$. Dette resultat vil her blive udvidet, sådan at der for alle idealer $I \subseteq k[x_1, \ldots, x_n]$, gælder, at de har et endeligt basis. Altså løses ideal description problemet. Denne type basis er så specielle, at de har fået deres eget navn, nemlig Gröbner-baser efter den østrigskfødte matematiker Wolfgang Gröbner. Teorien, som ledte frem til opdagelsen af Gröbnerbaser blev udviklet af endnu en østriger, Bruno Buchberger. Buchberger var også manden, der navngav de særlige baser, og når han gav dem navnet Gröbner, så skyldes det, at Wolfgang Gröbner var Buchbergers vejleder.

Vi får brug for at definere en bestemt type af monomielle idealer, som består af førende led fra et ideal. Husk, at givet et polynomium $f \in k[x_1, \ldots, x_n]$ og en monomiel ordning $>$, da har f jvf. definition 4.11 et førende led, som er entydigt bestemt. Dette vil blive benyttet i definitionen af, hvad det vil sige, at ideal har førende led.

Definition 4.13. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal forskelligt fra $\{0\}$.*

(i) Mængden

$$LT(I) = \{cx^\alpha | \textit{der findes et } f \in I \textit{ med } LT(f) = cx^\alpha\}, \tag{4.4}$$

siges at være de førende led til alle elementer i I.

(ii) Idealet frembragt af elementer fra I, noteres som $\langle LT(I) \rangle$, og det siges at være idealet af førende led.

Bemærk, at givet $I = \langle f_1, \ldots, f_s \rangle$, da er idealerne $\langle LT(I) \rangle$ og $\langle LT(f_1, \ldots, f_s) \rangle$ ikke nødvendigvis ens, hvilket ses af det næste eksempel.

Eksempel 4.10. *Tag $I = \langle f_1, f_2, f_3 \rangle$, hvor $f_1 = x^2 + xz^2$, $f_2 = y^2z - z$ og $f_3 = x^2z + y^3 - y$. Som monomiel ordning anvendes $>_{grevlex}$ fra definition 4.10, hvorved idealet af førende led er udtrykt ved $\langle xz^2, y^2z, y^3 \rangle$. Det bemærkes, at*

$$xf_1 + yf_2 - zf_3 = x^3,$$

hvoraf det ses, at $x^3 \in I$. Endvidere gælder, at $LT(x^3) = x^3$. Som i ligning (4.4) findes derved et polynomium i I med et førende led. Det betyder, at $x^3 \in \langle LT(I) \rangle$. Det ses, at med den valgte monomielle ordning er $LT(f_1) = xz^2$, $LT(f_2) = y^2z$ og $LT(f_3) = y^3$. Det ses også, at ingen af disse går op i x^3. Ifølge lemma 4.7 betyder det, at x^3 ikke ligger i $\langle LT(f_1), LT(f_2), LT(f_3) \rangle$. Ergo er

$$\langle LT(I) \rangle \neq \langle LT(f_1), LT(f_2), LT(f_3) \rangle .$$

Selvom de to idealer ikke altid er lig med hinanden, så vises, der i den følgende sætning, at der for ethvert ideal I altid findes et endeligt antal monomier i I, så deres førende led tilsammen danner $\langle LT(I) \rangle$. Et interessant faktum om $\langle LT(I) \rangle$ er også, at det rent faktisk er et monomielt ideal. Dette gør, at alle redskaber knyttet til monomielle idealer fra afsnit 4.3 virker på $\langle LT(I) \rangle$. Samtidig er det også en vigtig ingrediens i beviset for Hilberts basis sætning, som siger, at alle idealer i $k[x_1, \ldots, x_n]$ har et endelig basis.

Sætning 4.6. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal forskelligt fra $\{0\}$. Da gælder, at*

1. *$\langle LT(I) \rangle$ er et monomielt ideal, og*
2. *der findes $g_1, \ldots, g_t \in I$, sådan at*

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle .$$

Bevis. Først vises (i). Bemærk, at for alle $g \in I \backslash \{0\}$ vil de ledende monomier være udtrykt på formen $x^{\text{multideg}(g)}$, hvor multideg$(g) \in A \subseteq \mathbb{Z}^n_{\geq 0}$. Derfor gælder ifølge definition 4.12, at idealet $\langle LM(g) | g \in I \backslash \{0\} \rangle$ er monomielt. Det er da nok at vise, at

$$\langle LM(g) | g \in I \backslash \{0\} \rangle = \langle LT(I) \rangle . \tag{4.5}$$

Tag $g \in I \backslash \{0\}$, og lad $LT(g) = c_i x^{\alpha(i)} \in \langle LT(I) \rangle$. Det ses klart, at $x^{\alpha(i)}$ går op i $LT(g)$. Da $x^{\alpha}(i) \in \langle LM(g) | g \in I \backslash \{0\} \rangle$, som er et monomielt ideal, ligger $c_i x^{\alpha(i)}$ også i $\langle LM(g) | g \in I \backslash \{0\} \rangle$ ifølge lemma 4.7. Dvs., at

$$\langle LM(g) | g \in I \backslash \{0\} \rangle \supseteq \langle LT(I) \rangle . \tag{4.6}$$

eq:idealvsmonidealto Lad x^{α} være ledende monomium for $g \in I \backslash \{0\}$. Da gælder, at cx^{α} for alle c. Hermed ses, at $cx^{\alpha} \in \langle LT(I) \rangle$ for alle c. Dvs., at

$$\langle LM(g) | g \in I \backslash \{0\} \rangle \subseteq \langle LT(I) \rangle . \tag{4.7}$$

Ligningerne (4.6) og (4.7) giver til sammen, at ligning (4.5) er sand.

Til at bevise (ii) anvendes Dickson's lemma, sætning 4.5. Fra (i) haves, at $\langle LT(I) \rangle$ kan frembringes ud fra de ledende monomier $LM(g)$, hvor $g \in I \backslash \{0\}$. Dickson's lemma giver, at $\langle LT(I) \rangle$ har et endeligt basis $\langle LM(g_1, \ldots, LM(g_t)) \rangle$, hvor $g_1, \ldots, g_t \in I$. Igen da den eneste forskel på det ledende monomium og det førende led er en konstant forskelig fra nul, så

$$\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle .$$

□

Den næste er sætning er om muligt den vigtigste i dette afsnit. Endelig er det muligt at bevise, at alle idealer i $k[x_1, \ldots, x_n]$ kan frembringes af endeligt mange af elementer i idealet. Sætningen er opkaldt efter den tyske matematiker David Hilbert, som døde i 1943. Han beviste, at sætningen gælder for polynomielle ringe over et legeme, og han gjorde det uden at bruge Gröbnerbaser.

Sætning 4.7 (Hilberts basis sætning)**.** *Alle idealer $I \subseteq k[x_1, \ldots, x_n]$ har et endeligt basis, ie. $I = \langle g_1, \ldots, g_t \rangle$, for $g_1, \ldots, g_t \in I$.*

Bevis. Hvis $I = \{0\}$, sættes den frembringende mængde blot lig $\{0\}$. Mængden $\{0\}$ er tydeligvis endelig og frembringer hele I. Hvis til gengæld I er et ideal over $k[x_1, \ldots, x_n]$, som er forskelligt fra nul, er det en anden sag. Antag, at $I \subseteq k[x_1, \ldots, x_n]$ er et ideal forskelligt fra $\{0\}$. Det vides fra sætning 4.6, at der findes $g_1, \ldots, g_t \in I$, så $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Hvis det kan vises om g_i'erne, at

$$I \subseteq \langle g_1, \ldots, g_t \rangle \text{ og } I \supseteq \langle g_1, \ldots, g_t \rangle, \tag{4.8}$$

er sætningen bevist. Den anden inklusion er trivielt opfyldt for bemærk, at $g_i \in I$, hvilket betyder, at idealet frembragt af g_i'erne er indeholdt i I.

Tag polynomium $g \in I$ og antag, at en monomiel ordning er valgt. Jævnfør divisionsalgoritmen, sætning 4.4, kan g skrives som

$$g = a_1 g_1 + \cdots + a_t g_t + r, \tag{4.9}$$

hvor r enten er lig 0, eller også gælder der, at r er en linearkombination af monomier med koefficienter i k, som ej er dividerbare med $LT(f_1), \ldots, LT(f_s)$. Antag modsætningsvist at $r \neq 0$ og omrokér ligning (4.9)

$$r = g - a_1 g_1 - \cdots - a_t g_t,$$

så $LT(r) \in \langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$. Ifølge lemma 4.7 fås, at et $LT(g_i)$ går op i $LT(r)$, men dette er i modstrid med hvordan r er defineret. Derfor $r = 0$ og

$$g = a_1 g_1 + \cdots + a_t g_t.$$

Det ses hermed, at g ligger i $\langle g_1, \ldots, g_t \rangle$, hvorfor I også er indeholdt i idealet frembragt af g_i'erne. Begge mængderelationer fra (4.8) er opfyldt, og dermed gælder, at

$$I = \langle g_1, \ldots, g_t \rangle .$$

□

I beviset konstrueredes frembringende mængder med én særlig egenskab. Denne særlige type af baser for et ideal er, hvad der vil blive refereret til som Gröbnerbaser.

Definition 4.14. *En endelig delmængde $G = \{g_1, \ldots, g_t\}$ af et ideal I siges at være et Gröbnerbasis såfremt, at*

$$\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle . \tag{4.10}$$

Med andre ord er en mængde $G = \{g_1, \ldots, g_t\}$ af et ideal I et Gröbner basis hvis og kun hvis alle førende led LT til elementer i I er dividérbare med $LT(g_i)$. Dette følger af lemma 4.7. Endvidere kan der ud fra ovenstående definition sætning 4.7 opstilles følgende korollar.

Korollar 4.3. *Antag, at en monomiel ordning er valgt. Alle idealer $I \subseteq k[x_1, \ldots, x_n]$, som er forskellige fra nulmængden, har et Gröbnerbasis. Endvidere er ethvert Gröbnerbasis for I, også et endeligt basis for I.*

Bevis. Sætning 4.7 giver, at til alle idealer kan der konstrueres et endeligt basis. Hvis Idealet er forskelligt fra nulmængden, så gives i beviset for sætning 4.7 særligt et basis, $G = \{g_1, \ldots, g_t\}$, som opfylder formel (4.10). Dvs., at G er et Gröbnerbasis. Endvidere når (**??**) er opfyldt, er det vist i beviset for sætning 4.7, at $I = \langle g_1, \ldots, g_t \rangle$. Heraf ses, at G også er basis for I, fordi elementerne i G frembringer I. □

Sætning 4.7 giver anledning til et par sætninger, som vedrører idealers egenskaber. Den første sætning har med indlejrede idealer at gøre.

Definition 4.15. *En stigende kæde af idealer er en indlejret følge af idealer $I_1, I_2, \ldots$ over $k[x_1, \ldots, x_n]$, udtrykt som*

$$I_1 \subseteq I_2 \subseteq \cdots .$$

Eksempel 4.11. *Et eksempel på en stigende kæde af idealer er*

$$\langle x \rangle \subseteq \langle x, y \rangle \subseteq \langle x, y, z \rangle \subseteq k[x, y, z].$$

Kæden kan udvides på to måder. Enten med et ideal $\langle x, y, z, f \rangle$, hvor $f \in \langle x, y, z \rangle$. I dette tilfælde vil $\langle x, y, z, f \rangle$ blot være lig $\langle x, y, z \rangle$. Den anden måde, hvorpå vi kan udvide kæden er ved at tilføje idealet $\langle x, y, z, f \rangle$, hvor $f \notin \langle x, y, z \rangle$. Det kan vises, at der dermed gælder $\langle x, y, z, f \rangle = k[x, y, z]$.

Eksemplet viser, at uanset hvordan den stigende kæde udvides, da findes et stabilt ideal. Dette er også hovedessensen i den følgende sætning.

Sætning 4.8. *Lad*

$$I_1 \subseteq I_2 \subseteq \cdots$$

være en stigende kæde af idealer over $k[x_1, \ldots, x_n]$. Da findes $N \geq 1$, sådan at $I_N = I_{N+1} = \cdots$.

Bevis. Antag at en stigende kæde $I_1 \subseteq I_2 \subseteq \cdots$ er givet, og lad $I = \bigcup_{i=1}^{\infty}$. Det skal vises, at I er et ideal i $k[x_1, \ldots, x_n]$. De tre betingelser i definition 4.2 skal altså være opfyldt. For det først så tilhører 0 alle I_i, da de er idealer. Det er derfor trivielt opfyldt, at også $0 \in I$. Tag nu $f, g \in I$, så må $f \in I_i$ og $g \in I_j$. Antag uden tab af generalitet, at $i \leq j$. Pr. definition af en stigende kæde så må både f og g ligge i I_j. I og med at I_j jo er et ideal, så ligger $f + g$ også i I_j. Det vil sige, at $f + g$ også ligger i I. Hvis $r \in k[x_1, \ldots, x_n]$ så $rf \in I_i$, da I_i er et ideal. Derfor ses også, at $rf \in I$. De tre betingelser er opfyldt, og I er et ideal.

Sætning 4.7 kan anvendes og der gælder, at I har et endeligt basis, således at $I = \langle f_1, \ldots, f_s \rangle$. Hver af generatorpolynomierne må ligge i et I_i. Hvis N være det største i, så $f_i \in I_N$ for alle i. Hvis hvert af generatorpolynomierne tilhører I_N, så gør også idealet frembragt af generatorpolynomierne (exercise 2 tilhørende idealerafsnittet). Hermed ses, at

$$I = \langle f_1, \ldots, f_s \rangle \subseteq I_N \subseteq I_{N+1} \subseteq \cdots \subseteq I,$$

hvorfor der må gælde, at $I_N = I_{N+1} = \cdots$. □

Den anden sætning som Hilberts basis sætning skaber grobund for omhandler affine varieteter, eller nærmere bestemt affine varieteter til idealer. Hilberts Basissætning har nemlig den konsekvens, at ethvert ideal kan være definerende mængde for en affin varietet.

Definition 4.16. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal. Den affine varietet til I, $\boldsymbol{V}(I)$, er udtrykt ved*

$$\boldsymbol{V}(I) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for alle } f \in I\}.$$

En affin varietet til et ideal I består af alle de n-tupler, hvor alle elementer i I forsvinder. Det huskes fra afsnit 4.1, definition 4.5, at det ikke er det samme, som idealet frembragt af en affin varietet.

Sætning 4.9. *$\boldsymbol{V}(I)$ fra ovenstående definition er en affin varietet. Specielt hvis $I = \langle f_1, \ldots, f_s \rangle$, så $\boldsymbol{V}(I) = V(f_1, \ldots, f_s)$.*

Bevis. At $\mathbf{V}(I)$ følger direkte af definition 4.1. Istedet for givne polynomier betragtes blot her en mængde med elementer på polynomiumsform. Til at bevise anden del af sætningen anvendes Hilberts basis sætning, sætning 4.7. Ifølge den findes nemlig et endelig basis til idealet I, så $I = \langle f_1, \ldots, f_s \rangle$. Det skal vises, at

$$\mathbf{V}(I) \subseteq \mathbf{V}(f_1, \ldots, f_s) \text{ og } \mathbf{V}(I) \supseteq \mathbf{V}(f_1, \ldots, f_s). \tag{4.11}$$

For det første da $f_i \in I$, hvis $f(a_1, \ldots, a_n) = 0$ for alle $f \in I$, så gælder også, at $f_i(a_1, \ldots, a_n) = 0$. Heraf ses, at den første mængderelation i (4.11) er sand.

For det andet tages $(a_1, \ldots, a_n) \in \mathbf{V}(i)$ og $f \in I$, fås, at

$$f = \sum_{i=1}^{s} h_i f_i,$$

for et $h_i \in k[x_1, \ldots, x_n]$, idet $I = \langle f_1, \ldots, f_s \rangle$. Der må derfor gælde, at

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_1(a_1, \ldots, a_n) f_i(a_1, \ldots, a_n)$$

$$\sum_{i=1}^{s} h_1(a_1, \ldots, a_n) \cdot 0 = 0.$$

Ergo må også den anden mængderelation i formel (4.11) være sand. □

Det vigtigste i afsnittet er konstruktionen af Gröbnerbasis. Disse betragtes som baser for idealer, der har særligt anvendelige egenskaber. For at skabe forståelse for, hvorfor dette begreb har en særlig betydning indenfor især algebraen, vil det næste afsnit omhandle et Gröbnerbasis's egenskaber.

4.5 Gröbnerbasis og dets egenskaber

I jagten på at vise, at alle idealer over $k[x_1, \ldots, x_n]$ har et endeligt basis, opstod i forrige afsnit det såkaldte Gröbnerbasis. Det blev vist, at alle polynomielle idealer har et Gröbnerbasis. I dette afsnit

undersøges Gröbnerbasen nærmere og særligt vil afsnittet give en metode til at afgøre, hvornår et basis er et Gröbnerbasis (Buchbergers kriterium). Den første sætning i dette afsnit relaterer til divisionsalgoritmen sætning 4.4. Det huskes, at resultatet i divisionsalgoritmen afhænger af den valgte ordning og rækkefølgen af de polynomier, der divideres med. Divisionsalgoritmen er særligt anvendelig, når man ønsker at vide om et givet polynomium ligger i et bestemt ideal$I$. Polynomiet tilhører I såfremt det kan skrives som en linearkombination af frembringerne for I. Derfor giver divisionsalgoritmen ej et entydigt resultat men med konstruktionen af Gröbnerbaser kan dette problem omgås. Forskellen ligger blot i, at i denne reviderede divisionsalgoritme divideres et polynomium med en særlig tuppel af polynomier, nemlig et Gröbnerbasis.

Sætning 4.10. *Lad $G = \{g_1, \ldots, g_t\}$ være et Gröbnerbasis for idealet $I \subseteq k[x_1, \ldots, x_n]$. For $f \in k[x_1, \ldots, x_n]$ findes $r \in k[x_1, \ldots, x_n]$, som opfylder, at*

(i) Leddene $LT(g_1), \ldots, LT(g_t)$ går ikle op i nogen af leddene i r.

(ii) Der findes et $g \in I$, sådan at $f = g + r$.

Endvidere gælder, at r er entydigt bestemt.

Bevis. Punkterne (i) og (ii) følger direkte af divisionsalgoritmen sætning 4.4. Ifølge divisionsalgoritmen fås $f = a_1g_1 + \cdots + a_tg_t + r$, hvor $a_i, r \in k[x_1, \ldots, x_n]$ og hvor r enten er lig 0 eller også gælder der, at r er en linearkombination af monomier med koefficienter i k, som ej er dividerbare med $LT(g_1), \ldots, LT(g_t)$. Hvis man sætter $g = a_1g_1 + \cdots + a_tg_t$, så er også (ii) opfyldt.

Tag $f = f'$, hvor $f = g + r$, $f' = g' + r'$ og $f, f' \in k[x_1, \ldots, x_n]$. Antag modsætningsvist, at $r \neq r'$. Der gælder, at $r - r' = g - g' \in I$, da I er et ideal, og både g og g' ligger i I. Da $r - r'$ dermed også tilhører I, haves at $LT(r - r') \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$ ifølge definition 4.10. Det huskes fra sætning 4.6, at $\langle LT(I)\rangle$ er et monomielt ideal, hvilket jævnfør lemma 4.7 betyder, at der findes et $LT(g_i)$, som går op i $LT(r - r')$. Dette er dog i modstrid med at intet $LT(g_i)$ går op i hverken r eller r', så antagelsen om at $r \neq r'$ må være usand. Hermed er entydigheden også bevist. □

Selvom leddene i et polynomium arrangeres anderledes ændrer det ikke på resten ved division med et Gröbnerbasis. Til gengæld er koefficienterne a_i ikke entydigt bestemte, og de vil blive påvirket af en eventuel rearrangering af leddene i polynomiet. Følgende eksempel illustrerer problematikken.

Eksempel 4.12. *Tag $f = xy$ og $G = \{x + z, y - z\}$. Det skal først tjekkes, at G er et Gröbnerbasis til idealet $I = \langle x + z, y - z\rangle$ med den leksikografiske ordning def. 4.8, hvor $x > y > z$. Til dette anvendes programmet Singular.*

```
> ring R=3,(x,y,z),lp;
> ideal I=x+z,y-z;
> std(I);
_[1]=y-z
_[2]=x+z
```

Det ses, at G er Gröbnerbasis for I. Ved division af f med G fås, at

$$f = y(x + z) - z(y - z) - z^2,$$

hvoraf det ses, at $a_1 = y$ og $a_2 = -z$. Hvis der byttes om på rækkefølgen af polynomierne i G ændres koefficienterne. I denne situation fås

$$f = x(y - z) + z(x + z) - z^2.$$

Det ses, at her er $a_1 = x$ og $a_2 = z$.

Sætning 4.10 giver grundlaget for et meget nyttigt korollar. Et korollar som senere vil blive anvendt i forbindelse med at konstruere en algoritme, der kan afgøre ud fra et givet Gröbnerbasis G og et polynomium $f \in k[x_1, \ldots, x_n]$, om f ligger i det tilhørende ideal.

Korollar 4.4. *Lad $G = \{g_1, \ldots, g_t\}$ være et Gröbnerbasis for idealet $I \subseteq k[x_1, \ldots, x_n]$ og tag $f \in k[x_1, \ldots, x_n]$. Da gælder, at $f \in I$ hvis og kun hvis resten ved division af f med G er lig nul.*

Bevis. Hvis resten er lig nul haves ifølge sætning 4.10, at $f = a_1 g_1 + \cdots + a_t g_t$. I og med at $g_1, \ldots, g_t \in I$, så også $f \in I$.

Antag istedet at $f \in I$. Da ses, at $f = f + 0$ opfylder begge betingelser i sætning 4.10, hvorfor resten må være lig nul. □

Det bemærkes, at implikationen fra højre mod venstre i ovenstående korollar altid er sand, også selvom G ikke er et Gröbnerbasis. Dvs. hvis resten er lig nul, så ligger f i I. Korollaret indikerer også, at hvis resten ej er lig nul, og G er et Gröbnerbasis, så ligger f ikke i I. Hvad korollaret ikke siger noget om, er hvad der sker, når resten er forskellig fra nul, men G ikke er et Gröbnerbasis. I det følgende gives et eksempel på et basis der ej er Gröbner.

Eksempel 4.13. *Lad $B = \{x^2 + y, x^2y + 1\}$, og tag $f = y^2 - 1 \in k[x, y]$. Som monomiel ordning er valgt den leksikografiske ordning med $x > y$. Det ses, at G er basis for idealet $I = \langle x^2 + y, x^2y + 1 \rangle$ og at $f \in I$, da*

$$y^2 - 1 = y(x^2 + y) - (x^2y + 1).$$

Jvf. korollar 4.4 må det betyde, at f ved division med et Gröbnerbasis for I må give nul. Igen benyttes Singular til at finde et Gröbnerbasis til I.

```
> ring R=3,(x,y,z),lp;
> ideal J=x2+y,x2y+1;
> std(J);
_[1]=y2-1
_[2]=x2+y
```

Det ses, at $G = \{y^2 - 1, x^2 + y\}$ er Gröbnerbasis for I. Ved division af f med G fås, at

```
> reduce(y2-1,std(J));
0
```

og det ses, at korollaret er opfyldt.

Der indføres nu følgende notation:

Definition 4.17. *Resten ved division af et polynomium $f \in k[x_1, \ldots, x_n]$ med $F = \{f_1, \ldots, f_s\}$ skrives som $\overline{f}^F$.*

Bemærk, at hvis F er et Groebner basis, så er rækkefølgen af polynomierne ifølge sætning 4.10 ubetydende ift. resten $\overline{f}^F$. Betragt eksempel 4.12. Det ses, at $\overline{f}^G = -z^2$.

Næste punkt på dagsordenen er at konstruere en algoritme, som kan afgøre, om et givet basis til et ideal er et Gröbnerbasis. Husk, at $G = \{g_1, \ldots, g_t\}$ af et ideal I et Gröbnerbasis hvis og kun hvis alle førende led LT til elementer i I er dividérbare med $LT(g_i)$ (se definition 4.14). Det vil sige, at hvis en mængde $G = \{g_1, \ldots, g_t\}$ er et Gröbnerbasis for idealet I, da gælder, at $LT(f_i) \in \langle LT(g_i)\rangle$, for $f_i \in I$. Derfor hvis det førende led i et polynomium $f_i \in I$ ikke også ligger i idealet frembragt af $LT(g_i)$, så er G ej et Gröbnerbasis. I eksempel 4.10 havde man faktisk en situation, hvor den frembringende mængde ikke var et Gröbnerbasis. Det, der gik galt i eksemplet, var, der på den ene side fandtes førende led

$$ax^\alpha f_i - bx^\beta f_j,$$

som eliminerede hinanden, og efterlod led af mindre potenser, så

$$ax^\alpha f_i - bx^\beta f_j = h_{i,j} \notin \langle LT(f_i), LT(f_j)\rangle\,.$$

På den anden side blev det vist, at $h_{i,j} \in I$ og dermed også $h_{i,j} \in \langle LT(I)\rangle$. Til at afgøre om et givet basis for et ideal er et Gröbner, behøves det såkaldte S-polynomium.

Definition 4.18. *Lad $f, g \in k[x_1, \ldots, x_n]$ være polynomier forskellige fra nulpolynomiet.*

(i) Hvis multideg$(f) = \alpha$ og multideg$(g) = \beta$, sæt $\gamma = (\gamma_1, \ldots, \gamma_n)$, hvor $\gamma_i = max\{\alpha_i, \beta_i\}$ for hvert i. Det mindste fælles multiplum er da defineret ved x^γ, og det skrives

$$LCM(LM(f), LM(g)).$$

(ii) S-polynomiet til f og g er defineret ved

$$S(f,g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$$

Eksempel 4.14. *Lad $f = 2x^4y^3 - x^2z^5 + y^2$ og $g = x^3z - y^2z + z^3$ i $\mathbb{R}[x, y, z]$, og benyt den graduerede reverse leksikografiske ordning, sætning 4.10. For f og g ses, at*

$$f : (4,3,0) >_{grevlex} (2,0,5) >_{grevlex} (0,2,0),$$
$$g : (3,0,1) >_{grevlex} (0,2,1) >_{grevlex} (0,0,3).$$

Endvidere haves at multideg$(f) = (4,3,0)$ og multideg$(g) = (3,0,1)$. Hermed sættes $\gamma = (4,3,1)$, hvorved x^4y^3z er det mindste fælles multiplum for f og g. Hermed er S-polynomiet for f og g udtrykt ved

$$\begin{aligned} S(f,g) &= \frac{x^4y^3z}{2x^4y^3} \cdot f - \frac{x^4y^3z}{x^3z} \cdot g \\ &= \frac{1}{2}z \cdot f - xy^3 \cdot g \\ &= -\frac{1}{2}x^3z^6 + \frac{1}{2}y^2z - xy^5z + xy^3z^3. \end{aligned}$$

Det ses, at det førende led for f er elimineret.

Som det ses af eksemplet er S-polynomiet særligt anvendeligt til eliminering af førende led i et polynomium. Det kan vises, at alle procedurer til eliminering af førende led i polynomier med samme multigrad sker ved hjælp af S-polynomiet. Se det følgende lemma, som iøvrigt også vil blive anvendt til at vise Buchbergers kriterium.

Lemma 4.9. *Lad $\sum_{i=1}^{s} c_i f_i$ være givet, hvor $c_i \in k$ og multideg$(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ for alle i. Hvis multideg$(\sum_{i=1}^{s} c_i f_i) < \delta$, da gælder, at $\sum_{i=1}^{s} c_i f_i$ er en linearkombination af S-polynomier, $S(f_j, f_l)$, med koefficienter, der tager værdier i k, og hvor $1 \leq j, l \leq s$. endvidere gælder, at hvert $S(f_j, f_k)$ har multigrad mindre end δ.*

Bevis. Lad d_i være den ledende koefficient til $f_i \in k[x_1, \ldots, x_n]$, sådan at $LC(c_i f_i) = c_i d_i$. Pr. antagelse haves at multideg$(f_i) = \delta$, og da $c_i \in k$, så også multideg$(c_i f_i) = \delta$ for alle i. Hvis samtidigt at multideg $(\sum_{i=1}^{s} c_i f_i) < \delta$ skal være sandt, må hvert led i summen forsvinde, sådan at

$$\sum_{i=1}^{s} c_i f_i = 0. \tag{4.12}$$

Sæt $p_i = \frac{f_i}{d_i}$, så må den førende koefficient for p_i, $LC(p_i)$, være lig 1. Ved hjælp af p_i omskrives $\sum_{i=1}^{s} c_i f_i$, så

$$\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i p_i d_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \tag{4.13}$$

$$(c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s. \tag{4.14}$$

Da d_i er førende koefficient for f_i for alle i, og multigraden til alle led i $\sum_{i=1}^{s} c_i f_i$ er δ opnås, at $LT(f_i) = d_i x^\delta$. Det vil sige, at $LM(f_j) = LM(f_k) = x^\delta$, hvilket medfører, at

$$LCM(LM(f_j), LM(f_k)) = x^\delta.$$

S-polynomiet kan opskrives som

$$S(f_j, f_k) = \frac{x^\delta}{d_j x^\delta} \cdot f_j - \frac{x^d elta}{d_k x^\delta} \cdot f_k = p_j - p_k. \tag{4.15}$$

Dette udtryk og ligningen fra (4.12) anvendes til at omskrive (4.13). Herved fås

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s),$$

og den første del af lemmaet er bevist. For den anden del huskes, at p_j og p_k har multigrad δ og førende koefficienter 1. Derfor må $p_j - p_k$ have en multigrad skarpt mindre end δ. Ifølge ligning (4.15) har alle S-polynomierne dermed også en multigrad mindre end δ. □

Det vil sige, at hvis polynomierne $f_1, \ldots, f_s$ opfylder betingelserne i lemma 4.9, da gælder, at

$$\sum_{i=1}^{s} c_i f_i = \sum_{j,k} c_{j,k} S(f_j, f_k). \tag{4.16}$$

Ved at anvende ovenstående lemma og eksistensen af S-polynomier, er det muligt at bestemme hvornår et givet basis er Gröbner. Sætningen er kendt under navnet Buchbergers kriterium.

Sætning 4.11 (Buchbergers kriterium)**.** *Lad I være et ideal over $k[x_1, \ldots, x_n]$. Et basis $G = \{g_1, \ldots, g_t\}$ for I er et Gröbnerbasis hvis og kun hvis for alle par $i \neq j$ at resten ved division af $S(g_i, g_j)$ med G er lig nul.*

Bevis. Antag for det først at $G = \{g_1, \ldots, g_t\}$ er et Gröbnerbasis for idealet $I \subseteq k[x_1, \ldots, x_n]$. Pr. definition af S-polynomiet så $S(g_i, g_j) \in I$, $i \neq j$. Ifølge korollar 4.4 gælder da, at resten ved division af $S(g_i, g_j)$ med G er lig nul.

Anden del af beviset er lidt mere besværligt. Pr. antagelse er I et ideal over $k[x_1, \ldots, x_n]$ hvilket ifølge Hilberts basis sætning, sætning 4.7 kan skrives som $I = \langle g_1, \ldots, g_t \rangle$ for nogle $g_1, \ldots, g_t \in I$. Det skal vises, at hvis resten ved division af alle S-polynomier med G er nul, så $\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$ (se definition 4.14). Med andre ord, for et ikke-nul polynomium $f \in I$ skal der gælde, at $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$. Bemærk, at der findes polynomier $h_i \in k[x_1, \ldots, x_n]$, sådan at

$$f = \sum_{i=1}^{t} h_i g_i.$$

Om f gælder jvf. lemma 4.6, at

$$\begin{aligned} \text{multideg}(f) &= \text{multideg}\left(\sum_{i=1}^{t} h_i g_i\right) \\ &\leq \max\left\{\text{multideg}(h_i g_i)\right\}. \end{aligned} \tag{4.17}$$

Resten af beviset handler om at vise at der rent faktisk gælder lighed i formel (4.17). For hvis der gælder lighed, må $LT(f) = LT(h_i g_i)$. Når dette er tilfældet, så ses, at

$$\begin{aligned} LT(f) = LT(h_i g_i) = LC(h_i g_i) LM(h_i g_i) &= LC(h_i g_i) x^{\text{multideg}(h_i g_i)} \\ &= LC(h_i g_i) x^{\text{multideg}(h_i) + \text{multideg}(h_i)} \\ &= LC(h_i g_i) x^{\text{multideg}(h_i)} x^{\text{multideg}(g_i)} \\ &= LC(h_i g_i) LM(h_i) LM(g_i), \end{aligned}$$

hvilket giver, at $LT(g_i)$ går op i $LT(f)$. Da alle idealer over $k[x_1, \ldots, x_n]$ er monomielle ifølge sætning 4.6, så betyder det jvf. lemma 4.7, at $LT(f) \in \langle LT(g_1), \ldots, LT(g_t) \rangle$. Det skal derfor vises, at

$$\text{multideg}(f) = \max\left\{\text{multideg}(h_i g_i)\right\}. \tag{4.18}$$

Definér $m(i) = \text{multideg}(h_i g_i)$ og $\delta = \max(m(1), \ldots, m(t))$, sådan at der ved indsættelse i ulighed (4.17) gælder, at

$$\text{multideg}(f) \leq \delta. \tag{4.19}$$

Det bemærkes, at selvom f er udtrykt på formen $\sum_{i=1}^{t} h_i g_i$, så er dette ikke endtydigt. Det vil sige, at der findes muligvis mange forskellige måder at opskrive f på, hvor f har denne form. For hver af disse måder at opskrive f på, findes et δ, men alle δ'erne er ikke nødvendigvis ens. Fordi en monomiel ordning er valgt, og ordningen pr. definition er vel-ordnet, så findes et mindste δ. Det giver derfor mening at vælge δ til at være minimalt. Spørgsmålet er så, om det mindst mulige δ er multideg(f). Dette må simpelthen være tilfældet, såfremt det kan vises, at multideg(f) $\geq \delta$. Dette

gøres ved et modstridsbevis. Antag modsætningsvist multideg$(f) < \delta$, og omskriv f:

$$\begin{aligned} f &= \sum_{m(i)=\delta}^{t} h_i g_i + \sum_{m(i)<\delta}^{t} h_i g_i \\ &= \sum_{m(i)=\delta}^{t} LT(h_i) g_i + \sum_{m(i)=\delta}^{t} \left(h_i - LT(h_i)\right) g_i + \sum_{m(i)<\delta}^{t} h_i g_i. \end{aligned} \tag{4.20}$$

Det bemærkes, at monomierne i den anden og tredie sum i ovenstående udtryk alle har en grad mindre end δ. I sum nummer to kan $h_i g_i$ som maksimum have grad δ, men da $LT(h_i)g_i$ trækkes fra i summen, må monomierne i hele summen have grad mindre end δ. Ifølge antagelsen om, at multideg$(f) < \delta$, så må det betyde, at multigraden til den første sum må være mindre end δ. Det vil blive vist, at dette resultat medfører, at multigraden til hvert led i summen er mindre end δ, hvilket er i modstrid med, at δ er minimal. Til at skabe modstriden anvendes S-polynomierne.

Lad $LT(h_i) = c_i x^{\alpha(i)}$, så $\sum_{m(i)=\delta}^{t} LT(h_i)g_i = \sum_{m(i)=\delta}^{t} c_i x^{\alpha(i)} g_i$. Ifølge lemma 4.9, eller nærmere bestemt ligning (4.16), gælder, at

$$\sum_{m(i)=\delta}^{t} c_i x^{\alpha(i)} g_i = \sum_{j,k} c_{j,k} S(f_j, f_k) \tag{4.21}$$

hvor $f_i = x^{\alpha(i)} g_i$. Betragtes S-polynomierne kan de skrives som

$$\begin{aligned} S(f_j, f_k) &= S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) \\ &= \frac{x^\delta}{LT(x^{\alpha(j)} g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{LT(x^{\alpha(k)} g_k)} x^{\alpha(k)} g_k. \end{aligned}$$

Ved brug af lemma 4.5 giver det, at

$$\begin{aligned} S(f_j, f_k) &= \frac{x^\delta}{x^{\alpha(j)} LT(g_j)} x^{\alpha(j)} g_j - \frac{x^\delta}{x^{\alpha(k)} LT(g_k)} x^{\alpha(k)} g_k \\ &= \frac{x^\delta}{LT(g_j)} g_j - \frac{x^\delta}{LT(g_k)} g_k \\ &= x^\delta \left(\frac{1}{LT(g_j)} g_j - \frac{1}{LT(g_k)} g_k. \right) \end{aligned}$$

Lad $x^{\gamma_{j,k}} = LCM(LM(g_j), LM(g_k))$, da fås jvf. defnitionen af S-polynomiet 4.18, at

$$\begin{aligned} S(f_j, f_k) &= x^{\delta - \gamma_{j,k}} \left(\frac{x^{\gamma_{j,k}}}{LT(g_j)} g_j - \frac{x^{\gamma_{j,k}}}{LT(g_k)} g_k \right) \\ &= x^{\delta - \gamma_{j,k}} S(g_j, g_k). \end{aligned}$$

Indføres denne omskrivning af S-polynomierne i udtrykket fra (4.21), giver det, at

$$\sum_{m(i)=\delta}^{t} LT(h_i) g_i = \sum_{j,k} c_{j,k} x^{\delta - \gamma_{j,k}} S(g_j, g_k).$$

Husk, at beviset blev initieret med en antagelse om, at resten ved division af $S(g_i, g_j)$ med G var lig nul. Dette gør, at S-polynomierne kan omskrives endnu engang. Ved divisionsalgoritmen for

polynomier i flere variable, sætning 4.4, hvor $S(g_j, g_k) \in k[x_1, \ldots, x_n]$, og G er en ordnet tuppel er polynomier over $k[x_1, \ldots, x_n]$, fås da, at

$$S(g_j, g_k) = \sum_{i=1}^{s} a_{i,j,k} g_i \Rightarrow \tag{4.22}$$

$$\sum_{m(i)=\delta}^{t} LT(h_i) g_i = \sum_{j,k} c_{j,k} x^{\delta - \gamma_{j,k}} \sum_{i=1}^{s} a_{i,j,k} g_i, \tag{4.23}$$

med $a_{i,j,k} \in k[x_1, \ldots, x_n]$. Af sætning 4.4 følger også, at

$$\text{multideg}(a_{i,j,k} g_i) \leq \text{multideg}(S(g_j, g_k)). \tag{4.24}$$

Hvis udtrykket fra (4.22) multipliceres med $x^{\delta - \gamma_{j,k}}$ på begge sider af lighedstegnet, så

$$\begin{aligned} x^{\delta - \gamma_{j,k}} S(g_j, g_k) &= x^{\delta - \gamma_{j,k}} \sum_{i=1}^{s} a_{i,j,k} g_i \\ &= \sum_{i=1}^{s} b_{i,j,k} g_i \end{aligned} \tag{4.25}$$

hvor $b_{i,j,k} = x^{\delta - \gamma_{j,k}} a_{i,j,k}$, udledes samtidigt at følgende må gælde:

$$\text{multideg}(b_{i,j,k} g_i) \leq \text{multideg}(x^{\delta - \gamma_{j,k}} S(g_j, g_k)).$$

Det huskes, at vores antagelse i starten, $f < \delta$, sammen med lemma 4.9 førte til, at $S(g_i, g_j)$ havde en multigrad mindre end δ for alle i, j. Anvendes dette i ovenstående udtryk, gælder, at

$$\text{multideg}(b_{i,j,k} g_i) \leq \text{multideg}(x^{\delta - \gamma_{j,k}} S(g_j, g_k)) < \delta. \tag{4.26}$$

Tag nu udtrykket fra (4.25) og indsæt i (4.23). Dette giver, at

$$\sum_{m(i)=\delta}^{t} LT(h_i) g_i = \sum_{j,k} c_{j,k} \left(\sum_{i=1}^{s} b_{i,j,k} g_i \right) = \sum_{i} \tilde{h}_i g_i,$$

hvor jvf. uligheden i (4.26), at

$$\text{multideg}(\tilde{h}_i g_i) < \delta.$$

Hvis i ligning (4.20), at $\sum_{m(i)=\delta}^{t} LT(h_i) g_i$ udskiftes med $\sum_i \tilde{h}_i g_i$, så haves et udtryk for f, hvor alle led i udtrykket har en multigrad mindre end δ. Dette er i modstrid med at δ er minimal, så antagelsen om at $\text{multideg}(f) < \delta$ er ej sand. Ergo må $\text{multideg}(f) \geq \delta$ være sand og sammen med uligheden i (4.19) fås, at $\text{multideg}(f) = \delta$. Dvs. udtrykket i (4.18) er sand, og dermed ligger $LT(f)$ i $\langle LT(g_1), \ldots, LT(g_t) \rangle$, hvorfor G er et Gröbnerbasis. □

Eksempel 4.15. *Lad $I = \langle xy + x^2, 3y + x \rangle$ være et ideal over $k[x, y, z]$. Påstanden er da, at $G = \{g_1, g_2\}$, hvor $g_1 = x - 2y$ og $g_2 = y^2 - 2z^2$, er et Gröbnerbasis for I. Til at afgøre om påstanden er sand anvendes Buchbergers kriterium. Som monomiel ordning vil den graduerede*

reverse leksikografiske ordning blive anvendt, sætning 4.10. Først opskrives S-polynomiet for g_1 og g_2:

$$\begin{aligned} S(g_1, g_2) &= \frac{xy^2}{x}(x - 2y) - \frac{xy^2}{y^2}\left(y^2 - 2z^2\right) \\ &= y^2(x - 2y) - x(y^2 - 2z^2) \\ &= -2y^3 + 2xz^2 \end{aligned}$$

Ved at anvende algoritmen for division af polynomier i flere vaiable, sætning 4.4, til at dividére G op i $S(g_1, g_2)$ fås, at

$$S(g_1, g_2) = -2y^3 + 2xz^2 = 2z^2(x - 2y) + (-2y)(y^2 - 2z^2) + 0.$$

Det ses derfor, at resten ved division af S-polynomiet med G er lig nul, hvorfor G ifølge sætning 4.11 er et Gröbnerbasis.

Med Buchbergers kriterium eksisterer derved en metode til at bestemme, hvornår et givet basis er et Gröbnerbasis. Sætningen siger dog intet om, hvordan man konstruerer et Gröbnerbasis til et givet ideal, og det vides jo fra korollar 4.3, at alle idealer I over $k[x_1, \ldots, x_n]$ forskelligt fra nulidealet har et Gröbnerbasis. I det næste afsnit ses nærmere på, hvordan et Gröbnerbasis konstrueres.

4.6 Buchbergers algoritme

I det følgende afsnit præsenteres en algoritme til bestemmelse af Gröbnerbaser for ikke-nul idealer over $k[x_1, \ldots, x_n]$. Algoritmen har sin grundidé i at udvide et givet basis til idealet I med S-polynomierne. Det hører med til historien, at der findes korrektioner til Buchbergers algoritme, som gør den mere effektiv. Når den følgende udgave af Bucbergers algoritme er valgt, skyldes det, at det er nemt at gennemskue, hvad der foregår og så er det samme udgave som fremgår i kap. 2, §7 [2008 Cox, Little & O´Shea].

Sætning 4.12. *Lad $I = \langle f_1, \ldots, f_s \rangle$ være et ideal over $k[x_1, \ldots, x_n]$, som er forskelligt fra nulidealet. Ved følgende algoritme konstrueres da et Gröbnerbasis til I:*

Input: *Et system af polynomier $F = (f_1, \ldots, f_s)$*
Output: *Et Gröbnerbasis $G = \{g_1, \ldots, g_t\}$ til I, sådan at $F \subseteq G$*
$G := F$
Gentag
  $G' := G$
  For *hvert par $\{p, q\}$, $p \neq q$ i G'* ***gør***
    $S := \overline{S(p, g)}^{G'}$
    Hvis $S \neq 0$, ***så*** $G := G \cup \{S\}$
Indtil $G = G'$

Bevis. Strategien i beviset er at benytte Buchbergers kriterium til at afgøre om outputtet er Gröbnerbasis for I. Det vil sige, at to ting skal vises. For det første skal det vises, at G er et et

basis for I. Dernæst skal det vises, at resten ved division af S-polynomierne med G være lig nul. For at lette arbejdsbyrden indføres først følgende notation. For $G = \{g_1, \ldots, g_t\}$ defineres idealerne $\langle G \rangle$ og $\langle LT(G) \rangle$ som udtrykt ved

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle$$
$$\langle LT(G) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle .$$

Da G til at starte med i algoritmen sættes lig F, så er G klart indeholdt i I. Spørgsmålet er, om G også er indeholdt i I efter udvidelsen. Udvidelsen sker ved at tilføje $S := \overline{S(p,g)}^{G'}$, for $p, q \in G$ til G. Når $G \subseteq I$, betyder det, at også $p, q \in I$. Når $p, q \in I$, så endvidere også $S(p,q) \in I$. Da $S(p,q)$ divideres med $G' \in I$, så $S := \overline{S(p,g)}^{G'} \subseteq I$. Dette medfører, at også $G \cup \{S\} \subseteq I$. Det bemærkes, at F dermed er indeholdt i G, men F var et basis for I, så derfor må G også være et basis for I. Algoritmen standser for $G = G'$, og dette sker når $S := \overline{S(p,g)}^{G'} = 0$. Ifølge sætning 4.11 fås derfor, at G er et Gröbnerbasis, hvis algoritmen standser, og sætningen er bevist. Der er derfor tilbage at vise, at algoritmen er endelig.

Husk, at G er konstrueret ud fra det forrige G, nemlig G', og S. Nødvendigvis må der gælde, at $G' \subseteq G$. Dette medfører, at

$$\langle LT(G') \rangle \subseteq \langle LT(G) \rangle . \tag{4.27}$$

Specielt gælder, at hvis $G' \neq G$, så $\langle LT(G') \rangle \subsetneq \langle LT(G) \rangle$. At dette er sandt ses af følgende overvejelse. Antag f.eks. at resten ved division af S-polynomiet er blevet tilføjet i G. Siden at r er resten som fås ved division med G', så er $LT(r)$ ej indeholdt i $\langle LT(G') \rangle$. Men $LT(r) \in \langle LT(G') \rangle$, hvorfor påstanden er vist. Det ses jvf. udtrykket i (4.27), at idealerne $\langle LT(G') \rangle$ danner en stigende kæde af idealer over $k[x_1, \ldots, x_n]$, så ifølge sætning 4.8 vil kæden stabilisere sig efter et bestemt antal iterationer, hvorved $\langle LT(G') \rangle = \langle LT(G) \rangle$. Pga. den idligere diskussion haves dermed at $G' = G$ og at algoritmen stopper efter et bestemt antal iterationer. □

Algoritmen er en såkaldt heuristisk algoritme, hvilket betyder, at den prøver sig frem indtil et Gröbnerbasis er fundet. Algoritmen gør det muligt at konstruere programmer, som direkte kan bestemme Gröbnerbaser til et givet ideal. Imidlertid er det også værd at bemærke, at sætning 4.12 blot er en udgave ud af mange, som konstruerer det ønskede. Der findes udvidelser af algoritmen, som har flere forskellige fordele. Programmet Singular anvender i grove træk algoritmen fra sætning 4.12 til at bestemme Gröbnerbaser. Kommandoen i Singular, som finder et Gröbnerbasis til et givet ideal, er std. I det følgende eksempel illustreres, hvor nemt det er at konstruere Gröbnerbaser i programmet Singular.

Eksempel 4.16. *Lad $I = \langle 3xz^2 + xy, x^3 - y^4z^2 \rangle \subseteq \mathbb{F}_5[x,y,z]$. Den leksikografiske ordning anvendes med $x > y > z$. Kommandoen std(I) i singular udregner basis for idealet.*

```
> ring R=5,(x,y,z),lp;
> ideal I=3xz2+xy, x3-y4z2;
> std(I);
_[1]=y5z2-2y4z4
_[2]=xy-2xz2
_[3]=x3-y4z2
```

Det vil sige, at $G = \{y^5z^2 - 2y^4z^4, xy - 2xz^2, x^3 - y^4z^2\}$ er et Gröbnerbasis for I.

Det fundne Gröbnerbasis i eksemplet er dog ikke nødvendigvis entydigt bestemt. Faktisk er $\tilde{G} = \{y^5z^2 - 2y^4z^4, xy - 2xz^2, x^3 - y^4z^2 + axy\}$, med $a \in k$ en konstant, også et Gröbnerbasis til I. Det er ønskværdigt med et entydigt Gröbnerbasis, fordi man da, ud fra dem kan afgøre om to idealer er ens. Gør nu følgende iagttagelse:

Lemma 4.10. *Lad G være et Gröbnerbasis for idealet I over $k[x_1, \ldots, x_n]$ og tag et polynonium $g \in G$, hvor $LT(g) \in \langle LT(G - \{g\})\rangle$. Da gælder, at $G - \{g\}$ også er et Gröbnerbasis for I.*

Bevis. Da G er et Gröbnerbasis for I, så gælder pr. definition, at $\langle LT(G)\rangle = \langle LT(I)\rangle$. Hvis $LT(g) \in \langle LT(G - \{g\})\rangle$, må der gælde, at

$$\langle LT(G - \{g\})\rangle = \langle LT(G)\rangle = \langle LT(I)\rangle .$$

Dvs., at $G - \{g\}$ er Gröbnerbasis for I. □

Lemmaet fortæller os, at hvis vi multiplicerer alle polynomier i et Gröbnerbasis med en passende konstant, sådan at alle ledende koefficienter bliver lig 1, og fjerner alle polynomier g med $LT(g) \in \langle LT(G - \{g\})\rangle$, så vil det resterende $G - \{g\}$ også være et Gröbnerbasis. Med denne handling fjernes altså alle de overflødige polynomier fra Gröbnerbasen. Dette er et skridt i jagten på at finde et entydigt Gröbnerbasis og giver dermed mening til nedenstående definition.

Definition 4.19. *Et minimalt Gröbnerbasis til et ideal I over $k[x_1, \ldots, x_n]$ er et basis G for I som opfylder, at*

(i) $LC(g) = 1$ *for alle* $g \in G$.

(ii) For alle $g \in G$ gælder, at $LT(g) \notin \langle LT(G - \{g\})\rangle$.

Eksempel 4.17. *I eksemplet fra før, fandt Singular Gröbnerbasis $G = \{y^5z^2 - 2y^4z^4, xy - 2xz^2, x^3 - y^4z^2\}$ til idealet $I = \langle 3xz^2 + xy, x^3 - y^4z^2\rangle \subseteq \mathbb{F}_5[x, y, z]$. Det ses, at Singular dermed også direkte finder det minimale Gröbnerbasis. Alle de ledende koefficienter er 1, så dette skal vi ikke bekymre os om. Til gengæld bemærkes, at ingen af de førende led til polynomierne i G, kan udtrykkes ved hjælp af de andre. De tre førende led ved brug af den leksikografiske ordning er y^5z^2, xy og x^3, hvor alle er en sammensætning af forskellige variable. Husk også, at det fundne Gröbnerbasis ej var entydigt, hvilket vil sige, at det minimale Gröbnerbasis ej heller er entydigt.*

Et minimalt Gröbnerbasis er stadig ikke entydigt, men der findes faktisk et specielt minimalt Gröbnerbasis, som er entydigt bestemt. Dette kaldes for *det reducerede Gröbnerbasis.*

Definition 4.20. *Et reduceret Gröbnerbasis til et ideal I over $k[x_1, \ldots, x_n]$ er et basis G for I som opfylder, at*

(i) $LC(p) = 1$ *for alle* $p \in G$

(ii) For alle $p \in G$, gælder, at intet monomium i p ligger i $\langle LT(G - \{p\})\rangle$.

At det reducerede Gröbnerbasis er entydigt bestemt, vises i følgende sætning

Sætning 4.13. *Lad I være et ideal over $k[x_1, \ldots, x_n]$, som er forskelligt fra nul-idealet. Givet en monomiel ordning til I, da har I ét og kun ét reduceret Gröbnerbasis.*

Bevis. Beviset er et eksistens og entydighedsbevis. Først vises eksistensen af et reduceret Gröbnerbasis, og dernæst vises at det er entydigt bestemt. Lad G være et minimalt Gröbnerbasis for et ikke-nul ideal I. Om $g \in G$ siges, at g er reduceret ift. G såfremt at intet monomium i g tilhører idealet $\langle LT(G - \{g\})\rangle$. Målet er at korrigere G indtil det er et reduceret Gröbnerbasis for I. Til at starte med gøres en observation vedrørende g. Hvis g er reduceret ift. G, da er g også reduceret ift. ethvert andet minimalt Gröbnerbasis D til I, som g er indeholdt i, og hvor mængden af førende led til D er lig mængden af førende led til G. Denne påstand følger af definitionen for reduceret Gröbnerbasis, hvor kun de førende led er involveret.

Lad nu $g \in G$ være givet og sæt hhv. $g' = \tilde{g}^{G-\{g\}}$ og $G' = (G - \{g\} \cup \{g'\})$. Det vil nu blive vist, at G' er et minimalt Gröbnerbasis til I. At G' først og fremmest er et Gröbnerbasis ses jvf. def. 4.14. Der gælder nemlig, at $LT(g') = LT(g)$ fordi ved division af g med $G - \{g\}$ indgår $LT(g)$ som en del af resten. Dette skyldes at $LT(g)$ ej er dividerbart med noget element i mængden $LT(G - \{g\})$. Heraf fås, at $\langle LT(G')\rangle = \langle LT(G)\rangle$. Da G' er indeholdt i I, må det være et Gröbnerbasis. Jævnfør diskussionen ledende op til definition 4.19, så findes også et minimalt Gröbnerbasis til I. Pr. konstruktion er g' reduceret i forhold til G'.

Gør ovenstående for alle elementerne i G. Hver gang maskinen gennemløbes én gang, kan det ændre på Gröbnerbasen men uanset hvad, bliver resultatet et reducerende Gröbnerbasis, for når først et Gröbnerbasis er reducerende, så forbliver det også reducerende. De førende led ændres nemlig ikke. For sat bevise entyidigheden tages to recucerede Gröbnerbaser G og $\tilde{G}$ for det samme ideal. Særligt gælder om de begge, at de er minimale Gröbnerbaser, hvorfor der gælder, at $LT(G) = LT(\tilde{G})$. Det vil sige, at givet $g \in G$, findes et $\tilde{g} \in \tilde{G}$, sådan at $LT(g) = LT(\tilde{g})$. Hvis det kan vises, at $g = \tilde{g}$, så $G = \tilde{G}$, og sætningen er bevist.

Betragt $g - \tilde{g}$. Dette ligger i I og da G er et Gröbnerbasis for I, så $\overline{g - \tilde{g}}^{G} = 0$ jvf. Buchbergers kriterium, sætning 4.11. Da endvidere $LT(g) = LT(\tilde{g})$, forsvinder disse led i $g - \tilde{g}$. Dermed er der ingen led tilbage som er dividérbare med $LT(G) = LT(\tilde{G})$ fordi både G og $\tilde{G}$ er reducerede. Dette viser, at $\overline{g - \tilde{g}}^{G} = g - \tilde{g}$, hvilket medfører, at $g - \tilde{g} = 0$. □

Når to idealer skal sammenlignes i en eller anden forstand giver det altså mening at betragte de reducerede Gröbnerbaser. F.eks. kunne man stille spørgsmålet om to idealer er ens. For at besvare det findes de reducerede Gröbnerbaser for de to idealer, og er de ens, så må idealerne også være ens. Er de to reducerede Gröbnerbaser forskellige, så er ligeså også idealerne. Faktisk haves nu to metoder til at afgøre om to idealer er ens.

4.7 Hilberts Nullstellensatz

I dette afsnit præsenteres Hilberts (svage) Nullstellensatz. Denne vil senere blive brugt i beviset for et meget vigtigt resultat ift. netværkskodning. For et reelt bevis for sætningen refereres til [2008 Cox, Little & O´Shea]. Her vil istedet indgå en forklaring af, hvad sætningen gør. Husk fra afsnit 4.1 mængden $\mathbf{I}(V)$ for en affin variant $V \subseteq k^n$ blev defineret ved

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] | f(x) = 0 \text{ for alle } x \in V\}.$$

Vi så, at hvis man ønskede at sige noget om V, da var det nok at betragte $\mathbf{I}(V)$. Det vil sige, at vi fandt en afbilding, som gik fra affine varianter til idealer. I afsnit 4.4 definerede vi desuden for

et givet ideal $I \subseteq k[x_1, \ldots, x_n]$ mængden

$$\mathbf{V}(I) = \{x \in k^n \mid f(x) = 0 \text{ for alle } f \in I\}$$

Det blev vist, at $\mathbf{V}(I)$ er en affin variant, og hvis $I = \langle f_1, \ldots, f_s \rangle$, så $\mathbf{V}(I) = V(f_1, \ldots, f_s)$. Mængden $\mathbf{V}(I)$ består af fælles rødder til polynomierne $f_1, \ldots, f_s$. Hermed haves også en afbilding fra et ideal I over i en verdenen af affine varianter $\mathbf{V}(I)$. Det kunne være rart, hvis både I og V er én-til-én afbildinger, men sådan forholder det sig i midlertid ikke. Dette ses bl.a. af at to forskellige idealer godt kan have den samme tilhørende affine variant, så V er ikke én-til-én. F.eks. er idealerne $\langle x \rangle$ og $\langle x^2 \rangle$ ens i $k[x]$, men $\mathbf{V}(x) = \mathbf{V}(x^2) = 0$.

En særlig situation kan opstå, hvis legemet k ikke er algebraisk lukket.

Definition 4.21. *Et legeme k siges at være algebraisk lukket, hvis ethvert polynomium med en variabel af grad mindst en og koefficienter i k, har rødder i k.*

Betragt f.eks. polynomierne $f = 1$, $h = 1 + x^2$ og $p = 1 + x^2 + x^4$ i $\mathbb{R}[x]$. Disse genererer idealerne

$$I_1 = \langle 1 \rangle = \mathbb{R}[x] \qquad I_2 = \langle 1 + x^2 \rangle \qquad I_3 = \langle 1 + x^2 + x^4 \rangle,$$

hvilke alle er forskellige. Hverken f,h eller p har reelle rødder, så derfor haves, at $\mathbf{V}(I_1) = \mathbf{V}(I_2) = \mathbf{V}(I_3) = \emptyset$. Til forskel fra eksemplet fra før er de tre idealer inden for verdenen af affine varianter nu repræsenteret ved den tomme mængde. Spørgsmålet er da, om det samme er tilfældet, hvis legemet var under et algebraisk aflukke. Det er nemt at se, at problemet i hvert fald forsvinder i det en-dimensionelle tilfælde over $k[x]$:

For det første indses, at ethvert ideal I over $k[x]$ kan frembringes af et polynomium, ie. $I = \langle f \rangle$, hvor $f \in k[x]$. Så må $\mathbf{V}(I)$ være rødderne til f, som med andre ord er de a'er, $a \in k$, som opfylder, at $f(a) = 0$. Da k er algebraisk lukket, har ethvert ikke-konstant polynomium i legemet mindst en rod. Den eneste tidspunkt, hvor $\mathbf{V}(I)$ bliver tom, må da være, hvis polynomiet er lig en konstant forskellig fra nul. I dette tilfælde vil $\frac{1}{f} \in k$. Det medfører, at $1 = \frac{1}{f} \cdot f \in I$, som igen betyder, at $g = g \cdot 1 \in I$ for alle $g \in k$. Ergo må $I = k[x]$ være det eneste ideal, hvor $\mathbf{V}(I) = \emptyset$, så længe at k er algebraisk lukket. Det viser sig, at hvis polynomier af flere variable betragtes, så er idealet $I = \overline{k}[x_1, \ldots, x_n]$ det eneste ideal, som opfylder, at $\mathbf{V}(I) = \emptyset$. Her er $\overline{k}[x_1, \ldots, x_n]$ det algebraiske aflukke til $k[x_1, \ldots, x_n]$. Dette er essensen i Hilberts svage Nullstellensatz.

Sætning 4.14 (Hilberts svage Nullstellensatz)**.** *Lad k være et algebraisk lukket legeme, og lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal som opfylder, at $\boldsymbol{V}(I) = \emptyset$. Da gælder, at $I = k[x_1, \ldots, x_n]$*

Beviset kan findes i kap. 4, §1 i [2008 Cox, Little & O´Shea]. I det særlige tilfælde hvor $k = \mathbb{C}$ refereres sætningen ofte til som *Fundamental Theorem of Algebra for multivariable polynomials.* Sætningen har fået navn efter den tyske matematiker David Hilbert (1862-1943), som anses for at have været en af de matamatikere, der i nyere tid har haft størst betydning for matematikken. Omkring år 1900 fremlagde han en samling af matematiske problemer, som kom til at danne rammen for forskningen i årene efter.

Sætningen er ikke kun vigtig, fordi den hjælper os til at bevise hovederesultatet for teorikapitlet.

Dette er blot en lille sidegevinst. Faktisk er sætningen med til at afgøre om et givet system

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 0 \\ &\vdots \\ f_s &= 0, \end{aligned}$$

hvor $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, har en løsning i $\mathbb{C}^n$. Hvis systemet ikke har en fælles løsning, så svarer det til, at $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$. Ifølge sætning 4.14 så er ligningerne overholdt, hvis og kun hvis $1 \in \langle f_1, \ldots, f_s \rangle$. For at se, at 1 tilhører idealet frembragt af $f_1, \ldots, f_s$, får vi brug for en påstand om, at for enhver monomiel ordning er $\{1\}$ det eneste reducerede Gröbnerbasis for idealet $\langle 1 \rangle$. For at vise påstanden lad $\{g_1, \ldots, g_t\}$ være et Gröbnerbasis til $I = \langle 1 \rangle$. Hermed gælder, at $1 \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Jvf. lemma 4.7 så findes et $LT(g_i)$, som går op i 1. Antag at dette er $LT(g_1)$. Dette betyder, at $LT(g_1)$ må være en kostant, og alle andre $LT(g_i)$ er et multiplum af $LT(g_1)$. Ifølge lemma 4.10 kan $g_2, \ldots, g_t$ fjernes fra vores Gröbnerbasis. Det ses også, at da $LT(g_1)$ er en konstant, så må også g_1 være en konstant, fordi ethvert ikke-konstant monomium ifølge korollar 4.2 er skarpt større end 1. Det er muligt at multiplicere g_1 med en passende kostant, så $g_1 = 1$ fås. Dvs., at det reducerede Gröbnerbasis er $\{1\}$.

Med påstanden vist, giver den, at systemet fra før har en løsning i $\mathbb{C}^n$, såfremt at idealet frembragt af $f_1, \ldots, f_s$ ikke har det reducerede Gröbnerbasis $\{1\}$. Dette kriterium er altså nok for at afgøre om systemet har den ønskede løsning. Hilberts svage Nullstellensatz findes også i en 'stærk' udgave.

Sætning 4.15 (Hilberts (stærke) Nullstellensatz)**.** *Lad k være et algebraisk lukket legeme. Hvis $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ er valgt, så $f \in \boldsymbol{I}(\boldsymbol{V}(f_1, \ldots, f_s))$, da findes et helt tal $m \geq 1$, sådan at*

$$f^m \in \langle f_1, \ldots, f_s \rangle .$$

I det følgende afsnit introduceres begrebet et radikalt ideal, da der er speciel sammenhæng mellem radikale idealer og affine varieteter.

4.8 Radikale idealer

I dette afsnit vil vi undersøge de idealer nærmere, som indeholder *alle* polynomier, der forsvinder på en given affin varietet. Disse kaldes for radikale idealer, og der er en særlig sammenhæng imellem disse og de affine varieteter. Først gøres følgende iagttagelse om $I(V)$:

Lemma 4.11. *Lad $\boldsymbol{V}$ være en affin varietet. Hvis $f^m \in I(V)$, så $f \in I(V)$.*

Bevis. Beviset for lemmaet kommer ret nemt. Lad $x \in \mathbf{V}$. Hvis $f^m \in I(V)$, så $(f(x))^m = 0$. Dette medfører, at $f(x) = 0$. Da $x \in \mathbf{V}$ var valgt arbitrært, så $f(x) \in I(V)$. □

Lemmaet angiver at hvis et ideal indeholdende alle polynomier, som forsvinder på en given affin varietet, haves, da gælder, at hvis et polynomium opløftet i en potens tilhører idealet, så tilhører polynomiet i sig selv også idealet. Resten af afsnittet handler om det specielle ved denne type af idealer. Endda er de så specielle at de har fået deres eget navn.

Definition 4.22. *Et ideal I siges at være radikalt, hvis for et polynomium f^m, $m \geq 1$, der gælder, at $f \in I$.*

Korollar 4.5. *$\boldsymbol{I}(V)$ er et radikalt ideal.*

Bevis. Korollaret følger direkte af lemma 4.11 og definition 4.22. □

$\mathbf{I}(V)$ er et eksempel på et radikalt ideal.

På den anden sige giver Hilberts Nullstellensatz, sætning 4.14 at den eneste måde, hvorpå et ideal ikke kan være idealet indeholdende alle polynomier, som forsvinder på $\mathbf{V}(I)$, er ved I indeholder polynomier f^m, hvor f ej ligger i I. Et ideal I kan altså ikke være idealet indeholdende alle polynomier, som forsvinder på $\mathbf{V}(I)$, såfremt I er et radikalt ideal. Det tyder på at der er en one-to-one korrespondence imellem radikale idealer og affine varieteter. For at undersøge dette fænomen nærmere introduceres først følgende notation:

Definition 4.23. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal. Radikalet til idealet skrives som $\sqrt{I}$ og er udtrykt ved mængden*

$$\sqrt{I} = \{f \mid f^m \in I \text{for et helt tal } m \geq 1\}.$$

Navnet på begrebet i definition 4.22 og mængden i ovenstående definition er selvfølgelig ikke tilfældigt valgte. Faktisk er det en og samme ting, hvilket ses i det følgende korollar.

Korollar 4.6. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal. Idealet I er radikalt hvis og kun hvis $I = \sqrt{I}$.*

Bevis. Det bemærkes, at inklusionen $I \subseteq \sqrt{I}$ altid gælder, uanset om I er et radikalt ideal eller ej. Tag f.eks. $f \in I$, så $f = f^1 \in I$. Dvs. at også $f \in \sqrt{I}$ pr. konstruktion, og inklusionen gælder. Antag at I er et radikalt ideal. Jvf. def. 4.22 er I radikalt hvis og kun hvis I indeholder alle de polynomier f, som opfylder, at hvis $f^m \in I$, m helt tal større end nul, så også $f \in I$. Det ses, at hvis $\sqrt{I}$ også er et radikalt ideal, må de to idealer være ens. Tag polynomium $f \in \sqrt{I}$, så gælder pr. konstruktion af $\sqrt{I}$, at $f^m \in I$ for et helt tal $m \geq 1$. Lad $h = \frac{1}{f^{m-1}}$, så $h \in k[x_1, \ldots, x_n]$. Da I er et ideal, så gælder jvf. (iii) i def. 4.2, at $hf \in I$. Da $hf = f$, så endvidere $f \in I$. Ergo må $\sqrt{I}$ være et radikalt ideal. □

Lemma 4.12. *Hvis $I \subseteq k[x_1, \ldots, x_n]$ er et ideal, da er også $\sqrt{I}$ et ideal i $k[x_1, \ldots, x_n]$.*

Bevis. De tre betingelser i definition 4.2 skal være opfyldt, for at $\sqrt{I}$ kan være et ideal. Husk, at $I \subseteq \sqrt{I}$ altid gælder, hvorfor $0 \in \sqrt{I}$. Tag $f, g \in \sqrt{I}$, så findes positive hele tal m, l sådan at $f^m, g^l \in I$. Betragt $(f+g)^{m+l-1}$. I den binomielle udviddelse til dette udtryk vil der i hvert led indgå faktoren $f^i g^j$, hvor $i + j = m + l - 1$. Idet at hverken $i \geq m$ eller $j \geq l$, så må enten f^i eller g^j ligge i I. Det betyder, at $f^i g^j \in I$ og endvidere at alle led i udviddelsen ligger i I. Ergo må også $(f+g)^{m+l-1} \in I$, hvilket medfører, at også $f + g \in I$. Antag at $f \in \sqrt{I}$ og $h \in k[x_1, \ldots, x_n]$. Da haves, at $f^m \in I$ for et positivt helt tal m. Fordi I er et ideal, giver det, at $h^m f^m \in I$. Heraf fås, at $hf \in \sqrt{I}$, hvorfor $\sqrt{I}$ må være et ideal. □

I det følgende eksempel benyttes programmet Singular til at udregne radikalet til et ideal I.

Eksempel 4.18. *Lad $I = \langle x^2 + x^3 z, xy - 1 \rangle \subseteq \mathbb{F}_4[x, y, x]$ være et ideal med den graduerede reverse leksikografiske ordning. Radikalet til I findes ved følgende kommandoer*

```
> LIB "primdec.lib";
> ring R=4,(x,y,z),dp;
> ideal I=x2+x3z,xy-1;
> I;
I[1]=x3z+x2
I[2]=xy-1
> ideal pr=radical(I);
> pr;
pr[1]=y+z
pr[2]=xz+1
```

Heraf ses, at radikalet til I er frembragt af polynomierne $pr[1] = y + z$ og $pr[2] = xz + 1$, hvorfor $\sqrt{I} = \langle y + z, xz + 1\rangle$.

Som tidligere nævnt var målet med dette afsnit at kunne bevæge sig mellem den geometriske verden af affine varieteter og den algebraiske verden af idealer. Derfor søgtes en beskrivelse af afbildingerne $\mathbf{I}$ og $\mathbf{V}$. Det blev også vist i afsnit 4.7, at der ej var tale om bijektive afbildinger. Til gengæld med indførslen af radikale idealer bliver de korresponderende afbildinger bijektive. Resultaterne er samlet i følgende sætning.

Sætning 4.16 (Ideal- og affin varietet korrespondencen)**.** *Lad k være et arbitrært legeme.*

(i) Afbildingerne

$$\textit{affine varieteter} \xrightarrow{\boldsymbol{I}} \textit{idealer}$$
$$\textit{idealer} \xrightarrow{\boldsymbol{V}} \textit{affine varieteter}$$

er inklusionsreversible, med hvilket der menes, at $I_1 \subseteq I_2$ er idealer, når $\boldsymbol{V}(I_1) \supseteq \boldsymbol{V}(I_2)$, og similært $V_1 \subseteq V_2$ er affine varieteter såfremt at $\boldsymbol{I}(V_1) \supseteq \boldsymbol{I}(V_2)$. Endvidere haves for alle varieteter V, at $\boldsymbol{V}(\boldsymbol{I}(V)) = V$, hvorved $\boldsymbol{I}$ altid er one-to-one.

(ii) Hvis k er algebraisk lukket, og radikale idealer betragtes, da er afbildingerne

$$\textit{affine varieteter} \xrightarrow{\boldsymbol{I}} \textit{radikale idealer}$$
$$\textit{radikale idealer} \xrightarrow{\boldsymbol{V}} \textit{affine varieteter}$$

hinandens inverse, ie. bijektive.

Bevis. (i) Det overlades til læseren at bevise at afbildingerne er inklusionsreversible. Tilbage er der under dette punkt at vise at der for en subvarietet $V = \mathbf{V}(f_1, \ldots, f_s)$ til k^n varieteter gælder, at $\mathbf{V}(\mathbf{I}(V)) = V$. Tag $f \in \mathbf{I}(V)$, så forsvinder f på V. Pr. definition af $\mathbf{V}$ følger det direkte, at $V \subseteq \mathbf{V}(\mathbf{I}(V))$. Bemærk samtidigt, at $f_1, \ldots, f_s \in \mathbf{I}(V)$ jvf. definitionen af $\mathbf{I}$. Deraf haves, at $\langle f_1, \ldots, f_s\rangle \subseteq \mathbf{I}(V)$. Da $\mathbf{V}$ er inklusionsreversibel, så følger det, at $\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_1, \ldots, f_s\rangle) = V$. Det vil sige, at ligningen er vist og $\mathbf{I}$ er one-to-one.

(ii) Fra korollar 4.5 haves at $\mathbf{I}(V)$ er et radikalt ideal. Derfor vil $\mathbf{I}$ blive betragtes som en funktion der afbilder affine varieteter over i radikale idealer. Det vides fra (i), at for alle varieteter V gælder, at $\mathbf{V}(\mathbf{I}(V)) = V$. Det skal vises, at når I er et radikalt ideal, så $\mathbf{I}(\mathbf{V}(I)) = V$. Ifølge

Hilberts Nullstellensatz, sætning 4.14 haves, at $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$, og da I er radikalt, så giver korollar 4.6, at $I = \sqrt{I}$. Det vil sige, at $\mathbf{V}$ og $\mathbf{I}$ er hinandens inverse.

□

Ovenstående sætning gør det bl.a. muligt at oversætte ethvert problem, der har med affine varieteter at gøre, til et problem der har med radikale idealer at gøre. Dette bliver der ikke brug for i arbejdet med netværkskodning, da der her ikke arbejdes med algebraisk lukkede legemer. Afsnittet og resultaterne er blot med for at vise, hvordan den ideelle situation ville udforme sig. Sætningen udtaler sig dog også om forholdet mellem idealer og affine varieteter, og det ses, at der medtages flere løsninger, når legemet ikke er algebraisk lukket. Pointen er dog, at der i det ovenstående er blevet etableret en forbindelse imellem affine varieteter og idealer. Da idealer er algebraiske objekter giver det også mening at tillægge regneoperationer for hvert par af idealer. Regneoperationerne, som her vil blive nævnt, er summation, multiplikation og fællesmængden for to idealer.

Definition 4.24. *Lad I og J være idealer over $k[x_1, \ldots, x_n]$. Da er summen for de to idealer $I+J$ defineret ved*

$$I + J = \{f + g \mid f \in I \text{ og } g \in J\}.$$

Produktet af to idealer $I \cdot J$ er defineret ved

$$I \cdot J = \{f_1 g_1 + \cdots + f_r g_r \mid f_1, \ldots f_r \in I, g_1, \ldots, g_r \in J \text{ og } r \in \mathbb{Z}_{\geq 0}\}.$$

Fællesmængden for de to idealer $I \cap J$ er defineret ved

$$I \cap J = \{f_1, \ldots, f_s \mid f_1, \ldots, f_s \in I, J\}.$$

Det kan vises, at både summen af to idealer, produktet og fællesmængden også er idealer. Beviserne kan findes i kap. 4, § 3 i [2008 Cox, Little & O´Shea]. Operationerne kan endvidere overføres til verdenen af affine varieteter, hvilket samlet set resulterer i nedenstående sætning.

Sætning 4.17. *Lad I og J være idealer over $k[x_1, \ldots, x_n]$. Da gælder, at*

1. $\boldsymbol{V}(I + J) = \boldsymbol{V}(I) \cap \boldsymbol{V}(J)$
2. $\boldsymbol{V}(I \cdot J) = \boldsymbol{V}(I) \cup \boldsymbol{V}(J)$
3. $\boldsymbol{V}(I \cap J) = \boldsymbol{V}(I) \cup \boldsymbol{V}(J)$

Det bemærkes, at den affine varietet til et produkt af to idealer, faktisk giver samme resultat som den affine varietet til fællesmængden for de samme to idealer. Baggrunden for alligevel at indføre begge operationer har med radikale idealer at gøre. Fællesmængden for to radikale idealer giver et nyt radikalt ideal, men med produktet forholder det sig anderledes. Produktet giver ikke nødvendigvis et nyt radikalt ideal. I det følgende afsnit undersøges affine varieteters indbyrdes forbindelse.

4.9 Affine varieteters indbyrdes korrespondence

Afsnittet omhandler en særlig type afbilding imellem affine varieteter, nemlig polynomielle afbildinger. Det vil blive vist, at afbildingerne har særlige egenskaber, som gør dem givtige ift. til teorien om netværkskodning. Afsnittet er skrevet ud fra [2008 Cox, Little & O´Shea].

Vi vil initiere afsnittet med en definition af polynomielle afbildinger.

Definition 4.25. *Lad $V \subseteq k^m$, $W \subseteq k^n$ være affine varieteter. En funktion $\phi : V \to W$ kaldes for en polynomiel afbilding, hvis der findes polynomier $f_1, \ldots, f_s \in k[x_1, \ldots, x_m]$, sådan at*

$$\phi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_s(a_1, \ldots, a_m)) \tag{4.28}$$

for alle $(a_1, \ldots, a_m) \in V$. Hermed siges s-tuplen $(f_1, \ldots, f_s) \in (k[x_1, \ldots, x_m])^n$ at være repræsentationen af ϕ.

Med ovenstående definition skelnes imellem polynomielle repræsentanter og polynomielle afbildinger (funktioner). Hvis i ovenstående definition, at ϕ afbilder over i $W = k$, k et legeme, så bliver ϕ en funktion, der afbilder polynomier over i skalarer. Det gode ved at undersøge afbildinger fra V til k, er, at der samtidig hentes informationer om afbildinger fra V til k^n. Dette skyldes, at en afbilding $\phi : V \to k^n$ er konstrueret ud fra n polynomielle funktioner $\phi : V \to k$. Det bemærkes endvidere, at ovenstående definition siger, at en afbilding $\phi : V \to k$ er polynomiel, hvis der findes polynomium $f \in k[x_1, \ldots, x_m]$, som repræsenterer ϕ. Det er ikke så svært at finde repræsentanterne. Det svære er at finde entydige repræsenterende polynomier. I det følgende eksempel vises, hvordan polynomier kan repræsentere den samme funktion.

Eksempel 4.19. *Lad V være varieteten $\boldsymbol{V}(y^2 - x) \subseteq \mathbb{R}^2$. Polynomiet $f = x^2 + y^4$ repræsenterer en polynomiel funktion $\phi : V \to \mathbb{R}$. Det ses dog, at polynomierne $g = x^2 + y^4 + (y^2 - x)$ og $l = x^3 + y^3 + A(x, y)(y - x^2)$ for alle $A \in \mathbb{F}[x, y],$, har den samme egenskab. Disse er også repræsentanter for en afbilding fra V til $\mathbb{R}$.*

Der er altså brug for en metode til at afgøre, hvornår to polynomier er repræsentanter for den samme afbilding. Følgende sætning giver afhjælper dette problem.

Sætning 4.18. *Lad $V \subseteq k^m$ være en affin varietet. Da gælder, at*

1. *$f, g \in k[x_1, \ldots, x_m]$ repræsenterer den samme polynomielle funktion på V hvis og kun hvis $f - g \in \boldsymbol{I}(V)$.*
2. *Tuplerne $(f_1, \ldots, f_n)$ og $(g_1, \ldots, g_n)$ repræsenterer den samme polynomielle afbilding fra V til k^n hvis og kun hvis $f_i - g_i \in \boldsymbol{I}(V)$, $1 \leq i \leq n$.*

Bevis. Først vises (i). Det ses, at $h = f - g \in \mathbf{I}(V)$, hvis og kun hvis der for alle $p = (a_1, \ldots, a_m) \in V$ gælder, at $h(p) = 0$. Dette gælder til gengæld hvis og kun hvis, at $f(p) - g(p) = 0$, hvorfor de to polynomier, f og g, repræsenterer den samme funktion på V. Antag nu omvendt at f og g repræsenter den samme funktion på V. For enhvert $p \in V$ haves da, at $f(p) - g(p) = 0$. Ergo må $f - g \in \mathbf{I}(V)$. Punktet (ii) følger direkte af (i), fordi alle polynomiumsafbildinger har polynomiumsfunktioner som komponenter. □

Sætningen viser, at der er en en-til-en korrespondence imellem polynomier i $k[x_1, \ldots, x_m]$ og polynomielle funktioner, så længe at $\mathbf{I}(V) = \{0\}$. Dette giver også, at man kan arbejde med polynomielle afbildinger på affine varieteter på to måder. Enten kan man samle alle de polynomier, som repræsenterer den samme funktion på V, i en klasse, og betragte klassen som et hele. Eller også kan man tage det simpleste polynomium, som repræsenterer alle funktioner på V, og arbejde med det, som en repræsentation for de øvrige. Vi vil se lidt nærmere på den første mulighed, men først gøres endnu en iagttagelse vedrørerende polynomielle funktioner.

Definition 4.26. *Samlingen af alle polynomielle funktioner $\phi : V \to k$ noteres som $k[V]$.*

Da k er et legeme, giver det mening at definere sum og multiplikation for funktioner $\phi, \psi : V \to k$. For hvert $p \in V$ defineres:

$$(\phi + \psi)(p) = \phi(p) + \psi(p)$$
$$(\phi \cdot \psi)(p) = \phi(p) \cdot \psi(p).$$

Hvis polynomier på affin varieteter anskues ved at tage udvælge et polynomium på V, som repræsenterer alle funktioner på V, så giver det mening at vælge repræsentative polynomier f, g for ϕ, ψ. Dette giver, at funktionssummen og multiplikationssummen istedet kan repræsenteres ved $f + g$ og $f \cdot g$. Ergo har mængden $k[V]$ definerede summer og produkt operationer, som er nedarvet fra $k[x_1, \ldots, x_m]$. Mængden $k[V]$ opfylder dermed betingelserne for en kommutativ ring (se side 112 i [2003 Lauritzen]).

En anden grund til at mængden $k[V]$ er lidt speciel skyldes, at den tilhører en særlig klasse af kommutative ringe. Dette vil blive undersøgt nærmere i det efterfølgende afsnit.

4.10 Polynomielle kvotientringe

Mængden $k[V]$, som blev defineret i forrige afsnit, er et specialtilfælde af det der siges at være kvotienten til $k[x_1, \ldots, x_n]$ modulo et ideal I. I samme afsnit blev der nævnt to muligheder ift. arbejdet med polynomier på affine varieteter. Dette afsnit handler om den første af de to muligheder, hvor idéen var at samle alle de polynomier, som repræsenterer den samme funktion på V i en klasse. Til at starte med indføres følgende sprogbrug:

Definition 4.27. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal, og lad $f, g \in k[x_1, \ldots, x_n]$. Polynomierne f, g siges at være kongruente modulo I, hvilket skrives*

$$f \equiv g \mod I,$$

såfremt at $f - g \in I$.

Eksempel 4.20. *Tag f.eks. idealet $I = \langle x, y^2 \rangle \subseteq k[x, y]$, og polynomierne $f = x^2y^3 - x + y^2$ og $g = xy^2 - 2x$ med den leksikografiske ordning, hvor $x > y$. Da gælder, at*

$$f \equiv g \mod I.$$

Dette ses af, at

$$\begin{aligned} f - g &= x^2y^3 - xy^2 + x + y^2 \\ &= y^2(x^2y + 1) - x(y^2 - 1) \in I. \end{aligned}$$

Ergo er f og g kongruente modulo I. Med Singular kan det også tjekkes om $f-g$ ligger i I. Det huskes, at $f-g$ ligger i I, såfremt at resten ved division med et Gröbnerbasis for I er nul(sætning 4.10):

```
> ring R=5,(x,y,z),lp;
> poly f=x2y3-x+y2;
> poly g=xy2-2x;
> ideal I=x,y2;
> reduce(f-g,std(I));
0
```

Eksemplet giver mening til kongruensrelationen og viser, at den eksisterer. Men hvad der er endnu bedre, så viser det sig, at kongruensrelationen samtidigt er en ækvivalensrelation.

Sætning 4.19. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal. Relationen defineret i 4.27 er en ækvivalensrelation på $k[x_1, \ldots, x_n]$.*

Bevis. For at kongruensen modulo I er en ækvivalensrelation, er der tre ting der skal vises. Relationen skal være både refleksiv, symmetrisk og transitiv. Det er trivielt opfyldt, at for alle $f \in k[x_1, \ldots, x_n]$ gælder, at $f - f = 0 \in I$, hvorfor relationen er refleksiv. For at vise symmetrien antag, at $f \equiv g \mathrm{mod} I$. Det betyder, at $g - f = (-1)(f - g) \in I$. Heraf ses, at $g \equiv f \mod I$ også gælder. Angående transitiviteten, lad nu $f \equiv g \mod I$ og $g \equiv h \mod I$ være sande. Så gælder, at $f - g$ og $g - h$ begge tilhører I. Da I er lukket under addition så $f - h = (f - g) + (g - h) \in I$, hvilket medfører, at $f \equiv h \mod I$. □

Det bemærkes, at en ækvivalensrelation på en mængde S inddeler S i disjunkte mængder. De disjunkte mængder kaldes for ækvivalensklasser. Det vil sige, at for ethvert $f \in k[x_1, \ldots, x_n]$ er ækvivalensklassen til f givet ved

$$[f] = \{g \in k[x_1, \ldots, x_n] \mid g \equiv f \mod I\},$$

hvor I er et ideal over $k[x_1, \ldots, x_n]$. Det ses, at denne definition gælder for alle idealer, så hvis $I = \mathbf{I}(V)$, som jo ifølge lemma 4.2 er et ideal, må der jvf. sætning 4.18 gælde, at $f \equiv g \mod \mathbf{I}(V)$ hvis og kun hvis f og g definerer den samme funktion på V. Som nævnt sidst i afsnit 4.9 kunne man arbejde med polynomielle afbildinger på affine varieteter på to måder, og den ene af disse var ved at samle alle polynomier, som repræsenterer den samme funktion på V i en klasse, og det er, hvad der nu er blevet gjort. At man frit kan bevæge sig mellem verdenen af affine varieteter og ækvivalensklasser til kongruensrelationen modulo $\mathbf{I}(V)$ er formuleret i den følgende sætning:

Sætning 4.20. *Funktionerne $\phi : V \to k$ er i én-til-én korrespondence med polynomielle ækvivalensklasser underlagt kongruens modulo $\boldsymbol{I}(V)$.*

Ækvivalensklasserne kan anvendes til at definere en anden type kommutativ ring. At ringen er kommutativ, og den i det hele taget er en ring, godtgøres i sætningerne, som følger definitionen under.

Definition 4.28. *Kvotienten til $k[x_1, \ldots, x_n]$ modulo I, hvilket skrives $k[x_1, \ldots, x_n]/I$, er mængden af ækvivalensklasser for kongruens modulo I:*

$$k[x_1, \ldots, x_n]/I = \{[f] \mid f \in k[x_1, \ldots, x_n]\}.$$

I afsnit 4.11 behandles elementerne tilhørende kvotientringen nærmere. Her gives først et simpelt eksempel på en kvotientring.

Eksempel 4.21. *Lad $k = \mathbb{R}$, $n = 1$ og $I = \langle x^2 - 2 \rangle \subseteq \mathbb{R}[x]$ med den leksikografiske ordning. Da er det muligt at beskrive alle de tilhørende ækvivalensklasser kongruens modulo I. Ifølge divisionsalgoritmen sætning 4.4 kan alle $f \in \mathbb{R}[x]$ skrives som $f = q \cdot (x^2 - 2) + r$, hvor $r = ax + b$, $a, b \in \mathbb{R}$, og $q \in \mathbb{R}[x]$. Ifølge definitionerne 4.28 og 4.27, da $f - r = q(x^2 - 2) \in I$, gælder, at $f \equiv r \mod I$. Det vil sige, at ethvert element i $\mathbb{R}[x]$ tilhører enten $[ax + b]$ eller $\mathbb{R}[x]/I = \{[ax + b] \mid a, b \in \mathbb{R}\}$. Denne måde at beskrive alle elementerne i en kvotientring på, vil blive generaliseret i det næste afsnit.*

Det ønskes, at definere addition og multiplikation inden for denne nye kvotientklasse. En naturlig måde at definere operationerne på, fordi $k[x_1, \ldots, x_n]$ er en ring, er for $[f], [g] \in k[x_1, \ldots, x_n]/I$ at lade

$$[f] + [g] = [f + g] \tag{4.29}$$
$$[f] \cdot [g] = [f \cdot g]. \tag{4.30}$$

Det er dog ikke sikkert, at operationerne er veldefineret, så det skal vises, at for $f' \in [f]$ og $g' \in [g]$, så er $[f' + g'] = [f + g]$ og $[f' \cdot g'] = [f \cdot g]$. Dette stadfæstes i nedenstående sætning.

Sætning 4.21. *Operationerne givet i* (4.29) *og i* (4.30) *er veldefinerede.*

Bevis. Først vises at addition er en veldefineret operation. Tag $f' \in [f]$ og $g' \in [g]$, så $f' = f + a$ og $g' = g + b$, hvor $a, b \in I$. Da gælder, at

$$f' + g' = (f + a) + (g + b) = (f + g) + (a + b).$$

Da I er et ideal, så $a + b \in I$, hvorfor $f' + g' \equiv f + g \mod I$. Dette er det samme som, at $[f' + g'] = [f + g]$. Samme fremgangsmetode benyttes til at vise at også multiplikation er en veldefineret operation. Der fås, at

$$f' \cdot g' = (f + a) \cdot (g + b) = fg + ag + fb + ab.$$

Da både a og b ligger i I, så må $ag + fb + ab$ også ligge i I, for I er et ideal. Det vil sige, at $f' \cdot g' \equiv f \cdot g$, hvilket igen er det samme som, at $[f' \cdot g'] = [f \cdot g]$. □

Eksempel 4.22. *Operationerne er ret ligetil at anvende. Alligevel gives dog et lille eksempel på anvendelsen heraf. Betragt de to ækvivalensklasser $[f] = [x + y]$ og $[g] = [x - y]$ med $f, g \in k[x, y]$. Da gælder, at*

$$[f] + [g] = [2x]$$
$$[f] \cdot [g] = [x^2 - y^2].$$

Det, at der nu findes veldefinerede operationer, addition og multiplikation på kvotientringen, gør det nemt at vise, at selvsamme kvotientring faktisk er en kommutativ ring. Det udmønter sig i nedenstående sætning.

Sætning 4.22. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal. Kvotientringen $k[x_1, \ldots, x_n]/I$ er en kommutativ ring underlagt operationerne defineret ved* (4.29) *og i* (4.30).

Bevis. Der er en række af betingelser, der skal tjekkes, når det skal afgøres om $k[x_1, \ldots, x_n]/I$ er en kommutativ ring, da en ring for det første er en abelsk gruppe, og derfor skal opfylde bl.a. den associative lov (se side 112 og 124 i [2003 Lauritzen]). Det er ret nemt at vise, at alle betingelser er overholdt, så her bevises blot, at den associative lov er overholdt for summer i $k[x_1, \ldots, x_n]/I$. Hvis $[f], [g], [h] \in k[x_1, \ldots, x_n]/I$, så

$$\begin{aligned}([f] + [g]) + [h] &= [f + g] + [h] \\ &= [(f + g) + h] \\ &= [f + (g + h)] \\ &= [f] + [g + h] \\ &= [f] + ([g] + [h]).\end{aligned}$$

Den associative lov er altså overholdt i forhold til (4.29). Det er samme fremgangsmåde, når den associative lov skal vises med komnpositionen givet i (4.30). □

Som der blev nævnt i starten af afsnittet er der en relation imellem $k[V]$ og $k[x_1, \ldots, x_n]/I$. Der er tale om, at de til en vis grad er ens.

Sætning 4.23. *Én-til-én korrespondencen imellem elementer i $k[V]$ og elementer i $k[x_1, \ldots, x_n]/\boldsymbol{I}(V)$ fra sætning 4.20 bibevarer summer og produkter.*

Bevis. Lad $\Phi : k[x_1, \ldots, x_n]/\mathbf{I}(V) \to k[V]$ være en afbilding defineret ved $\Phi([f]) = \phi$, hvor ϕ er den polynomielle funktion repræsenteret ved f. Da alle elementer i $k[V]$ da er repræsenteret ved ét polynomium, så er Φ en surjektiv afbilding. Antag, at $\Phi([f]) = \Phi([g])$. Ifølge sætning 4.20, så er $f \equiv g \mod \mathbf{I}(V)$. Dette giver, at $[f] = [g]$ i $k[x_1, \ldots, x_n]/\mathbf{I}(V)$, så Φ er også injektiv.

Lad nu $[f], [g] \in k[x_1, \ldots, x_n]/\mathbf{I}(V)$, hvorved $\Phi([f] + [g]) = \Phi([f + g])$ ifølge definition 4.28. Hvis f repræsenterer den polynomielle funktion ϕ og g repræsenterer den polynomielle funktion ψ, så er $\phi + \psi$ repræsenteret ved $f + g$. Dette giver, at

$$\Phi([f + g]) = \phi + \psi = \Phi([f]) + \Phi([g]),$$

hvorfor ϕ bibevarer summerne. Ligeledes ses, at da

$$\Phi([f] \cdot [g]) = \Phi([f \cdot g]) = \phi \cdot \psi = \Phi([f]) \cdot \Phi([g]).$$

□

Det lader altså til, at hvis der kan frembringes repræsentanter for ækvivalensklasser med kongruens modulo I, så kan summer og produkter for elementer i en kvotientring udregnes. I det følgende afsnit vil vi se nærmere på, hvordan dette gøres.

4.11 Fodaftryksgrænsen

I det forrige afsnit introduceredes kvotientringen $k[x_1, \ldots, x_n]/I$ som en samling af polynomier, $f \in k[x_1, \ldots, x_n]$, som alle repræsenterer den samme funktion på en affin varietet V. Der blev endvidere givet mening til summation og multiplikation i kvotientringen. I dette afsnit udforskes

regneoperationerne nærmere, og der vil blive givet en specifik metode til udregning af både summer og produkter. Som et biprodukt, men i virkeligheden et af hovedresultaterne ift. netværkskodning, bevises fodaftryksgrænsen, som er en grænse for, hvor mange nulpunkter, der højst kan være i V. Fodaftryksgrænsen bevises først for idealer over $\mathbb{C}[x_1, \ldots, x_n]$, som er den form, man i bibliografien normalt ser fodaftryksgrænsen i, men med udgangspunkt i denne sætning overføres det til situationen, hvor et ideal over $\mathbb{F}_q[x_1, \ldots, x_n]$ haves. Dette gøres for at kunne relatere resultatet til netværkskodning. Først defineres dog, hvad der forstås som fodaftrykket til et ideal.

Definition 4.29 (Fodaftryk)**.** *Givet et ideal $I \subseteq k[x_1, \ldots, x_n]$, lad da $\langle LT(I)\rangle$ være idealet frembragt af de førende led fra I i forhold til en valgt monomiel ordning $>$. Fodaftrykket $\Delta(I)$ består da af alle de monomier, som ligger i komplementærmængden til $\langle LT(I)\rangle$.*

I den næste sætning vises det, at alle elementerne i $k[x_1, \ldots, x_n]/I$ er linearkombinationer af fodaftrykket, og at monomierne i fodaftrykket er lineært uafhængige. Dermed kan monomierne anvendes som basis for kvotientringen.

Sætning 4.24. *Lad $>$ være en monomiel ordning på $k[x_1, \ldots, x_n]$ og $I \subseteq k[x_1, \ldots, x_n]$ være et ideal.*

1. *Ethvert $f \in k[x_1, \ldots, x_n]$ er kongruent modulo I til et entydigt polynomium r, som er en k-linearkombination af monomier i fodaftrykket til $\langle LT(I)\rangle$.*
2. *Elementerne i $\{x^\alpha \mid x^a \notin \langle LT(I)\rangle\}$ er lineært uafhængige modulo I. Med andre ord så hvis*

$$\sum_\alpha c_\alpha x^\alpha \equiv 0 \mod I,$$

hvor x^α alle ligger i komplementet til $\langle LT(I)\rangle$, gælder, at $c_\alpha = 0$ for alle α.

Bevis. Først vises (i). Lad G være et Gröbnerbasis for I og $f \in k[x_1, \ldots, x_n]$. Ifølge divisionsalgoritmen, sætning 4.4, så opfylder resten $r = \overline{f}^G$, at $f = q + r$, hvor $q \in I$. Det vil sige, at $f - r = q \in I$, hvorfor at $f \equiv r \mod I$. Divisionsalgoritmen giver ligeledes, at r er en k-linearkombination af monomier $x^\alpha \notin \langle LT(I)\rangle$. Resten r er envidere enydigt bestemt jvf. sætning 4.10 og sætningen giver også at intet led i resten er deleligt med noget $LT(g_i)$ for $g_i \in G$.

Fremgangsmetoden for at vise (ii) er den samme som i beviset for sætning 4.10(ii). Antag, at $\sum_\alpha c_\alpha x^\alpha \equiv 0 \mod I$, hvor $x^\alpha \in \Delta(I)$. Dermed gælder, at $x^\alpha \notin \langle LT(I)\rangle$, hvilket medfører, at $\sum_\alpha c_\alpha x^\alpha \in I$. Antag modsætningsvist $\sum_\alpha c_\alpha x^\alpha \neq 0$, så $LT\left(\sum_\alpha c_\alpha x^\alpha\right) \in \langle LT(I)\rangle$. Pr. antagelse tilhørte ingen af monomierne x^α idealet $\langle LT(I)\rangle$, så der haves en modstrid. Derfor må $\sum_\alpha c_\alpha x^\alpha \neq 0$ for alle x, hvilket kun kan lade sig gøre, når $c_\alpha = 0$ for alle α. □

Ifølge ovenstående sætning har alle polynomier i $k[x_1, \ldots, x_n]$ en repræsentant i kvotientringen, udtrykt ved rest der fremkommer, når polynomierne divideres med et Gröbnerbasis for I. Polynomiet er en linearkombination af de lineært uafhængige monomier i fodaftrykket, hvorfor $\Delta(I)$ er basis for kvotientringen $k[x_1, \ldots, x_n]/I$.

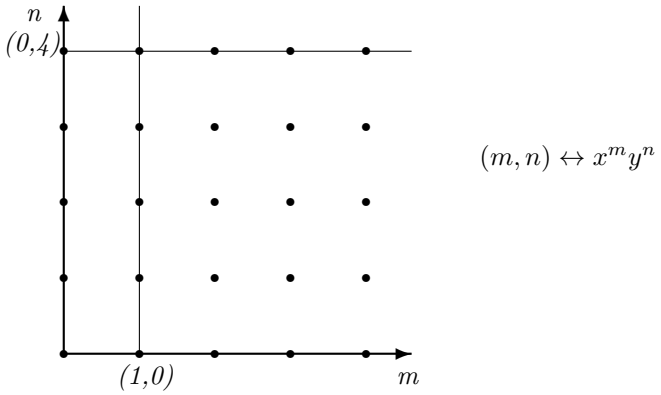
Eksempel 4.23. *Betragt idealet $I = \langle x^2y^3 - 3x, y + xy\rangle \subseteq \mathbb{F}_5[x, y]$ med den leksikografiske ordning, hvor $x > y$. Ved hjælp af Singular og følgende kommando*

```
> ring R=5,(x,y),lp;
> ideal I=x2y3-3x,y+xy;
> std(I);
_[1]=y4-2y
_[2]=x-2y3
```

ses, at $G = \{y^4 - 2y, x - 2y^3\}$ *er et Gröbnerbasis for* I*. Dette betyder, at vi kan udtrykke* $\langle LT(I)\rangle$ *som* $\langle y^4, x\rangle$*. Eksponenterne kan derved udtrykkes i et diagram i* $\mathbb{Z}^2_{\geq 0}$ *med vektorerne* $\alpha(1) = (0,4)$ *og* $\alpha(2) = (1,0)$*. Vektorerne siges at være eksponentvektorer til frembringerne for* $\langle LT(I)\rangle$*. Dermed må mængden*

$$((0,4) + \mathbb{Z}^2_{\geq 0}) \cup ((1,0) + \mathbb{Z}^2_{\geq 0})$$

være eksponenterne til alle monomier i $\langle LT(I)\rangle$*. Alle monomier i* $\langle LT(I)\rangle$ *repræsenteres da i følgende diagram:*



Givet et hvilket som helst $f \in \mathbb{F}_5[x_1, \ldots, x_n]$*, så følger det af sætning 4.24, at resten* $\overline{f}^G$ *vil være en* $\mathbb{F}_5$*-linearkombination af monomierne* $1, y, y^2, y^3$*. Det er her vigtigt at bemærke, var der fra start valgt en anden monomiel ordning, er det ikke sikkert, at linearkombinationen vil bestå af samme monomier.*

I eksemplet var fodaftrykekt en endelig mængde. Det er dog ikke altid tilfældet. Planen er nu at anvende sætning 4.24 til at beskrive den algebraiske struktur for kvotientringen. Inden dette er det nødvendigt at gøre sig bekendt med begrebet isomorfi, som er et udtryk, der bruges om sammenhængen mellem elementer i to algebraiske struktur.

Definition 4.30. *Lad* R, S *være kommutative ringe.*

(i) En afbilding $\phi : R \to S$ *siges at være en isomorfi, såfremt at følgende tre betingelser er opfyldt:*

(a) Afbildingen ϕ *bibevarer summation:* $\phi(r + r') = \phi(r) + \phi(r')$ *for alle* $r, r' \in R$*.*

(b) Afbildingen ϕ *bibevarer multiplikation:* $\phi(r \cdot r') = \phi(r) \cdot \phi(r')$ *for alle* $r, r' \in R$*.*

(c) Afbildingen ϕ *er bijektiv.*

(ii) To ringe R, S *er isomorfe, hvis der findes en ring isomorfi* $\phi : R \to S$*. Dette skrives* $R \cong S$*.*

(iii) En afbilding $\phi : R \to S$ siges at være en ring homomorfi, hvis ϕ opfylder (a) og (b) i (i) men ikke nødvendigvis (c), og hvis ϕ afbilder $1 \in R$ over i $1 \in S$.

Det bemærkes, at ifølge sætning 4.23 er $k[V]$ og $k[x_1, \ldots, x_n]/I(V)$ isomorfe. Dette er dog ikke det samme som, at $k[V]$ og $k[x_1, \ldots, x_n]/I$ for ethvert ideal I er isomorfe, hvilket de ikke nødvendigvis er. Den følgende sætning udtaler sig mere specifikt om elementerne i $k[x_1, \ldots, x_n]/I$.

Sætning 4.25. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal. Da gælder, at kvotientringen $k[x_1, \ldots, x_n]/I$ som vektorrum er isomorf med $S = Span(x^\alpha \mid x^\alpha \notin \langle LT(I)\rangle)$.*

Bevis. Ifølge definition 4.30 hvis $k[x_1, \ldots, x_n]/I$ skal være isomorf med S, så skal afbildingen $\Phi : k[x_1, \ldots, x_n]/I \to S$, defineret ved $\Phi([f]) = \overline{f}^G$, være både bijektiv og den skal bevare additions- og multiplikationsoperationerne fra kvotientringen. At afbildingen er bijektiv følger direkte af 4.24, så vi mangler blot at vise, at operationerne fra kvotientringen er velbevaret. Først betragtes summation i kvotientringen. Tag $[f], [g] \in k[x_1, \ldots, x_n]/I$, for et ideal $I \subseteq k[x_1, \ldots, x_n]$. Ifølge sætning 4.24 så

$$\overline{f}^G = \sum_\alpha c_\alpha x^\alpha \qquad \text{og} \qquad \overline{g}^G = \sum_\alpha d_\alpha x^\alpha,$$

hvor der summeres over de α'er, hvor $x^\alpha \notin \langle LT(I)\rangle$. Idet at $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$ fås, at

$$\begin{aligned}\overline{f+g}^G &= \sum_\alpha c_\alpha x^\alpha + \sum_\alpha d_\alpha x^\alpha \\ &= \sum_\alpha (c_\alpha + d_\alpha) x^\alpha,\end{aligned}$$

hvor der summeres over de α'er, hvor $x^\alpha \notin \langle LT(I)\rangle$. Heraf ses, at addition i $k[x_1, \ldots, x_n]/I$ er ligedan med addition af vektorer i k-rummet $S = \text{Span}(x^\alpha \mid x^\alpha \notin \langle LT(I)\rangle)$.

For at vise at multiplikationsoperationerne også overføres, tag $c \in k$. Da gælder, at $\overline{c \cdot f}^G = c \cdot \overline{f}^G$, hvorfor

$$\begin{aligned}\overline{c \cdot f}^G &= c \cdot \sum_\alpha c_\alpha x^\alpha \\ &= \sum_\alpha c c_\alpha x^\alpha,\end{aligned}$$

hvor der igen summeres over de α'er, hvor $x^\alpha \notin \langle LT(I)\rangle$. Ergo svarer multiplikation med en konstant i kvotientringen til skalarmultiplikatio i S. Da regneoperationerne bibevares ved Φ, så er $k[x_1, \ldots, x_n]/I$ isomorf med S. □

Mht. det direkte produkt af to ækvivalensklasser, så skal man være lidt opmærksom. Hvorfor vil blive illustreret i det følgende eksempel.

Eksempel 4.24. *Lad $I = \langle x^2y^3 - 3x, y + xy\rangle \subseteq \mathbb{F}_5[x, y]$ med den leksikografiske ordning, hvor $x > y$, være et ideal. I eksempel 4.23 så vi, hvordan Singular kunne anvendes til at finde Gröbnerbasen $G = \{y^4 - 2y, x - 2y^3\}$, hvilket gav, at $\langle LT(I)\rangle = \langle y^4, x\rangle$. Dette gav et basis for vektorrummet bestående af resterne modulo I udtrykt som $\{1, y, y^2, y^3\}$. Det ses, at funktionerne $f = y + y^2$*

og $g = y^3 - 1$ begge ligger i $\mathbb{F}_5[x, y]$. Antag at repræsenativet for udregning af produkter mellem ækvivalensklasserne $[f]$ og $[g]$ er det direkte produkt givet ved

$$f \cdot g = y^5 + y^4 - y^2 - y. \tag{4.31}$$

Det ses, at monomiet y^4 er indeholdt i $\langle LT(I)\rangle$. Det direkte produkt kan derfor ikke være repræsentativ i sig selv. For at undgå problemet divideres udtrykket i (4.31) med G. Vi får Singular til at bestemme resultatet for os:

```
> ring R=5,(x,y),lp;
> ideal I=x2y3-3x,y+xy;
> reduce(y5+y4-y2-y,std(I));
y2+y
```

Singular giver altså, at $\overline{f \cdot g}^G = y^2 + y$, hvor ingen af monomierne nu er indeholdt i $\langle LT(I)\rangle$.

Sammenlignes resultatet fra sætning 4.25 med ovenstående eksempel haves dermed en måde at repræsentere summer og produkter af ækvivalensklasser i kvotientringen $k[x_1, \ldots, x_n]/I$.

Sætning 4.26. *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal, og lad G være et Gröbnerbasis for I med en tillagt monomiel ordning. Hvis hvert $[f] \in k[x_1, \ldots, x_n]/I$ repræsenteres ved $\overline{f}^G$ i $S = Span(x^\alpha \mid x^\alpha \notin \langle LT(I)\rangle)$, da gælder, at*

(i) Summen $[f] + [g]$ kan repræsenteres ved $\overline{f} + \overline{g}$.

(ii) Produktet $[f] \cdot [g]$ kan repræsenteres ved $\overline{\overline{f} + \overline{g}}^G$.

Målet er nu at kunne afgøre hvornår en affin varietet V i et endeligt legeme $\mathbb{F}_q$ har endelig dimension og i så fald give et bud på, hvor mange elementer der er indeholdt i V. I kap. 5, §3i [2008 Cox, Little & O´Shea] gives et kriterium for hvornår en affin varietet på et algebraisk aflukke har endelig dimension. Dette resultat vil her blive korrigeret så det istedet udtaler sig om, hvornår affine varieteter i endelige legemer indeholder et endeligt antal punkter. Først vises sætningen for det algebraiske aflukke.

Sætning 4.27. *Lad $V = \boldsymbol{V}(I)$ være en affin varietet på $\mathbb{C}^n$, og vælg en monomiel ordning til $\mathbb{C}[x_1, \ldots, x_n]$. Følgende udsagn er da ækvivalente:*

(i) Mængden V er endelig.

(ii) For hvert i, $1 \leq i \leq n$, findes et $m_i \geq 0$, sådan at $x_i^{m_i} \in \langle LT(I)\rangle$.

(iii) Lad G være et Gröbnerbasis for I. For hvert i, $1 \leq i \leq n$, findes et $m_i \geq 0$ sådan at $x_i^{m_i} = LM(g_i)$ for $g_i \in G$.

(iv) $\mathbb{C}$-vektorrummet $S = Span(x^\alpha \mid x^\alpha \notin \langle LT(I)\rangle)$ har endelig dimension.

(v) $\mathbb{C}$-vektorrummet $\mathbb{C}[x_1, \ldots, x_n]/I$ er har endelig dimension.

Bevis. Beviset for at (i) medfører (ii) udelades, da dette punkt udgår i den raffinerede udgave af sætningen, hvor et endeligt legeme betragtes fremfor et algebraisk aflukke. Det skal dog nævnes at udsagnet følger ved anvendelse af Hilberts svage basissætning, sætning 4.14. Beviset initieres istedet med at vise, at (ii) medfører (iii). Fra (ii) haves at der findes et $m_i \geq 0$, sådan at $x_i^{m_i} \in \langle LT(I) \rangle$. Idet G er et Gröbnerbasis for I, så gælder, at $\langle LT(I) \rangle = \langle LT(g) \rangle$ for $g \in G$. Ifølge lemma 4.7 findes da et $g_i \in G$ sådan, at $LT(g_i)$ går op i $x_i^{m_i}$. Dette betyder, at $LT(g_i)$ er en potens af x_i, hvorfor (iii) er sand. At (iii) rent faktisk også medfører (ii) ses, ved at gøre det samme bare i modsat rækkefølge.

Det vil nu blive vist at (ii) medfører (iv). Igen haves $x_i^{m_i} \in \langle LT(I) \rangle$ for hvert i. Dette betyder, at monomierne $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, for nogle $\alpha_i \geq m_i$, alle tilhører idealet $\langle LT(I) \rangle$. Modsat vides da, om monomierne i komplementærmængden til $\langle LT(I) \rangle$, at $\alpha_i \leq m_i$, hvoraf det ses, at antallet af monomier i komplementærmængden til højst kan være $m_1 \cdots m_n$.

At (iv) medfører (v) følger direkte af sætning 4.25. Det vil sige, at hvis det kan vises, at (v) medfører (i), så kommer vi hele vejen rundt, og alle udsagn er ækvivalente. Igen da (i) ikke gælder for $\mathbb{C} = k$ eller nærmere bestemt $\mathbb{F}_q$ overlades denne del også til læseren. □

Hvis vi istedet betragter sætningen i forhold til et endeligt legeme fjernes som tidligere nævnt et af de fem kriterier. Beviset køres dog på trods af ændringerne similært med ovenstående bevis, så der ses ingen grund til at gentage dette.

Sætning 4.28. *Lad $V = \boldsymbol{V}(I)$ være en affin varietet på $\mathbb{F}_q^n$, og vælg en monomiel ordning til $\mathbb{F}_q[x_1, \ldots, x_n]$. Følgende udsagn er da ækvivalente:*

(i) For hvert i, $1 \leq i \leq n$, findes et $m_i \geq 0$, sådan at $x_i^{m_i} \in \langle LT(I) \rangle$.

(ii) Lad G være et Gröbnerbasis for I. For hvert i, $1 \leq i \leq n$, findes et $m_i \geq 0$ sådan at $x_i^{m_i} = LM(g_i)$ for $g_i \in G$.

(iii) $\mathbb{F}_q$-vektorrummet $S = Span(x^\alpha \mid x^\alpha \notin \langle LT(I) \rangle)$ har endelig dimension.

(iv) $\mathbb{F}_q$-vektorrummet $\mathbb{F}_q[x_1, \ldots, x_n]/I$ har endelig dimension.

Vi er nu rustet til at kunne give en estimation på hvor mange nulpunkter der er i $V = \mathbf{V}(I)$, I et ideal over et algebraisk aflukke, eller rettere sagt en grænse for hvor mange punkter der højst kan være. Sætningen vises igen for utopien med et algebraisk aflukke og korrigeres, så den relaterer til et endeligt legeme. Som det var tilfældet med sætning 4.27, så er estimationen af antal punkter i V, hvor V ligger i et algebraisk aflukke, et resultat fra kap. 5, §3i [2008 Cox, Little & O´Shea].

Sætning 4.29 (Fodaftryksgrænsen for algebraisk aflukke)**.** *Lad $I \subseteq k[x_1, \ldots, x_n]$ være et ideal, hvor $k = \overline{k}$, så $V = \boldsymbol{V}(I)$ er en endelig mængde. Følgende to påstande er da sande:*

(i) Antallet af punkter i V er mindre end eller lig $dim(k[x_1, \ldots, x_n]/I)$.

(ii) Hvis I samtidigt er et radikalt ideal, så er antallet af punkter i V præcis $dim(k[x_1, \ldots, x_n]/I)$.

Bevis. Først vises, at givet forskellige punkter $p_1, \ldots, p_m \in k^n$, findes et polynomium $f_1 \in k[x_1, \ldots, x_n]$, hvor $f_1(p_1) = 1$ og $f_1(p_2) = \cdots = f_1(p_m) = 0$. Bemærk, at to punkter $a, b \in k^n$ er forskellige, hvis de adskiller sig på mindst én af koordinaterne. Det antages, at de adskiller sig på

koordinat j. Det følger, at funktionen $g = \frac{x_j - b_j}{a_j - b_j}$ opfylder de to kriterier, $g(a) = 1$ og $g(b) = 0$. Da alle p_i'erne er forskellige, så kan denne observation anvendes for hvert par $p_1 \neq p_i$, $i \geq 2$. Derved fås polynomier g_i, hvor $g_i(p_1) = 1$ og $g_i(p_i) = 0$, $i \geq 2$. Det er derfor klart, at polynomiet $p_1 = g_2 \cdots g_m$ opfylder, at $f_1(p_1) = 1$ og $f_1(p_2) = \cdots = f_1(p_m) = 0$. På samme vis konstrueres polynomier $f_2, \ldots, f_m$, som også opfylder de to kriterier.

Antag at $V = \{p_1, \ldots, p_m\}$, hvor p_i, $i = 1, \ldots, m$, alle er forskellige. Da konstrueres polynomier $f_1, \ldots, f_m$ som først i beviset. For at vise (i) er det nu nok at vise, at ækvivalensklasserne $[f_1], \ldots, [f_m] \in k[x_1, \ldots, x_n]/I$ er lineært uafhængige, for så gælder, at

$$m \leq \dim(k[x_1, \ldots, x_n]/I).$$

Antag derfor, at $\sum_{i=1}^{n} a_i[f_i] = [0]$ i $k[x_1, \ldots, x_n]/I$, hvor $a_i \in k$. Sammenlignes med $k[x_1, \ldots, x_n]$ betyder det her, at $g = \sum_{i=1}^{n} a_i f_i \in I$, hvorved at g pr. konstruktion af f_i'erne forsvinder på V for alle punkter $p_1, \ldots, p_m$. For $1 \leq j \leq m$ haves da, at

$$0 = g(p_j) = \sum_{i=1}^{n} a_i f_i(p_j) = o + a_j f_j(p_j) = a_j \cdot 1 = a_j.$$

Heraf ses, at ækvivalensklasserne er lineært uafhængige, og (i) er vist.

Til (ii) antag, at I er et radikalt ideal. Det er nok at vise, at ækvivalensklasserne $[f_1], \ldots, [f_m]$ danner et basis for $k[x_1, \ldots, x_n]/I$. Det gør de, hvis de er lineært uafhængige, hvilket gælder ifølge (i), og hvis de udspænder hele $k[x_1, \ldots, x_n]/I$. Vælg $[g] \in k[x_1, \ldots, x_n]/I$ arbitrært, sæt $\alpha_i = g(p_i)$, og tag $h = g - \sum_{i=1}^{n} a_i f_i$. Konstruér $h(p_j) = 0$ for alle j, sådan at h ligger i $\mathbf{I}(V)$. Ved at benytte Ifølge Hilberts stærke Nullsatellensatz, sætning 4.15, hvor $\mathbf{I}(V) = \sqrt{I}$, og det, at I er et radikale, så $h \in I$. Ergo er $[h]$ lig $[0]$ i $\mathbb{C}[x_1, \ldots, x_n]/I$, hvilket medfører, at $[g] = \sum_{i=1}^{n} a_i[f_i]$. □

Det bemærkes, at det eneste tidspunkt, hvor der i beviset benyttes, at der arbejdes i det algebraiske aflukke er i (ii). Hvis der er tale om endelige legemer, kan sætningen derfor ikke direkte oversættes. Sætning 4.29 giver, at hvis $k = \overline{k}$, så $|V(I)| \leq \dim(k[x_1, \ldots, x_n]/I)$. Da endvidere $\mathbb{F}_q \subseteq \overline{\mathbb{F}_q}$, så også $|V(I)\,|\subseteq|\,V(J)|$, hvor $I \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ og $J \subseteq \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$. Sættes dette sammen med resultatet fra sætning 4.29 fås fodaftryksgrænsen for endelige legemer.

Sætning 4.30 (Fodaftryksgrænsen for endelige legemer)**.** *Lad $I \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ være et ideal, så $V = \boldsymbol{V}(I)$ er en endelig mængde. Antallet af punkter i V er mindre end eller lig $dim(\mathbb{F}_q[x_1, \ldots, x_n]/I)$.*

Eksempel 4.25. *Betragter vi igen eksemplet fra 4.23, så kunne vi nemt tælle antallet af nulpunkter. Der var fire nulpunkter, så $\boldsymbol{V}(I) = \{1, y, y^2, y^3\}$. Ifølge fodaftryksgrænsen skulle dette være mindre end dimensionen af $\mathbb{F}_5[x, y]/I$, hvilket er sandt, da $dim(\mathbb{F}_5[x_1, \ldots, x_n]/I) = 5 \geq 4$.*

Der findes endnu en udgave af fodaftryksgrænsen, som er den, der betegnes som den egentlige fodaftryksgrænse. Denne fremkommer ved at udvide sit ideal med *legemsligninger*.

Sætning 4.31 (Fodaftryksgrænsen)**.** *Lad $I \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$, $I = \langle f_1, \ldots, f_s \rangle$ være et ideal, hvor $f_1, ldots, f_s \in \mathbb{F}_q[x_1, \ldots, x_n]$, så at $V = \boldsymbol{V}(I)$ er en endelig mængde. For*

$$I' = \langle f_1, \ldots, f_s, x_1^q - x_1, \ldots, x_n^q - x_q \rangle$$

haves, at $|V(I')| \leq dim(\mathbb{F}_q[x_1, \ldots, x_n]/I)$.

Det ses, at for at kunne give et estimat af antallet af nulpunkter for en affin varietet i et endeligt legeme, skal $V = \mathbf{V}(I)$ være endelig. Og V er ifølge sætning 4.28 endelig, hvis et Gröbnerbasis til I kan findes, og der for hvert i, $1 \leq i \leq n$, findes et $m_i \geq 0$ sådan at $x_i^{m_i} = LM(g_i)$ for $g_i \in G$.

Fodaftryksgrænsen er særligt anvendeligt resultat ift. netværkskodning. Som vi vil se i kapitel 5 er denne en vigtig ingrediens i at afgøre, hvornår et multicast netværk virker. Med dette resultat in mente sættes der punktum for den teoretiske del. Formålet med kapitlet har været at opbygge en værktøjskasse med alle de nødvendige redskaber for at kunne forstå, hvad netværkskodning er for en størrelse.

Kapitel 5

Random Network Coding

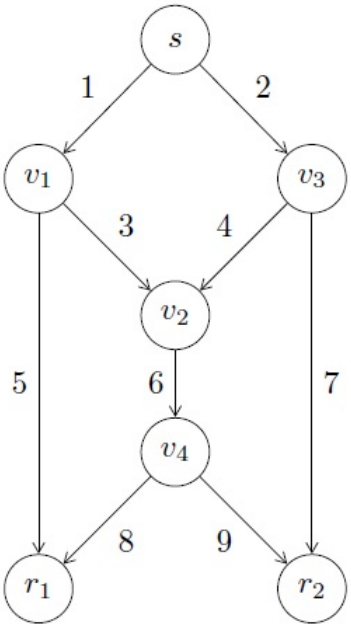
5.1 Introduktion

Netværkskodning udgør i dag et stort forskningsområde med mange forskellige aspekter. Netværkskodning handler først og fremmest om at forbedre transmissioner af informationer. Istedet for at forsinke transmissioner af dataoverførsel, gør netværkskodning det muligt at sende større mængder af data på samme tid. En måde at repræsentere punkt-til-punkt transmissioner på er ved en orienteret graf $G(V, E)$. Knudepunkterne repræsenterer de objekter mellem hvilke, der foregår transmissioner. Kanterne fortæller hvilken vej informationerne følger, for at komme fra en afsender til en modtager. Først illustreres et simpelt eksempel på, hvordan netværkskodning kan repræsenteres matematisk.

Betragt en orienteret graf $G(V, E)$, figur 5.1, med kanterne $1, \ldots, |E| = 9$. V repræsenterer mængden af knuder, og E repræsenterer mængden af kanter. At grafen er orienteret betyder, at data kun sendes i en retning, hvilket også ses af, at kanterne på figuren er illustreret som pile. Figuren kunne eksempelvis være en illustration af kommunikation imellem hjemmesider på internettet eller satelitter der kommunikerer i rummet. Man kan forestille sig, at hjemmesiden eller afsenderen s, gerne vil sende eller linke data til hjemmesiderne eller modtagerne r_1 og r_2.

Antag, at knuden s vil sende beskeden $\{a, b\}$ til modtagerne r_1 og r_2. Fra s til r_1 er der to mulige veje $\{(1, 5), (2, 4, 6, 8)\}$ og ligeledes fra s til r_2 $\{(1, 3, 6, 9)(2, 7)\}$. Disse mængder siges at være *flows* af størrelsen 2. Hvis beskeden a sendes via kant 1, beskeden b sendes via kant 2, og det antages at modtagerne r_1 og r_2 skal modtage både a og b, så vil beskederne følge de to flows. Med andre ord så følger a vejene $(1, 5)$ og $(1, 3, 6, 9)$ imens b følger vejene $(2, 4, 6, 8)$ og $(2, 7)$. Altså vil beskederne løbe ad fire veje. Der opstår dog et problem i v_2, hvis a og b sendes på samme tid, for hvilken besked skal så sendes videre ad kant 6. Antag at beskederne består af binære symboler $(1, 0)$, og lad beskeden, der sendes ad kant 6 være $a + b = x$. Da beskederne er binære symboler, giver summen mening. Modtageren r_1 får da a fra 5 og x fra 8. Hermed fås $x - a = b$. På samme måde modtages også både a og b i r_2. Problematikken er illustreret på figur 5.2.

Dette er altså princippet i netværkskodning. I det følgende afsnit introduceres læseren for den grundlæggende teori om netværkskodning. Rapporten vil fokusere på lineær netværkskodning i et multicast.



Figur 5.1: figuren viser et eksempel på et butterfly-netværk. Navnet kommer af grafens struktur, som til forveksling ligner kropper på en sommerfugl.

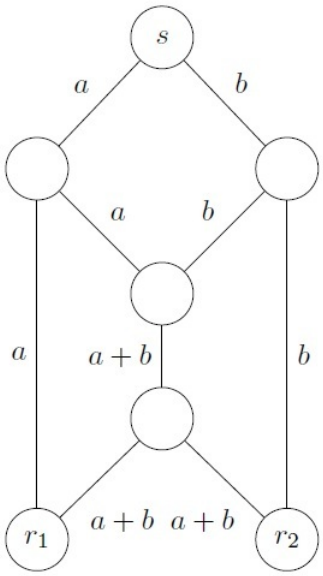
Definition 5.1 (Multicast)**.** *Et multicast defineres som et netværk, hvor alle modtagere modtager al information, som der gennemløber netværket.*

Kapitlet tager udgangspunkt i artiklen [2010 Geil & Thomsen] og suppleres op med information fra [2006 R. W. Yeung et al.], [2005 S. Jaggi et al.] og [2006 Lay]. I det følgende afsnit præsenteres begrebet *lineær netværkskodning.*

5.2 Network coding problem

Formålet med dette afsnit er at opbygge en ramme omkring lineær netværkskodning. Der vil blive taget udgangspunkt i butterfly-netværket fra figur 5.1 for at give både en grafisk og teoretisk fortolkning af begreb.

Lad $G = (V, E)$ være en orienteret graf som f.eks. butterfly-netværket, hvor V er mængden af knudepunkter, og E er mængden af kanter. Lad mængderne $S = \{s_1, \ldots, s_{|S|}\} \subseteq V$ og $R = \{r_1, \ldots, r_{|R|}\} \subseteq V$ være givet. Elementerne i S kaldes da for afsendere, og elementerne i R kaldes for modtagere. En besked sendes altså fra $s_1, \ldots, s_{|S|}$, og via en vej modtages beskeden af $\{r_1, \ldots, r_{|R|}\}$. En måde at beskrive en besked, som skal sendes via et netværk, er som en vektor. En besked-vektor er en vektor $\mathbf{X} = (X_1, \ldots, X_h) \in A^h$, hvor A er en endelig abelsk gruppe. Det huskes fra algebraen, at en abelsk gruppe er en gruppe, der opfylder den kommutative lov. Det vil sige, at en besked eksempelvis kan udtrykkes i binære symboler, $\mathbf{X} = (1, 0)$, hvorved den abelske gruppe er repræsenteres ved at endeligt legeme $\mathbb{F}_2^2$. Det giver mening at betragte det endelige legeme $\mathbb{F}_2$, da



Figur 5.2: Figuren illusterer beskeden $\{a, b\}$'s gennemløb af butterfly-netværket.

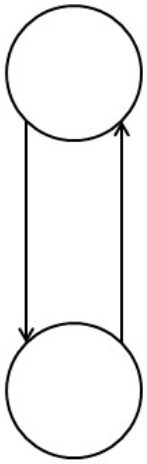
data i praksis sædvanligvis figurerer som et-taller og nuller.

Når data skal sendes over et netværk, skal det starte et sted fra. Derfor præsenteres *kildeafbildingen*. Denne er repræsenteret ved en surjektiv afbilding $K : \{X_1, \ldots, X_h\} \to S$. Det vil sige, at $K(X_j) = s_j$ svarer til, at afsenderen s_j sender beskeden X_j. Kildeafbildingen er dermed et udtryk for det data, som frembringes i den specifikke knude.

Lad endvidere $out(v)$ være kanterne væk fra en knude v, og antag for en kant $e = (u, v)$, at $out(e) = out(v)$. Da vi beskæftiger os med orienterede grafer, giver dette mening. Bemærk, at der gennem rapporten vil blive vekslet imellem brugen af notationen e og (u, v) for en kant. Similært defineres kanterne med retning mod en knude v som $in(v)$, og hvor der for en kant $e = (u, v)$ gælder, at $in(e) = in(v)$. For en kant v i en graf G er $in(v)$ altså de kanter, hvoraf v modtager beskeder, imens $out(v)$ er de kanter, hvoraf v videresender beskeder. Det er dermed muligt at beskrive retningen for hver enkelt kant i grafen. Det antages igennem rapporten, at netværkerne er cyklisk frie, hvilket vil sige, at ingen beskeder passerer igennem den samme knude to gange. Der er ingen loops. I netværket vil der derfor ikke opstå situationen, som er illustreret i figur 5.3.

Det betyder, at hver kant i vores orienteret acykliske graf kun transmitterer data en gang. Hver kant kant derfor gives en værdi. Det udtrykkes på følgende måde: for enhver kant j i den orienterede graf G haves en variabel $Y(j)$, som antager værdier i A. Spørgsmålet er så hvordan $Y(j)$'erne bestemmes. Det bemærkes dog, at beskeden, som sendes ad den j'te kant, må afhænge af hvad der kommer fra de indgående kanter, samt det, der genereres i den knude, som j udstikker fra. Altså for enhver kant $j \in G$ findes en funktion f_j, sådan at

$$Y(j) = f_j\left((Y(i)|i \in in(j)), (X_k|X_k \text{ genereres i } u)\right). \tag{5.1}$$



Figur 5.3: Figuren viser en cyklisk graf, hvor en besked kan passerer det samme knudepunkt mere end én gang.

Funktionen f_j vil blive refereret til som *kodningssfunktionen*, idet denne 'koder' beskeden, som sendes. Den data, der gennemløber en kant afhænger altså nu af en tredie ting, nemlig kodningfunktionen. Hvis værdien i parentesen for f_j er tom, sættes $Y(j) = 0$. Det svarer til, at beskeden, der sendes, ikke indeholder noget information. Når modtagerne til sidst i netværket modtager beskeder, vil de derfor være kodet. Der er derfor brug for en metode til at finde tilbage til de oprindelige beskeder. Her kommer mængden af *dekodningsfunktioner* D ind i billedet. Hvert element i mængden tager den indkomne information i den pågældende modtager, og oversætter den til de beskeder, som vi startede med at sende fra S. Det vil sige, at dekodningsfunktionerne D afbilder R over i mængden af ikke-tomme delmængder af $\{X_1, \ldots, X_h\}$. For hver modtaget besked i $r \in R$ fra en indkommmende kant til et $r \in R$ haves altså en variabel. Denne noteres som $Z_j^{(r)}$ og er udtrykt ved

$$Z_j^{(r)} = d_j^{(r)} \left(Y(i) | i \in in(r) \right),$$

hvor d_j er dekodningsfunktionen. For alle modtager $r \in R$ haves dermed $|D(r)|$ variable $Z_1^r, \ldots, Z_{|D(r)|}^{(r)}$, som tager værdier i A, fordi $D(r)$ indeholder alle dekodningsfunktionerne, og der findes én dekodningsfunktion for hver indkommende besked. På baggrund af ovenstående diskussion kan et netværksproblem defineres.

Definition 5.2. *Et netværk $G = (V, E)$ med afsendere S, modtagere R, beskedvektor $\mathbf{X} = (X_1, \ldots, X_h)$, en kildeafbilding K og dekodningsfunktioner D kaldes for et netværkskodningsproblem.*

Problemet siges at være løseligt, hvis der findes et ikke-trivielt alfabet A, en mængde af kodningsfunktioner f_j og dekodningsfunktioner $d_j^{(r)}$, således at

$$\left(Z_1^r, \ldots, Z_{|D(r)|}^{(r)} \right) = D(r)$$

gælder for alle $r \in R$.

Med andre ord er netværkskodningsproblemet løseligt såfremt at information når frem til alle modtagere. Det huskes, at et multicast var defineret som et netværk, hvor alle modtagere fik al information. I ovenstående terminologi svarer det til, at $D(r) = (X_1, \ldots, X_h)$ for alle $r \in R$. Da er der tale om et multicast netværk. Det ligger derfor også implicit i definition 5.1, at netværksproblemet er løseligt. Hvis der endvidere gælder, at $A = \mathbb{F}_q$, nemlig et endeligt legeme, og hvis alle $f_j, d_j^{(r)}$ er lineære i $\mathbb{F}_q$, så siges situationen at være et lineært netværksproblem. Givet et lineært netværksproblem, da kan $Y(j)$ og $Z_j^{(r)}$ udtrykkes som

$$Y(j) = \sum_{i \in in(j)} f_{ij} Y_i + \sum_{X_i \in S, K(X_i) = u} a_{ij} X_i, \quad \text{hvor } j = (u, v), \text{og} \tag{5.2}$$

$$Z_j^{(r)} = \sum_{i \in in(r)} b_{ij} Y_i. \tag{5.3}$$

At dette er sandt ses af, at vi nu bevæger os i et endeligt legeme. Funktionerne nedarver derfor reglerne for regneoperationer i en ring.

Antag i det følgende, at R og S er disjunkte mængder, sådan at ingen knude i netværket både er afsender og modtager. Givet et netvækskodningsproblem G, lad $r \in R$ og $D(r) = (X_{i_1}, \ldots, X_{i_t})$. Dette svarer til at en modtager i netværket efter dekodning, kommer frem til en besked $(X_{i_1}, \ldots, X_{i_t})$. Her vil et flow for modtageren r i den terminologi som blev præsenteret i introduktionen til kapitlet afsnit 5.1, være en mængde bestående af disjunkte veje fra afsendere i S til r. Der kan godt være flere veje, som udspringer af det samme $s \in S$, hvorfor vi indfører variablen $v^{(r)}(s)$. Denne defineres som antallet af veje fra S til modtageren r, som udspringer fra $s \in S$. Med definitionen af $D(r)$ som værende dekodningen af de beskeder, der ankommer til r, er $v^{(r)}(s)$ lig antallet af elementer i $D(r)$, som er frembragt af $s \in S$. Der findes jo nemlig en dekodningsfuknktion for hver vej ind i $r \in R$. Det bemærkes, at for at G skal kunne løses, da må der findes et flow for hver eneste $r \in R$ i G F.eks. fjernes kanterne (s, v_1) og (v_2, v_4) i netværket fra afsnit 5.1 sådan, at der ikke findes et flow for r_1, da overholder netværket ikke betingelser i definition 5.2. I dette tilfælde vil der nemlig ske det, at $D(r_1) = \emptyset$. Vi formulerer ovenstående diskussion i en sætning.

Sætning 5.1. *Hvis et netværksproblem G er løseligt, da findes et flow for hver eneste modtager i netværket.*

I det næste afsnit vil vi se på situationen, hvor $D(r) = (X_1, \ldots, X_h)$ for alle $r \in R$, for et lineært netværkskodningsproblem, også kaldet et multicast. I praksis er dette den ideelle situation, sådan at alle involverede parter i et netværk modtager den tilsigtede information. Pr. definition af et multicast så i relation til sætning 5.1 findes et flow til hver modtager. Inden multicast netværket udforskes nærmere eksemplificeres ovenstående teori dog via butterfly netværket fra introduktionen.

Eksempel 5.1. *Betragt netværket fra 5.1. Lad $\mathbf{X} = (X_1, X_2)$ være den besked, som skal sendes igennem netværket, hvor*

$$X_1 = 1 \qquad og \qquad X_2 = 0.$$

Det ses, at $\mathbf{X} \in \mathbb{F}_2^2$. Det ses, at $S = \{s_1\}$ og $R = \{r_1, r_2\}$. Vi er interesserede i en situation, hvor X_1 sendes ad (s, v_1) og X_2 sendes ad (s, v_3), præcis som i introduktionen med a og b. Udregnes

først $Y(1)$ *Ifølge* (5.2) *kan informationen, som sendes ad* (s, v_1)*, udtrykkes som*

$$\begin{aligned} Y(1) &= \sum_{i \in in(1)} f_{i,1} Y(i) + \sum_{X_i \in s, K(X_i)=u} a_{i,1} X_i \\ &= 0 + a_{1,1} X_1 + a_{2,1} X_2 \\ &= a_{1,1} \cdot 1 + a_{2,1} \cdot 0, \end{aligned}$$

da s *ikke har nogen indgående kanter. Hvis dette skal passe med, at* X_1 *sendes via kanten* (s, v_1)*, så må* $a_{1,1} = 1$ *og* $a_{2,1} = 0$*, da* $a_{ij} \in F_q$*. Udføres samme procedure for kanten* (s, v_3) *fås, at* $Y(2) = a_{1,2} \cdot 1 + a_{2,2} \cdot 0$*. Det vil sige, at* $a_{1,2} = 0$ *og* $a_{2,2} = 1$*. Dermed er stilen lagt, og informationen, der sendes af de øvrige kanter i netværket, kan udtrykkes efter samme fremgangsmåde. Det bemærkes, at der ikke genereres nye beskeder i* v_1*,* v_2*,* v_3*,* v_4*,* r_1 *og* r_2*, hvorfor*

$$\begin{aligned} Y(3) &= f_{1,3} Y(1), \\ Y(4) &= f_{2,4} Y(2), \\ Y(5) &= f_{1,5} Y(1), \\ Y(6) &= f_{3,6} Y(3) + f_{4,6} Y(4), \\ Y(7) &= f_{2,7} Y(2), \\ Y(8) &= f_{6,8} Y(6), \\ Y(9) &= f_{6,9} Y(6). \end{aligned}$$

Bemærk, at $f_{ij} \in \mathbb{F}_2$*, og for at alle modtagere skal modtage begge beskeder, så må ingen af* f_{ij}*'erne ovenfor være 0. Det huskes, at flows for de to modtagere var angivet ved hhv.* $\{(1,5),(2,4,6,8)\}$ *for* r_1 *og* $\{(1,3,6,9)(2,7)\}$ *for* r_2*. Hvis derfor et* $f_{i,j} = 0$*, vil det medføre et hul i vejen, og mindst én af de to modtagere vil ikke modtage det hele af den oprindelige besked. Så er der kun den ene mulighed, at de alle er 1. Dvs. alle* $Y(j)$*'er bestemmes til følgende:*

$$\begin{aligned} Y(1) &= 1 \qquad Y(2) = 0 \\ Y(3) &= 1 \qquad Y(4) = 0 \\ Y(5) &= 1 \qquad Y(6) = 1 \\ Y(7) &= 0 \qquad Y(8) = 1 \\ Y(9) &= 1. \end{aligned}$$

Vi vil nu bestemme outputtet for de to modtagere. Jvf. ovenstående diskussion står r_1 *med beskeden* X_1 *fra* (v_1, r_1) *og beskeden* $X_1 + X_2$ *fra* (v_4, r_1)*. Similært har* r_2 *modtaget* $X_1 + X_2$ *fra* (v_4, r_2) *og* X_2 *fra* (v_3, r_2)*. Opgaven lyder på at dekode beskederne* $X_1 + X_2$ *fra* (v_4, r_1) *og* $X_1 + X_2$ *fra* (v_4, r_2)*. Dette gøres ved* (5.3)*, så*

$$Z_{X_1}^{(r_1)} = \sum_{i \in in(r_1)} b_{i,1}^{(r_1)} Y_i = b_{5,1}^{(r_1)} Y(5) + b_{8,1}^{(r_1)} Y(8) = b_{5,1}^{(r_1)} \cdot 1 + b_{8,1}^{(r_1)} \cdot 1$$

$$\begin{aligned} Z_{X_2}^{(r_1)} &= b_{5,2}^{(r_1)} Y(5) + b_{8,2}^{(r_1)} Y(8) = b_{5,2}^{(r_1)} \cdot 1 + b_{8,2}^{(r_1)} \cdot 1 \\ Z_{X_1}^{(r_2)} &= b_{9,1}^{(r_2)} Y(9) + b_{7,1}^{(r_2)} Y(7) = b_{9,1}^{(r_2)} \cdot 0 + b_{7,1}^{(r_2)} \cdot 1 \\ Z_{X_2}^{(r_2)} &= b_{9,2}^{(r_2)} Y(9) + b_{7,2}^{(r_2)} Y(7) = b_{9,2}^{(r_2)} \cdot 1 + b_{7,2}^{(r_2)} \cdot 0. \end{aligned}$$

Heraf ses, at hvis $b_{5,1}^{(r_1)} = 1$, $b_{8,1}^{(r_1)} = 0$, $b_{5,2}^{(r_1)} = 0$ *og* $b_{8,2}^{(r_1)} = 0$, *så* $D(r_1) = (X_1, X_2)$. *På samme måde ses, at hvis* $b_{9,1}^{(r_2)} = 0$, $b_{7,1}^{(r_2)} = 1$, $b_{9,2}^{(r_2)} = 0$ *og* $b_{7,2}^{(r_2)} = 0$, *så* $D(r_2) = (X_1, X_2)$. *Ergo er der tale om et multicast, hvor alle modtagere får alle beskeder.*

I virkeligheden er det sjældent så nemt, som det her var tilfældet at bestemme a_{ij}'erne, f_{ij}'erne og b_{ij}'erne for dermed at afgøre om systemet er uden fejl. I det følgende vil vi se en metode til at afgøre dette, når det ikke er så ligetil at bestemme koefficienterne.

5.3 Linear network coding for multicast

Det ønskes at udforske multicastnetværket nærmere. Derfor betragtes i det følgende et lineært netværkskodningsproblem udtrykt ved definition 5.2, men hvor $D(r) = (X_1, \ldots, X_h)$ for alle $r \in R$. Vi får brug for at indføre tre typer af matricer. For yderligere forklaring af disse se eksempel 5.2. Lad A være en $h \times |E|$ matrix med a_{ij} på den (i,j)´te indgang, hvis $j \in out(K(X_i))$. Hvis $j \notin out(K(X_i))$, sættes $A = 0$. Her er h antallet af beskeder, som skal sendes, og $|E|$ er antal kanter i netværket.Størrelsen af A afhænger altså både af, hvor mange kanter der er i netværket, og hvor stor en besked, der skal sendes. Matricen A indeholder information om genereringen af beskeder i afsenderne.

Lad F være en $|E| \times |E|$ matrix med $f_{i,j}$ på den (i,j)´te indgang, hvis $j \in out(i)$, sådan at matricen indeholder alle kodningskoefficienterne for et netværk. Hvis $j \notin out(i)$, sættes $F = 0$. Matricen F indeholder altså information om kodningen af beskeder, som sendes via kanterne i netværket, og størrelsen af denne afhænger udelukkende af antallet af kanter i netværket.

For $r \in R$, lad $B^{(r)}$ være en $|E| \times h$ matrix med $b_{i,j}^{(r)}$ på den (i,j)´te indgang, hvis $i \in in(r)$. På den måde består $B^{(r)}$ af alle dekodningskoefficienterne. Hvis $i \notin in(r)$, så $B^{(r)} = 0$. Matricen B udgør det sidste led. Man kan sige, at A fortæller noget om genereringen af beskeder, F noget om kodningen og B noget om dekodningen. Samlet set udtaler de sig om alle flows for netværkets modtagere. Endvidere ses, at for ethvert ikke-negativt helt tal n, er den (i,j)'te indgang i F^n udtrykt ved

$$\sum_{(i=j_0,j_1,\ldots,j_n=j)} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j},$$

hvor $(i = j_0, j_1, \ldots, j_n = j)$ er en vej i G. Hvorfor, bliver mere klart, hvis man følger udregningerne i eksemplet, der følger dette afsnit. Det vil sige, at elementerne i F^n faktisk er kodningen af veje af længde n i netværket. Med længden af en vej menes antallet af kanter i vejen, så en vej af længde n, er en vej med n kanter. Da vi bevæger os i et endeligt legeme, F_q^n, $n \in \mathbb{N}$, da er den maksimale længde for en vej lig $n-1$. Det vil sige, at for et stort nok $N \in \mathbb{N}$, og da netværket som bekendt er acyklisk, vil matricen $F^N = 0$. For at summere op indeholder F information om veje af længde 1, F^2 information om veje af længde 2, F^3 information om veje af længde 3 osv.. Derfor vil matricen $(I + F + F^2 + \ldots + F^N - 1)$ indeholde information om alle veje af forskellig længde i netværket. Derfor kan vi konkludere, at følgende udsagn gælder:

$$(Y(1) \ldots Y(|E|)) = (X_1, \ldots, X_h)A(I + F + F^2 + \ldots + F^N - 1), \tag{5.4}$$

såfremt at $a_{i,j}$'erne og $f_{i,j}$'erne har en værdi. Informationen, som videresendes, er altså udtrykt ved (5.4). Eksempelvis afhænger beskeden, som sendes ad $Y(5)$ af genereringen af beskeder og vejene til Y(5). Næste skridt er at implementere dekodningen i ligningen. Det ses, at hvis der multipliceres

en matrix på begge sider i ligning (5.4), gælder ligheden stadig. Såfremt at $b_{i,j}$'erne har en værdi, kan outputtet i en modtager $r \in R$ udtrykkes som

$$(Y(1)\dots Y(|E|))B^{(r)} = (X_1,\dots,X_h)A(I+F+F^2+\dots+F^{N-1})B^{(r)} \tag{5.5}$$
$$= (X_1,\dots,X_h)M^{(r)}, \tag{5.6}$$

hvor $M^{(r)} = A(I+F+F^2+\dots+F^{N-1})B^{(r)}$. Fremover refereres til $M^{(r)}$ som værende transfermatricen. Bemærk, at da

$$\begin{aligned}(I-F)(I+F+\dots+F^{N-1}) &= I+F+\dots+F^{N-1}-F-F^2-\dots-F^{N-1}-F^N \\ &= I-F^N,\end{aligned}$$

og $F^N = 0$ for et stort nok $N \in \mathbb{N}$, så gælder, at

$$M^{(r)} = A(I-F)^{-1}B^{(r)}. \tag{5.7}$$

Det kan godt være tidskrævende at skulle udregne alle potenser af F, men med udtrykket i ligning (5.7) er det nok at invertere matricen $(I-F)$. Vi kræver nu, at transfermatricen har fuld rang. Vi husker, at rangen af en matrix er lig dimensionen af søjlerummet. At en matrix har fuld rang betyder, at matricen har den størst mulige rang. Ergo har transfermatricerne ingen nulsøjler, hvilket medfører, at determinanterne er forskellige fra nul. Heraf fås, at hvis $M^{(r)}$, som iøvrigt er en $h \times h$ matrix(se eksempel 5.2), har fuld rang, så medfører det, at

$$\prod_{r\in R} \det M^{(r)} \neq 0. \tag{5.8}$$

Polynomiet i (5.8) kaldes for *transferpolynomiet*. Hvis transferpolynbomiet er lig 0, så svarer det til, at en eller flere af determinanter er 0. Igen betyder det, at der for en af transfermatricen gælder, at den ikke har fuld rang og dermed har en nulsøjle. At den har en nulsøjle svarer til, at en eller flere af modtagerne i netværket ikke modtager beskeder fra S, hvilket er i modstrid med definitionen på et løseligt netværksproblem definition **??**. Det er derfor vigtigt, at give værdier til $f_{i,j}$'erne således, at transfermatricen får fuld rang. At transfermatricen har fuld rang er også en anden måde at sige, at vektorerne i transfermatricen skal være lineært uafhængige og udspænde hele $\mathbb{F}_q^n$.

Det bemærkes, at givet $a_{i,j}, f_{i,j}$ og $b_{i,j}^{(r)}$ således, at $M^{(r)}$ har fuld rang for et $r \in R$, da er det muligt, at korrigere $b_{i,j}^{(r)}$'erne således, at $M^{(r)} = \dots = M^{|R|}$. Det betyder, at for at bestemme om et lineært netværksproblem er løseligt, er det nok at afgøre om transferpolynomiet er forskellig fra nul. Variablerne $b_{i,j}^{(r)}$ skal blot korrigeres sådan, at vektorerne bliver lineært uafhængige.

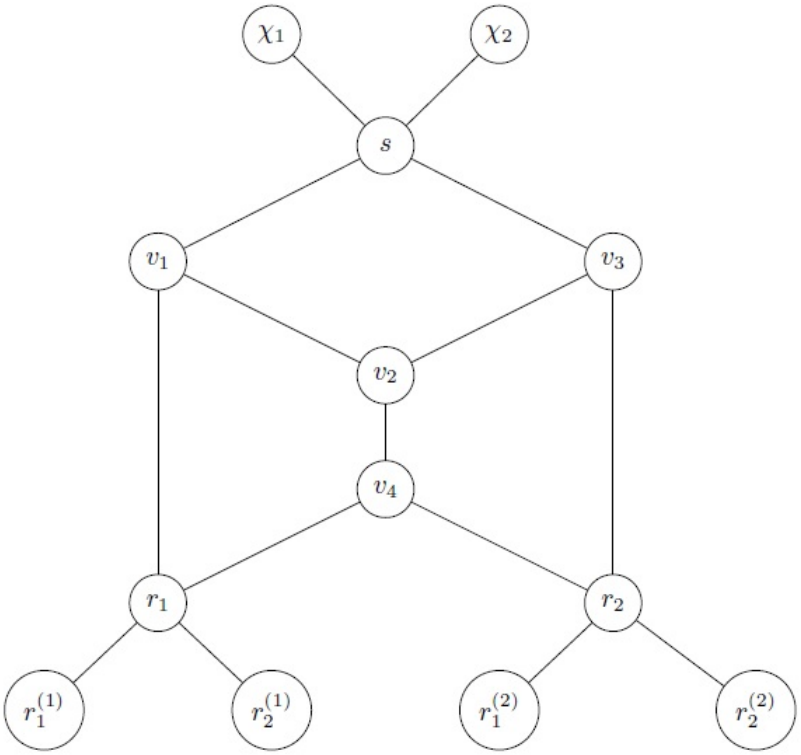
I bogen [2006 T. Ho et al.] introduceres *Edmondsmatricen*, $E^{(r)}$, og det bevises, at $\det M^{(r)}$ enten er lig $\det E^{(r)}$ eller $-\det E^{(r)}$, hvor

$$E^{(r)} = \begin{bmatrix} A & 0 \\ I-F & B^{(r)} \end{bmatrix}. \tag{5.9}$$

Edmondsmatricen er mere anvendelig end $M^{(r)}$, idet vi for det første ikke skal finde et N, således at $F^N = 0$. Det er derfor nok, at bestemme om $\prod_{r\in R} \det E^{(r)} \neq 0$, når der søges et svar på om $\prod_{r\in R} \det M^{(r)} \neq 0$.

Den foregående diskussion tyder på, at transfermatricen $M^{(r)}$ og transferpolynomiet er meget vigtige elementer i arbejdet med multicasts. At specielt transfermatricen indeholder mange informationer om et netværk ses særligt ved at udvide systemet. Givet et multicast netværk, udvides

grafen $G = (V, E)$. Dette gøres ved først at tilføje h nye knuder $\chi_1, \ldots, \chi_h$, altså samme antal som der er beskeder. Fra hver af disse knuder tilføjes en kant til S. Det betyder, at hvis f.eks. $\mathbf{X} = (X_1, X_2, X_3)$ og $S = (s_1, s_2)$ tilføjes seks nye kanter i grafen. I næste trin udvides grafen $G = (V, E)$ ved for ethvert $r \in R$ at tilføje h nye modtagere $r^{(1)}, \ldots, r^{(h)}$. Fra hver ny modtagere tilføjes en kant til r. Udføres denne udvidelse på butterfly-netværket fås en graf som vist på figur .



Figur 5.4: Figuren viser, hvordan butterfly-netværket udvides.

Vores gamle definition af et flow passer ikke helt med den udvidet graf, så denne opdateres. For alle modtagere $r \in R$ lader vi et *udvidet flow* $\mathcal{F}$ være en vej fra de nye afsendere $\chi_1, \ldots, \chi_h$ til de nye modtagere $r^{(1)}, \ldots, r^{(h)}$. Dermed bliver $\mathcal{F}$ en mængde bestående af h kantdisjunkte veje. Det vil sige, at element i $\mathcal{F}$ er en vej fra en afsender, χ_i, $i = 1, \ldots, h$, til en modtager $r_j^{(i)}$, og et sådant element forekommer ikke mere end én gang i mængden. Som i den ikke udvidede situation er en vej stadig pr. konstruktion et produkt af et $a_{i,j}$, nogle $f_{i,j}$'er og et $b_{i,j}$. Ét $a_{i,j}$ i genereringen af beskeder, $f_{i,j}$'er for hver kant i vejen, der haves, og til sidst et $b_{i,j}$ repræsenteret ved den sidste kant. Det er dermed klart, at den (i, j)'te indgang i $M^{(r)}$ beskriver alle veje fra χ_i til $r^{(j)}$. Samtidigt indses det, at afbildingen af flows i den udvidet graf over i monomierne i det$M^{(r)}$ faktisk er en injektiv afbilding.

Hvis $a_{i,j}$'erne, $f_{i,j}$'erne og $b_{i,j}$'erne er ukendte, vil vi tænke på dem som værende variable. Ovenstående diskussion giver anledning til følgende meget vigtige sætning:

Sætning 5.2. *Transferpolynomiet er forskellig fra 0 hvis og kun hvis der til hver modtager $r \in R$ findes et flow af størrelsen h.*

For at summere op givet et netværksproblem med på forhånd bestemte $a_{i,j}$'ere og $f_{i,j}$'ere, er det nok, at der findes et flow for hver modtager i netværket. For findes et flow, kan $b_{i,j}$'erne bestemmes, sådan at vektorerne i transfermatricen er lineært uafhængige. Hvis søjlerne i transferpolynomiet er lineært uafhængige og udspænder hele $\mathbb{F}_q^n$, da er transferpolynomiet forskelligt fra 0. Vi vil udvide ovenstående sætning for dermed at kunne afgøre, hvornår et multicast er løseligt blot ud fra tilstedeværelsen af flows til de forskellige modtagere i netværket. Husk, at et flow af størrelsen h er en mængde indeholdende h veje fra hver $s \in S$ til $r \in R$. Med dette in mente indføres begrebet *flowsystem*.

Definition 5.3. *Et flowsystem er en samling af alle flows for et netværk, ie.*

$$\mathcal{F} = \{F_1, \ldots, F_{|R|}\},$$

hvor F_i er et flow af størrelsen h for modtageren r_i, og $i = 1, \ldots, |R|$.

I eksempel 5.1 er flowsystemet udtrykt ved $\mathcal{F} = (F_1, F_2)$, hvor $F_1 = \{(1,5),(2,4,6,8)\}$ og $F_2 = \{(1,3,6,9)(2,7)\}$. Til at udvide sætning 5.2 behøves en særlig grænse, kaldet Fodaftryksgrænsen. I artiklen [2010 Geil & Thomsen] ses grænsen i den udformning, som kendes fra sætning 4.29. Artiklen definerer fodaftrykket som følgende:

Definition 5.4. *Lad $>$ være en monomiel ordning og $I \subseteq k[x_1, \ldots, x_n]$ et ideal. Fodaftrykket til et ideal med ordningen $>$ noteres som $\Delta_>(I)$ og svarer til mængden bestående af alle monomier i I, hvorom der gælder, at de ej er et ledende monomium til et polynomium i I.*

Det ses, at antallet punkter i fodaftrykket i artiklen svarer til $\dim(\mathbb{F}_q[x_1, \ldots, x_n]/I)$ fra teorien. Det huskes, at Fodaftryksgrænsen i dens generelle udformning var udtrykt ved sætning 4.31. Med udgangspunkt i denne kan der opskrives følgende korollar i det tilfælde, hvor blot et polynomium betragtes:

Korollar 5.1. *Lad $f \in k[x_1, \ldots, x_n]$ være et polynomium forskellig fra nulpolynomiet. Antag at det førende monomium til f er $x_1^{i_1} \cdots x_n^{i_n}$, hvor $0 \leq i_1, \ldots, i_n \leq q$. Antallet punkter, hvor polynomiet ej forsvinder i $\mathbb{F}_q^n$, er mindst*

$$(q - i_1) \cdots (q - i_n).$$

Bevis. Indse at

$$\begin{aligned} &\Delta\left(\langle x_1^q - x_1, \ldots, x_n^q - x_n, f\rangle\right) \\ \subseteq &\{x_1^{s_1} \cdots x_n^{s_n} \mid \text{ for } t = 1, \ldots, n \text{ og hvor} \\ &i_t \leq s_t \text{ikke gælder for alle } t = 1, \ldots, n\}, \end{aligned}$$

så er sætningen ved anvendelse af Fodaftryksgrænsen, sætning 4.31, sand. □

Det er nu muligt at give en bedre estimering af, hvornår et multicast er løseligt.

Sætning 5.3. *Et multicast netværkskodningsproblem er løseligt, hvis og kun hvis det tilhørende transferpolynomium er forskelligt fra nul. Endvidere når problemet er løseligt, så virker lineær netværkskodning for alle legemer $\mathbb{F}_q$, hvor $q \geq |R|$.*

Bevis. Antag først at det tilhørende transferpolynomium er forskelligt fra nul. Ifølge sætning 5.2 findes da for hver modtager et flow af størrelsen h, hvor h er antallet af forskellige veje til den samme modtager i netværket. Når der findes et flow for hver modtager af størrelsen h, betyder det endvidere, at der findes et flowsystem af størrelsen h. Det huskes, at definitionen på et multicast jo netop var, at alle modtagere fik al information, dvs. at der findes et flowsystem af størrelsen h. Ergo er problemet løseligt.

Antag nu på den anden side at problemet er løseligt. Da findes et flowsystem af størrelsen h, hvilket vil sige, der findes et flow for hver modtager af størrelsen h. Igen følger det da direkte af sætning 5.2, at transferpolynomiet må være forskelligt fra nul.

Den sidste del af sætningen kommer af korollar 5.1. Eksponenterne i transferpolynomiet kan ikke overskride $|R|$ i værdi, hvorfor der ifølge korollaret må findes en løsning til det lineære netværkskodningsproblem, så længe blot at $q \geq |R|$. □

Det vil vise sig, at $q = |R|$ faktisk er en tilstrækkelig betingelse for, at vores multicast er løseligt. Den første del af ovenstående sætning kunne også, som det er vist i beviset for denne, formuleres på følgende måde:

Sætning 5.4. *Et multicast netværkskodningsproblem er løseligt hvis og kun hvis den tilhørende graf indeholder et flowsystem af størrelsen h.*

I det følgende afsnit præsenteres en algoritme, som finder denne løsning, såfremt at et flowsystem af størrelse h er givet.

Eksempel 5.2. *Betragt eksemplet fra 5.1 med Butterflynetværket. Til at starte med udtrykkes matricerne beskrevet først i afsnittet. Hermed er A, F og $B^{(r)}$ udtrykt ved*

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ a_{2,1} & a_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.10}$$

$$F = \begin{bmatrix} 0 & 0 & f_{1,3} & 0 & f_{1,5} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_{2,4} & 0 & 0 & f_{2,7} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_{3,6} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_{4,6} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{6,8} & f_{6,9} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{5.11}$$

$$B^{(r)} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ b_{5,1}^{(r_1)} & b_{5,2}^{(r_1)} \\ 0 & 0 \\ b_{7,1}^{(r_2)} & b_{7,2}^{(r_2)} \\ b_{8,1}^{(r_1)} & b_{8,2}^{(r_1)} \\ b_{9,1}^{(r_2)} & b_{9,2}^{(r_2)} \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}. \tag{5.12}$$

Hvis eksemplet skal stemme overens med teorien, så findes et $N \in \mathbb{N}$, så F^N er lig nulmatricen. Bemærk, at for $N = 2$ så

$$F^N = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & f_{1,3}f_{3,6} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_{2,4}f_{4,6} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{3,6}f_{6,8} & f_{3,6}f_{6,9} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{4,6}f_{6,8} & f_{4,6}f_{6,9} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Det ses, at indgangene i F består af linearkombinationer af f_{ij}. Faktisk sættes $N = 3$, så $F^N = 0$. Vi ved på forhånd fra eksempel 5.1 at netværket er et multicast, hvilket også ses ved udregning af transferpolynomiet jvf. (5.5)*:*

$$M^{(r)} = A(I + F + F^2)B^{(r)} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$
$$det(M^{(r)}) = 1 \neq 0.$$

Jvf. ligning (5.9) *kunne vi også have opskrevet Edmondsmatricen. Denne er ved indsættelse af matricerne fra* (5.10) *udtrykt ved*

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

.

5.4 Flow-algoritme

I det følgende antages, at hvis der om et multicast netværkskodningsproblem vides, at det er løseligt, så kan man bestemme et tilhørende flowsystem. I dette afsnit præsenteres en af mange algoritmer til bestemmelse af løsninger til problemet over $\mathbb{F}_q$, med den betingelse at alle $q \geq |R|$. Det vil sige, at givet et løseligt multicast, da ligger tricket altså i at bestemme et flowsystem for netværket. Bestemmes flow-systemet behøver vi altså ikke bekymre os om, om det er muligt at løse netværksproblemet. Det er det, og løsningen kan findes ved hjælp af nedenstående algoritme. Algoritmen anvender et begreb kaldet globale kodningsvektorer.

Definition 5.5. *Givet et netværksproblem G, og antag at $a_{i,j}$ og $f_{i,j}$ er valgt på samme måde som tidligere. For enhver kant $j \in E$, som er mængden af kanter i G, defineres den globale kodningsvektor som $c_g(j) = (c_1, \ldots, c_h)$, såfremt at $Y(j) = c_1X_1 + \cdots + c_hX_h$.*

Den globale kodningsvektor $c_g(j)$ for en kant j, består af koefficienterne i linearkombinationen, som beskriver beskeden for den givne kant. Koefficienterne $c_1, \ldots, c_h$ kaldes for *kodningskoefficienterne*. I eksempel 5.1 ses, at den globale kodningsvektor for kant 1 er udtrykt ved $c_g(1) = (1, 0)$, hvor kodningskoefficienterne $c_1 = 1$ og $c_2 = 0$.

Bemærk, at hvis der for hver modtager $r \in G$ gælder, at de globale kodningsvektorer til hver af de indgående kanter udspænder hele F_q^h, så indgår kodningskoefficienterne $c_1, \ldots, c_h$ som en del af løsningen til problemet. Kodningskoefficienterne afhænger af de valgte $a_{i,j}$ og $f_{i,j}$, hvorfor der kun er tilbage at bestemme $b_{i,j}$'erne for at kunne dekode beskederne.

Det hele står og falder altså med om et flowsystem til et givet løseligt multicast kan bestemmes. Algoritmen starter ved, at vi udvider et givet multicast på følgende måde. Først tilføjes en ny knude s'. For hver $s_i \in S$ tilføjes $v(s_i)$ kanter fra s' til s_i, $i = 1, \ldots, |S|$, hvor $v(s_i)$ er lig antallet af beskeder, som genereres i s_i. I butterfly-netværket fra eksempel 5.1 haves kun en afsender, men som til gengæld sender to beskeder. Det vil sige, at ved tilføjelsen af s', tilføjes to kanter fra s' til s, og $v(s)$ er her lig 2.

Vi begynder nu på selve algoritmen. Antag, at alle beskeder genereres i s' fremfor i s_i'erne, og lad $\mathcal{F} = (F_1, \ldots, F_{|R|})$ være et flowsystem for netværket. Her er F_1 et flow for modtageren r_1, F_2 et flow for modtageren r_2 osv.. Gør nu følgende:

(a) Hvis (i, j) ikke indgår som en del af en vej i $\mathcal{F}$, da sættes $f_{i,j} = 0$.

(b) Kodningsfunktionerne, $f_{i,j}$'erne, til s' vælges sådan, at de globale kodningsvektorer for de nytilføjede kanter er udtrykt som enhedsvektorerne

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1). \tag{5.13}$$

Det vil sige, at beskederne som sendes af de h nye kanter, svarer til de beskeder, som fra start blev sendt fra S. Lad nu C_l være mængden bestående af de tilføjede kanter, som indgår i et flow til r_l, $l = 1, \ldots, |R|$. F.eks. hvis eksempel 5.1 igen betragtes, vil C_1 bestå af begge de nytilføjede kanter, da de begge kommer til at indgå i et flow for r_1. Lad endvidere $B_1, \ldots, B_{|R|}$ være de tilsvarende mængder bestående af de globale kodningsvektorer. I forhold til eksemplet består B_1 af de to globale kodningsvektorer for hhv. (v_1, r_1) og (v_4, r_1). Det springende punkt i algoritmen er et såkaldt loop, hvor C_l siges at blive *opdateret* og hvor kodningskoefficienter vælges sådan, at

(i) C_l er et cut i F_l.

(ii) Den ordnede mængde B_l bestående af globale kodningsvektorere udspænder hele $\mathbb{F}_q^h$.

Husk, at F_l er et flow for modtageren r_l. Om selve opdateringen gælder, at efter endeligt mange af dem, så $C_l = in(r_l) \cap F_l, l = 1, \ldots, |R|$, hvilket betyder, ifølge (ii), at hver modtager har nok information, som gør det muligt at udregne passende $b_{i,j}$'er. Sagt med ord kommer C_l til at bestå af de indgående kanter til r_l, som også er med i flow'et for r_l.

Nu til selve opdateringen. Betragtes en kant $j \in \mathcal{F}$, er det interessant at se på den eller de modtagere r_j, hvor j er en del af flow'et til disse. Lad nu j være en del af C_l og fjern den forrige kant, $in(j) \in F_l$, fra C_l. Sagt på en anden måde fjernes kanten i, som ligger i både C_l og $in(j)$, og hvor (i, j) er et cut i F_l. Lad $l_1, \ldots, l_k$ være de værdier for hvilke C_l opdateres, og lad $i_1, \ldots, i_k$ (muligt at $i_s = i_t$ for $s \neq t$) være de fjernede kanter fra $C_{l_1}, \ldots, C_{l_k}$. Spørgsmålet er da, om vi kan

vælge kodningskoefficienter $f_{i_1,j},\ldots,f_{i_k,j}$, sådan at alle globale kodningsvektorer for $B_{l_1},\ldots,B_{l_k}$ svarende til $C_{l_1},\ldots,C_{l_k}$ udspænder hele F_q^h. Det kan vi, og selv om kodningskoefficienterne vælges tilfældigt, er sandsynligheden for, at algoritmen finder et flowsystem, positiv. Dette sikres bl.a. af følgende lemma.

Lemma 5.1. *Givet et basis* $\left\{\overline{b_1},\ldots,\overline{b_h}\right\}$ *for* $\mathbb{F}_q^h$ *og* $\overline{c}\in\mathbb{F}_q^h$*, da findes præcis et* $a\in\mathbb{F}_q$ *sådan, at*

$$\overline{c}+a\overline{b}_h\in Span_{F_q}\left\{\overline{b}_1,\ldots,\overline{b}_{h-1}\right\}.$$

Bevis. Tag basis $\left\{\overline{b_1},\ldots,\overline{b_h}\right\}$ for $\mathbb{F}_q^h$ og $\overline{c}\in\mathbb{F}_q^h$. Det betyder, at vi kan skrive $\overline{c}$ som en linearkombination af vores basis:

$$\overline{c}=c_1\overline{b_1}+\cdots+c_h\overline{b_h}.$$

Det ses, at hvis $a=-c_h$ og kun når dette er tilfældet, da

$$\overline{c}-c_h\overline{b}_h=c_1\overline{b_1}+\cdots+c_{h-1}\overline{b_{h-1}}\in Span_{F_q}\left\{\overline{b}_1,\ldots,\overline{b}_{h-1}\right\}.$$

□

For hver af de fjernede kanter i_t anvendes ovenstående lemma med tilhørende basis B_{l_t}, og hvor $\overline{b_h}=c_g(i_t)$, og

$$\overline{c}=\sum_{l\in\{i_1,\ldots,i_k\}\setminus\{i_t\}}f_{l,j}c_g(l).$$

Lad nu $k'=|\{i_1,\ldots,i_k\}|=|(in(j)\cap\mathcal{F})|$. Sandsynligheden for succes i et gennemløb af algoritmen er mindst

$$\frac{q^{k'}-kq^{k'-1}+(k-1)}{q^{k'}}=1-\frac{k}{q}+\frac{k-1}{q^{k'}}. \tag{5.14}$$

For at forstå dette tænkes på det værste mulige tilfælde. I ovenstående udtryk er $q^{k'}$ alle de mulige valg og i tælleren fjernes derfor alle de dårlige valg. Hvis valget af kodningskoefficienter ikke giver nogen indkommende besked for modtageren r_{l_t}, så virker algoritmen i hvert fald for $r_{l_1},\ldots,r_{l_{t-1}},r_{l_{t+1}},\ldots,r_{l_k}$. Gøres dette, har vi talt $f_{i_1,j}=\cdots=f_{i_k,j}=0$ med k gange.

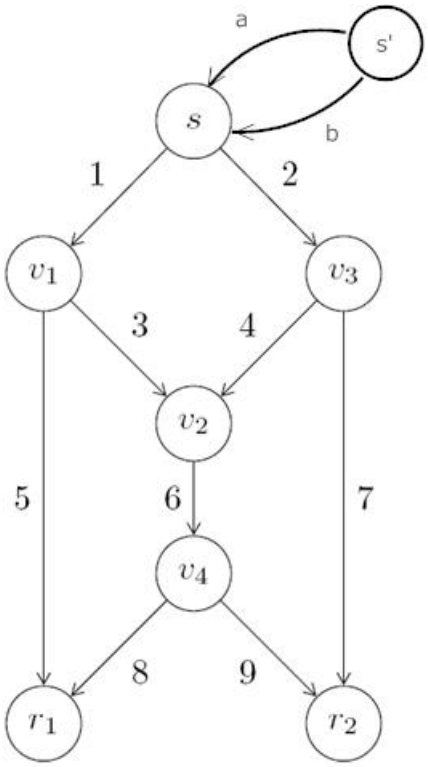
Det ses, at udtrykket i (5.14) er positivt for $q\geq k$, idet $\frac{k}{q}$ da er mindre end 1 og $\frac{k-1}{q^{k'}}$ bliver et meget lille tal. Det er derfor ønskværdigt, at $q\geq k$. Det vides, at $k\leq|R|$, så ved at vælge $q\geq|R|$, bliver udtrykket i (5.14) positivt, og dermed er $\mathbb{F}_q$ stor nok for et løseligt netværkskodningsproblem. Det betyder, at selvom kodningskoefficienter til systemet er valgt vilkårligt, så er der en positive sandsynlighed for, at netværket alligevel virker, så længe at $q\geq|R|$.

For at gøre det mere klart, hvordan flowalgoritmen virker, anvendes denne på Butterfly-netværket. Det sidste afsnit i kapitlet handler om, at komme sandsynligheden for succes lidt nærmere.

Eksempel 5.3. *I dette eksempel vil flow-algoritmen blive anvendt på netværket fra 5.1. Algoritmen starter med en udviddelse af netværket. Der tilføjes en knude s' og en kant fra s' til s for hver besked der sendes. Det vil sige, at netværket udvides med en knude og to kanter. De to nye kanter vil blive refereret til som a og b. Dette giver et netværk af følgende udseende:*

Lad nu $\mathcal{F}=(F_1,F_2)$ *være et flowsystem, hvor* F_1 *er et flow til modtageren* r_1 *og* F_2 *er et flow til modtageren* r_2*. De to flow's bliver da*

$$F_1=\{(a,1,5),(b,2,4,6,8)\}$$
$$F_2=\{(a,1,3,6,9)(b,2,7)\}.$$



Altså haves to flows af størrelsen 2. Ifølge algoritmen hvis der er kanter som ej er en del af et flow, da sættes $f_{i,j} = 0$*. Dette problem haves dog ej her, da alle kanter indgår i et flow. Herefter vælges kodningsfunktioner til* s' *sådan, at de globale kodningsvektorer til kanterne* a *og* b *er hhv.* $(1,0)$ *og* $(0,1)$*. Det vil sige, at de udspænder hele* $\mathbb{F}_q^2$*. Lad nu* $C_1 = \{a, b\} = C_2$ *og tilsvarende* $B_1 = \{(1,0),(0,1)\} = B_2$*. Betragt kanten* $1 = (s, v_1)$*. Om denne gælder, at* $1 \in F_1, F_2$*. Kanten tilføjes nu til* C_1 *og* C_2 *samtidig med at dens forgænger i både* F_1 *og* F_2 *fjernes. Det vil sige, at der nu haves* $C_1 = \{1, b\} = C_2$*, og* i_1 *sættes lig den fjernede kant* a*. Opgaven er nu at bestemme kodningskoefficienter* $f_{a,1}$ *og* $f_{b,1}$*. Da vi kun ønsker at sende den ene besked* X_1 *ad 1, sættes* $f_{a,1} = 1$ *og* $f_{b,1} = 0$*. Hermed fås, at*

$$\begin{aligned} Y(1) &= f_{a,1}X_1 + f_{b,1}X_2 \\ &= 1 \cdot X_1 + 0 \cdot X_2. \end{aligned} \tag{5.15}$$

Betragt nu kanten $2 = (s, v_3)$*. Princippet er her det samme som før, og vi får nu, at* $C_1 = \{1, 2\} = C_2$*. Kodningskoefficienterne er givet ved* $f_{a,2} = 0$ *og* $f_{b,2} = 1$*, hvorfor*

$$\begin{aligned} Y(2) &= f_{a,2}X_1 + f_{b,2}X_2 \\ &= 0 \cdot X_1 + 1 \cdot X_2. \end{aligned} \tag{5.16}$$

Af ligningerne (5.15) *og* (5.16) *ses nu, at* $c_g(1) = (1,0)$ *og* $c_g(2) = (0,1)$*, som tilsammen udspænder* $\mathbb{F}_q^2$*.*

Betragt nu kant $3 = (v_1, v_2) \in F_2$*. Kanten tilføjes til* C_2*, imens dens forgænger i* F_2 *fjernes. Det*

vil sige, at $C_2 = (3, 2)$*. Kodningskoefficienten* $f_{1,3}$ *sættes lig 1, hvorved*

$$\begin{aligned} Y(3) = f_{1,3}Y(1) &= 1 \cdot (1 \cdot X_1 + 0 \cdot X_2) \\ &= 1 \cdot X_1 + 0 \cdot X_2 \end{aligned}$$

Ligeledes fås for $4 = (v_3, v_2) \in F_1$*, at* $C_1 = (1, 4)$*. Kodningskoefficienten* $f_{2,4} = 1$*, for så*

$$\begin{aligned} Y(4) = f_{2,4}Y(2) &= 1 \cdot (0 \cdot X_1 + 1 \cdot X_2) \\ &= 0 \cdot X_1 + 1 \cdot X_2. \end{aligned}$$

Hermed ses, at $c_g(3) = c_g(1)$ *og* $c_g(4) = c_g(2)$ *og de udspænder stadig hele rummet.*

Betragt nu $5 = (v_1, r_1) \in F_1$*. Opdateres* C_1 *fås, at* $C_1 = (5, 4)$*. Kodningskoefficienten* $f_{1,5}$ *sættes lig 1, da det giver, at*

$$\begin{aligned} Y(5) = f_{1,5}Y(1) &= 1 \cdot (1 \cdot X_1 + 0 \cdot X_2) \\ &= 1 \cdot X_1 + 0 \cdot X_2 \end{aligned}$$

Tag nu kanten $6 = (v_2, v_4) \in F_1, F_2$*. Opdateres først* C_1 *fås* $C_1 = (5, 6)$*, hvor det ses, at kanten 5's forgænger i* F_1*, som er kant* 4*, er blevet erstattet med 5. Opdateres dernæst* C_2 *fås, at* $C_2 = (6, 2)$*, hvor kant 2 er blevet erstattet med kant 6. Kodningskoefficienterne* $f_{6,3}$ *og* $f6, 4$ *sættes begge lig 1, da*

$$\begin{aligned} Y(6) = f_{6,3}Y(3) + f6, 4Y(4) &= 1 \cdot (1 \cdot X_1 + 0 \cdot X_2) + 1 \cdot (0 \cdot X_1 + 1 \cdot X_2) \\ &= 1 \cdot X_1 + 1 \cdot X_2. \end{aligned}$$

Betragt kanten $7 = (v_3, r_2) \in F_2$*. Efter opdateringen af* C_2 *fås, at* $C_2 = (6, 7)$*, og kodningskoefficienten* $f_{2,7}$ *sættes lig 1, da*

$$\begin{aligned} Y(7) = f_{2,7} \cdot Y(2) &= 1 \cdot (0 \cdot X_1 + 1 \cdot X_2) \\ &= 0 \cdot X_1 + 1 \cdot X_2. \end{aligned}$$

Opsummeres ses, at $c_g(5) = c_g(1) = (1, 0)$*,* $c_g(6) = (1, 1)$ *og* $c_g(7) = c_g(2) = (0, 1)$*. Disse vektorer er parvis lineært uafhængige og udspænder parvis hele* $\mathbb{F}_q^2$*. Vi bevæger os nu til de sidste to kanter. Tag kanten* $8 = (v_4, r_1) \in F_1$*. Vi opdaterer* C_1 *sådan, at* $C_1 = (5, 8)$*. Kodningskoefficienten* $f_{6,8}$ *sættes lig 1, hvorfor*

$$\begin{aligned} Y(8) = f_{6,8} \cdot Y(6) &= 1 \cdot (1 \cdot X_1 + 1 \cdot X_2) \\ &= 1 \cdot X_1 + 1 \cdot X_2 \end{aligned}$$

Endelig betragt kant $9 = (v_4, r_2) \in F_2$*. Vi opdaterer* C_2 *sådan, at* $C_2 = (9, 8)$*. Kodningskoefficienten* $f_{6,9}$ *sættes lig 1, hvorfor*

$$\begin{aligned} Y(9) = f_{6,9} \cdot Y(6) &= 1 \cdot (1 \cdot X_1 + 1 \cdot X_2) \\ &= 1 \cdot X_1 + 1 \cdot X_2. \end{aligned}$$

Det ses, at $c_g(8) = c_g(9) = (1, 1)$*. Det bemærkes, at de globale kodningsvektorer i modtagerne* r_1 *og* r_2 *tilsammen udspænder hele* F_q^2*, hvilket gør det muligt at besteme* $b_{i,j}$*'er, for at fremkalde beskeder, præcis som vist i eksempel 5.1. Det ses, at i dette eksempel er* $q = 2$ *en tilstrækkelig forudsætning for, at algoritmen virker.*

5.5 Vilkårlig lineær netværkskodning

Betragt et løseligt netværkskodningsproblem. Ifølge korollar 5.1, så hvis q er stor nok, vil sandsynligheden for at vilkårligt valgte kodnings- og dekodningskoefficienter være positiv. I vilkårlig netværkskodning gives først værdi til en delmængde af alle kodningskoefficienter. Delmængden kan være tom, så det er ikke et direkte krav, at nogle kodningskoefficienter skal være bestemt på forhånd. I et løseligt netværkskodningsproblem kunne man f.eks. betragte kanten j med indgående kant i og give kodningskoefficienten $f_{i,j}$ værdien 1. Derefter vælges resten af kodningskoefficienterne typisk vilkårligt. Når kodningskoefficienterne er valgt, bliver det store spørgsmål så, hvordan dekodningen skal ske for at frembringe de oprindelige beskeder. I praksis foregår dette ved at lade beskederne

$$\mathbf{X} = (1, 0, \ldots, 0), \mathbf{X} = (0, 1, 0, \ldots, 0), \ldots, \mathbf{X} = (0, \ldots, 0, 1),$$

gennemløbe netværket. Det bemærkes, at disse svarer til de globale kodningsvektorer defineret i 5.5, hvorfor der er så mange beskeder, som der er modtagere i netværket. På denne måde får hver modtager blot den besked, der er sendt igennem netværket. Hvis og kun hvis hver modtager får en samling af globale kodningsvektorer, som udspænder hele $\mathbb{F}_q^h$, så er det muligt at vælge dekodningskoefficienter $b_{i,j}^{(r)}$ sådan, at en løsning til netværkskodningsproblemet haves. Det følgende afsnit omhandler sandsynligheden for, at vilkårligt valgte kodningskoefficienter gør det muligt at bestemme dekodningskoefficienter, sådan at netværket virker. Denne sandsynlighed noteres P_{succ} jvf. notationen anvendt i [2010 Geil & Thomsen]. Ved at anvende korollar 5.1 fås nedenstående sætning.

Sætning 5.5. *Betragt et løseligt netværkskodningsproblem, hvor nogle kodningskoefficienter er valgt på forhånd, sådan at de er en del af løsningen til problemet. Lad η være antallet af vilkårligt valgte kodningskoefficienter over $\mathbb{F}_q$. Hvis $q \geq |R|$, gælder*

$$P_{succ} \geq P_{Ho0} := \left(\frac{q - |R|}{q}\right)^{\eta}. \tag{5.17}$$

Bevis. Lad $p_{transfer} = \prod_{r \in R} \det M^{(r)}$ være transferpolynomiet for et løseligt netværkskodningsproblem med variable $a_{i,j}$, $f_{i,j}$ og $b_{i,j}^{(r)}$. Indsæt de på forhånd valgte kodningskoefficienter og supplér op med de vilkårligt valgte. Dekodningskoefficienterne betragtes da som værende konstanter, sådan at $p_{transfer} \in \mathbb{F}_q[y_1, \ldots, y_\omega]$, hvor $y_1, \ldots, y_\omega$ repræsenterer dekodningskoefficienterne. Denne udgave af transferpolynomiet kaldes for *a priori transferpolynomiet*, og polynomiet har η variable med eksponenter mindre end eller lig $|R|$.

Bemærk at de vilkårligt valgte kodningskoefficienter kan vælges på i alt q^η måder. Ifølge korollar 5.1 fås, at for mindst $(q - |R|)^\eta$ af de i alt q^η muligheder, at transferpolynomiet bliver forskelligt fra nul. Ergo er sandsynligheden for succes større end

$$\frac{q - |R|^\eta}{q^\eta}.$$

□

Antag at en monomiel ordning er valgt, og at det førende monomium i a priori transferpolynomiet

er $x_1^{i_1} \cdots x_m^{i_m}$. Da kan grænsen i 5.5 forbedres således, at

$$P_{succ} \geq P_{FP1} := \min \left\{ \prod_{j=1}^{m} \frac{q - i_1}{q} \mid x_1^{i_1} \cdots x_m^{i_m} \text{ monomium i transferpolynomiet} \right\}. \tag{5.18}$$

Hvis til gengæld kun transferpolynomiet kendes, og det ledende monomium er ukendt, da fås den lidt svagere grænse

$$P_{succ} \geq P_{FP2} := \prod_{j=1}^{m} \frac{q - i_1}{q}. \tag{5.19}$$

Forkortelsen FP i ovenstående udtryk refererer til fodaftrykket (på engelsk: Footprint). Grænsen fra udtrykket i (5.17) er ikke så god som dem i (5.18) og (5.19), men til gengæld er den relativt nem at udregne, hvor P_{FP1} og P_{FP2} er mere komplicerede udtryk. Det er endog muligt at forbedre grænsen i (5.17) uden at komplicere udregningerne. Til dette behøves følgende lemma:

Lemma 5.2. *Lad k være et legeme, som indeholder $\mathbb{F}_q$, og tag polynomium $f \in k[x_1, \ldots, x_n]$ forskelligt fra nul, hvor alle monomier $x_1^{j_1} \cdots x_m^{j_m}$ i støtten til f opfylder, at*

(i) $j_1, \ldots, j_m \leq d$, hvor d er et helt tal mindre end eller lig q.

(ii) $j_1 + \ldots + j_m \leq dN$ for et helt tal $N \leq m$.

Antag envidere, at $(x_1, \cdots, x_m) \in \mathbb{F}_q^m$ er valgt vilkårligt. Sandsynligheden for at $f(x_1, \ldots, x_m) \neq 0$ er da mindst

$$\left(\frac{q - d}{q} \right)^N. \tag{5.20}$$

Bevis. Målet er at bestemme en minimumsværdi for

$$\prod_{t=1}^{m} \left(\frac{q - j_t}{q} \right)$$

taget over alle mulige valg for $j_1, \ldots, j_m$, således at de to betingelser (i) og (ii) er overholdt. Først indses, at uligheden

$$(q - x)(q - y) > (q - (x + 1))(q - (y - 1)) \tag{5.21}$$

er sand, når $x \geq y$. Antag at $j_1, \ldots, j_m$ er valgt, sådan at udtrykket i (5.20) har mindste værdi. Da er ligheden i (ii) trivielt opfyldt. Antag nu uden tab af generalitet, at $j_1 \geq \ldots \geq j_m$. Ved at anvende påstanden fra (5.21) fås, at $j_1 = \cdots = j_N = d$ og $j_{N+1} = \cdots = j_m = 0$. Lemmaet er hermed bevist. □

Lad nu η' være det maksimale antal kanter i et flow, hvor kun nogle $a_{i,j}$ eller $f_{i,j}$ er valgt vilkårligt. Lad endvidere maksimum være taget i forhold til alle modtagere $r \in R$ og alle flows af størrelsen h til r. Hvis ingen kodningskoefficienter er valgt a priori, så er η' det maksimale antal kanter i et flow til en modtager i netværket. Antallet af kodningskoefficienter i monomiet hørende til et flow

er da η'. I og med at et flowsystem består af $|R|$ flows, så opfylder a priori transferpolynomiet betingelserne (i) og (ii) i lemma 5.2 med $d = |R|$ og $N = \eta'$. Dette giver, at

$$P_{succ} \geq P_{Ho2} := \left(\frac{q - |R|}{q}\right)^{\eta'}.$$

Antallet af kanter i et flow er tydeligvis højst lig antal kanter i et netværk. Derfor fås endvidere, at

$$P_{succ} \geq P_{Ho1} := \left(\frac{q - |R|}{q}\right)^{\eta''},$$

hvor η'' er antallet af kanter j i E, sådan at nogle $a_{i,j}$ eller $f_{i,j}$ ej er valgt på forhånd. I det tilfælde, hvor absolut ingen $a_{i,j}$ eller $f_{i,j}$ er valgt på forhånd, er $\eta'' = |E|$. Samles alle grænser opnås følgende sætning:

Sætning 5.6.

$$P_{Ho0} \leq P_{Ho1} \leq P_{Ho2} \leq P_{FP1} \leq P_{FP2} \leq P_{succ}.$$

Det bemærkes, at for at kunne benytte de to grænser P_{FP1} og P_{FP2} kræver det en viden om transferpolynomiet.

Principperne i lineær netværkskodning er blevet beskrevet, og der er givet kriterier til afgørelse for, hvornår et lineært netværkskodningsproblem er løseligt. Desuden er det vist, hvordan en løsning findes, og afslutningsvist er det blevet vist, at selvom kodningskoefficienterne i et multicast netværkskodningsproblem er valgt tilfældigt, så kan man med en vis sandsynlighed garantere en løsning til problemet.

Litteratur

[2010 Geil & Thomsen] *Aspects of random network coding*, Olav Geil & Casper Thomsen, Aalborg University 2010.

[2008 Cox, Little & O´Shea] *Ideals, Varieties and Algorithms*, 3. udgave, David Cox, John Little & Donal O´Shea, 2008 Springer, 978-0-387-35650-1

[2006 Lay] *Linear Algebra and Its Applications*, 3. udgave, David C. Lay, 2006 Pearson, 0-321-31485-9

[2006 T. Ho et al.] *A random linear network coding approach to multicast*, T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi og B. Leong , Trans. Inform. Theory, nr. 52, 2006

[2005 S. Jaggi et al.] *Polynomial time algorithms for multicast network code construction*, S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain og L. M. G. M. Tolhuizen, Trans. Inform. Theory, nr. 51, 2005

[2003 Lauritzen] *Concrete Abstract Algebra - From numbers to Gröbnerbases*, Niels Lauritzen, Cambridge University Press 2003, 0-521-53410-0

[2008 Greuel & Pfister] *A Singular Introduction to Commutative Algebra*, 2. udgave, Gert-Martin Greuel & Martin Pfister, Springer 2008, 3540735410

[2006 R. W. Yeung et al.] *Network Coding Theory*, R. W. Yeung, S.-Y. R. Li, N. Cai & Z. Zhang, Now Publishers Inc. 2006, 1-933019-24-7

[2000 Justesen & Høholdt] A Course in Error-correcting Codes, Jørn Justesen & Tom Høholdt, 2000 European Mathematical Society, 3-03719-001-9