Algebraisk Netværkskodning

Gröbner-Baser og Deres Anvendelse i Netværkskodning **&** *Fejlkorrigerende Netværkskodning*

af

Maria Simonsen & Majken Svendsen

Specialeafhandling i Anvendt Matematik

(Master Thesis in Applied Mathematics)

Vejleder: Olav Geil

Institut for Matematiske fag
Aalborg Universitet

Juni 2012

AALBORG UNIVERSITY
Institut for Matematiske fag I-17
Fredrik Bajers Vej 7G
9220 Aalborg Øst
http://www.math.aau.dk/

Titel:
Algebraisk Netværkskodning
- Gröbner-Baser og Deres Anvendelse i Netværkskodning & Fejlkorrigerende Netværkskodning

Title:
Algebraic Network Coding
- Application of Gröbner bases in Network Coding & Error Correcting Network Coding

Emneområde:
Netværkskodning

Projektperiode:
Forår 2012

Projektgruppe:
G4-102d

Medlemmer:

Maria Simonsen

Majken Svendsen

Vejleder:
Olav Geil

Antal printet kopier: 5.

Antal sider: 151.

Afsluttet: 1. juni 2012.

Synopsis:

Denne specialeafhandling benytter algebraisk netværkskodning til at undersøge muligheden for at optimere transmissionen af data i et netværk, og til at konstruere koder som er velegnet til fejlkorrigering. Gröbner-basis teori anvendes i første del til at fastsætte eksistensen af en løsning til et givent netværkskodningsproblem og til at undersøge sandsynligheden for at finde en løsning til et vilkårligt netværkskodningsproblem. I anden del af rapporten præsenterer vi først KK-koden som kan fejlkorrigere ved hjælp af en minimumsafstandsdekoder. Denne kode når tilnærmelsesvis Singleton Grænsen. Efterfølgende modificeres KK-koden til MV-koden som kan fejlkorrigere ved liste-L-dekodning. Vi ser at MV-koden har en bedre fejlretningsevne end KK-koden ved lave pakkehastigheder. Begge koder er konstrueret over ringen af lineariserede polynomier, hvorfor vi også præsenterer teori vedrørende disse.

Abstract

The content of this project is based on Algebraic Network Coding. We are looking into two main areas within this topic; The option to transmit multiple message at the same time to multiple receivers and the option to transmit information through a network without knowing the topology of the network.

In the first part of the report Gröbner base theory is presented. One of the main results here is Buchbergers Algorithm which constructs a Gröbner basis from a basis for an ideal. Another important result is the footprint bound, which gives the number of non-zeros for a polynomial in the finite field $\mathbb{F}_q^n$. We use this theory to bound the success probability of finding a solution to the multicast network coding problem when the network uses random network coding.

In chapter 3 we define the network coding problem. First we look into the multicast case. Here we show that the multicast network coding problem has a solution if and only if the corresponding transition polynomial is non-zero. The transition polynomial is based on the topology of the network, which means, that we here require knowledge about this. For the general network coding problem we show that there exists a solution if and only if the variety of the ideal of the network coding problem is non-empty. Also this is based on knowledge about the topology of the network.

In the second part of the report the focus is error correcting subspace codes. We present the KK-code and a modification of this; the MV-code. These codes are able to correct a number of errors and erasures which happens in the communication channel. In this part of the report the communication channel is called the operator channel. We consider the operator channel as a black box based on the fact, that the topology of the network is unknown. The KK-code and MV-code are constructed over the ring of linearized polynomials over the finite fields $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ respectively, so in chapter 5 we present this theory in detail.

To decode a received subspace from the KK-code we use a minimum distance decoder. This is able to correct up to half of the codes minimum distance and furthermore the information rate of the KK-code almost achieves the Singleton Bound. This is shown in chapter 7.

The MV-codes are decoded with a list-L-decoder. This means, that given a received subspace from the MV-code, the decoder constructs a list of size maximum L of possible transmitted subspaces.

In the last part of chapter 9 a comparison of the minimum distance decoder and the list-L-decoder is made. The minimum distance decoder gives the same package rate for the KK-kode and the MV-code. When list-L-decoding is used to decode MV-codes, they have a better error correction ability than the KK-code for low package rates, so depending on the requirement you can choose to decode the MV-code with the minimum distance decoder or

the list-L-decoder.

The report includes also a number of examples, which are intended to illustrate the presented theory and give the reader a better understanding of introduced methods.

Forord

Denne specialeafhandling er udarbejdet på Aalborg Universitet, forår semestret 2012, på Institut for Matematiske Fag indenfor hovedretningen Anvendt Matematik under vejledning af Olav Geil. Udgangspunktet for projektet er artiklerne "Aspects of Random Network Coding" af Olav Geil og Casper Thomsen, "Coding for Errors and Erasures in Random Network Coding" af Ralf Kötter og Frank R. Kschischang samt "Algebraic List-Decoding of Subspace Codes" af Hessam Mahdavifar og Alexander Vardy.

Det forudsættes at læseren har kendskab til abstrakt algebra, lineær algebra og grafteori.

Litteraturhenvisninger er angivet [XXYY,ZZ], hvor XX er baseret på forfatter(e), YY er årstallet for udgivelsen og ZZ informerer om hvor henvisningen kan findes i litteraturen. Litteraturlisten er at finde bagerst i rapporten før bilag. Når der henvises til sætninger, definitioner og lignende benyttes formuleringen "sætning 2.14" mens henvisninger til ligninger er angivet i parentes; (3.6).

Vi har i projektforløbet benyttet matematikprogrammerne Maple til konstruktion af figurer og eksempler.

Maria Simonsen & Majken Svendsen
Aalborg 31.05.2012

Indhold

Kapitel 1

Algebraisk Netværkskodning

Netværkskodning er en metode til at optimere transmissionen af data i et netværk. Idéen er at opdele det data som sendes ind i netværket i flere pakker, som så har mulighed for at tage forskellige veje fra kilden til destinationen. Undervejs i netværket kan der ske utilsigtede ændringer i nogle af pakkerne, som måske forårsager fejl i det data som modtages ved destinationen. Dog, hvis blot tilstrækkeligt mange pakker modtages med korrekt data, så kan modtageren udlede det originale data fra de pakker som er modtaget. Fordele ved netværkskodning fremfor routing er muligheden for fejlkorrigering, kapacitetsoptimering og i nogle tilfælde også minimering af omkostningerne. Til gengæld kan en ulempe være øget forsinkelse af data.

I dette projekt har vi specielt fokuseret på algebraisk netværkskodning. Her kan polynomier bruges til at beskrive netværkets topologi, og ud fra disse kan løsninger til et netværkskodningsproblem, samt sandsynligheder for løsninger til netværkskodningsproblemer bestemmes. Desuden giver algebraisk netværkskodning også mulighed for at fejlkorrigere information transmitteret gennem et netværk, selv i situationer hvor vi ikke har kendskab til netværkets topologi.

I første del af rapporten er netværkskodning anvendt til at optimere transmissionen af information gennem et netværk således at netværkets kapacitet øges. Netværkskodning er udnyttet til at sende flere informationsbeskeder til flere modtagere på en gang. Her transmitteres informationen gennem netværket som vektorer bestående af bits. Vi betragter specielt multicast netværkskodningsproblemet i kapitel 3, mens det generelle netværkskodningsproblem gennemgås i kapitel 4. Gröbner-basis teori benyttes

til at fastsætte, hvorvidt der findes en løsning i et givent netværkskodningsproblem. Desuden, hvis det vides at der findes en løsning til et netværkskodningsproblem, så kan Gröbner-basis teorien anvendes til at undersøge sandsynligheden for at finde en løsning ved vilkårlig netværkskodning.

I anden del af rapporten er fokus flyttet til fejlkorrigering. Vi betragter ikke længere netværkets topologi, men i stedet for koncentrerer vi os om at konstruere koder som er velegnet til fejlkorrigering. Det vil sige koder hvis kodeord sendes gennem et netværk, der udfører vilkårlig netværkskodning og ved modtageren kan dekodes til det oprindelige afsendte kodeord. Her består den afsendte information(kodeord) af underrum af et vektorrum. I dette tilfælde er vi kun i stand til at sende én informationsbesked ad gangen gennem netværket i modsætning til første del af rapporten.

1.1 Læsevejledning

Der er i rapporten løbende inkluderet eksempler. Formålet med disse er primært at illustrere den gennemgåede teori, men også at give læseren en mere konkret indsigt i og forståelse for aspekterne ved de beskrevne metoder.

1.1.1 Begrebsforståelse

Fortløbende gennem rapporten benyttes forskellige betegnelser for det samme. For at afhjælpe forvirring med hensyn til læserens forståelse opsummeres her kort hvilke begreber som omtales på flere måder.

Når vi i kapitel 3 og 4 snakker om "multicast netværket" og "det generelle netværk" så er det underforstået at vi henviser til hhv. multicast netværkskodningsproblemet og det generelle netværkskodningsproblem.

Den information som transmitteres gennem et netværk bliver løbende udtryk ved forskellige begreber. Betegnelsen "beskeder" benyttes i tilfælde hvor det ønskes at sende forskellig information evt. til forskellige og/eller samme modtagere. Når det kun er muligt at sende den samme information ind i netværket betegnes den afsendte information som kodeord.

1.1.2 Legemer

Fortløbende gennem dette projekt benyttes forskellige legemer uden yderligere forklaring. Når det er tale om et vilkårligt legeme benyttes betegnelsen

$\mathbb{F}$, mens et endeligt legeme betegnes $\mathbb{F}_q$. Notationen $\mathbb{F}_q^n$ betegner vektorrummet bestående af alle n-tupler over det endelige legeme $\mathbb{F}_q$. Ved notationen $\mathbb{F}_q[\mathbf{x}]$ betegnes altid mængden af polynomier afhængig af $\mathbf{x} = (x_1, \ldots, x_n)$ med koefficienter i $\mathbb{F}_q$. I visse tilfælde er vi interesseret i antallet af nulpunkter for et polynomium indeholdt i et givent legeme. Der findes polynomier uden nulpunkter i et legeme, hvilket følgende eksempel illustrerer.

Eksempel 1.1. Betragt $f = x_1^2x_2 + x_1x_2 + 1 \in \mathbb{F}_2[x_1, x_2]$. Polynomiet f har ingen nulpunkter i $\mathbb{F}_2^2$ da

$$\begin{aligned} f(0,0) &= 0^2 \cdot 0 + 0 \cdot 0 + 1 = 1 \\ f(1,0) &= 1^2 \cdot 0 + 1 \cdot 0 + 1 = 1 \\ f(0,1) &= 0^2 \cdot 1 + 0 \cdot 1 + 1 = 1 \\ f(1,1) &= 1^2 \cdot 1 + 1 \cdot 1 + 1 = 1 \end{aligned}$$

▲

En måde at sikre sig at ethvert polynomium har et nulpunkt er ved at udvidede legemet. Til dette formål defineres den algebraiske aflukning.

Definition 1.2 (Algebraisk aflukning)**.** Et legeme $\mathbb{F}$ siges at være algebraisk aflukket, hvis ethvert polynomium af grad 1 eller højere i $\mathbb{F}[\mathbf{x}]$ har en rod i $\mathbb{F}$. Den algebraiske aflukning af et legeme $\mathbb{F}$ skrives $\overline{\mathbb{F}}$. [Lan02, s.231]

Eksempel 1.3. Der ses på legemet $\mathbb{F} = \mathbb{R}$, hvor $\mathbb{R}$ er de reelle tal, og polynomiet $f(x) = x^2 + 1$, som ingen rod har i $\mathbb{R}$. Det er derfor nødvendigt at udvide $\mathbb{R}$ til et legeme der indeholder en rod for $f(x)$. Den algebraiske aflukning af $\mathbb{R}$ bliver herved de komplekse tal $\mathbb{C}$. ▲

Del I

Gröbner - Baser og Deres Anvendelse i Netværkskodning

I denne del undersøges hvorledes netværkskodning kan benyttes til at transmittere information til flere modtagere på en gang. Her betragtes altid transmissioner der benytter lineær netværkskodning. Dette betyder at informationen består af elementer fra et endeligt legeme $\mathbb{F}_q$, samt at kodningen igennem netværket kun består af lineære operationer over legemet $\mathbb{F}_q$. Herudover betragtes der kun støjfrie kanaler, hvilket vil sige, at der ikke tilføres fejlinformation til det afsendte data. Desuden er der heller ikke mulighed for at genskabe tabt information, altså tilstræber vi at foretage netværkskodning hvor sletninger undgås. Det vil sige at fejlkorrigering ikke er tilknyttet netværkskodningen i denne del af rapporten. De efterfølgende kapitler anvendes i stedet til at definere samt forstå grundbegreber og metoder indenfor netværkskodningsproblemet både for multicast og generelle netværker.

Som forarbejde til netværkskodningen betragtes Gröbner-baser og egenskaber for disse i kapitel 2. I Gröbner-basis teori er Buchbergers Algoritme og Fodaftryksgrænsen de vigtigste resultater. Fodaftryksgrænsen angiver det mindst mulige antal af ikke-nulpunkter som et polynomium kan have i $\mathbb{F}_q^n$, hvor $\mathbb{F}_q$ er et endeligt legeme, mens Buchbergers Algoritme anvendes til bestemme Gröbner-baser for idealer. Disse to resultater kan bruges til at afgøre hvornår en løsning til et netværkskodningsproblem eksisterer.

I kapitel 3 betragter vi primært multicast netværkskodningsproblemet, men her defineres også grundlæggende begreber anvendt i netværkskodning. Disse vil også optræde i kapitel 4, hvor det generelle netværkskodningsproblem betragtes. Fælles for multicast netværkskodningsproblemet og det generelle netværkskodningsproblem er at kun forsinkelsesfrie samt kredsfrie netværker betragtes.

Kapitel 2

Gröbner-Baser

I dette kapitel defineres en Gröbner-basis samt dens egenskaber. Desuden betragtes varieteten af et ideal og størrelsen af denne. Fortløbende gennem kapitlet benyttes bagvedliggende teori og resultater fra algebra, disse forefindes i bilag A og B.

Det at bestemme en Gröbner-basis kan være en omstændig proces, men Buchberger har konstrueret en algoritme som kan udvide enhver mængde af polynomier til en Gröbner-basis. Vi vil i kapitel 4 anvende denne algoritme. Her bliver Gröbner-baser benyttet til løsning af det generelle netværkskodningsproblem. Ved hjælp af Hilberts Nullstellensatz vedrørende varieteten af et ideal og Gröbner-basen hørende til dette, afgøres om et givent netværkskodningsproblem har en løsning.

2.1 Gröbner-Basis

Givet et ideal er det altid muligt at bestemme en Gröbner-basis som frembringer idealet. Definitionen af en Gröbner-basis er baseret på egenskaber for et ideal af ledende led.

Definition 2.1 (Ideal af Ledende Led)**.** Lad $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ være et ideal $\mathbf{I} \neq \{0\}$.

(i) Mængden af ledende led af elementerne i $\mathbf{I}$ betegnes ved $\mathrm{LT}(\mathbf{I})$, hvor

$$\mathrm{LT}(\mathbf{I}) = \{c \cdot \mathbf{x}^{\alpha} | \text{ der findes et } f \in \mathbf{I} \text{ hvor } \mathrm{LT}(f) = c \cdot \mathbf{x}^{\alpha}\} .$$

(ii) Idealet frembragt af elementerne i $\mathrm{LT}(\mathbf{I})$ betegnes ved $\langle \mathrm{LT}(\mathbf{I}) \rangle$.

[CLO92, s.75]

Følgende eksempel bestemmer mængden af ledende led for et konkret ideal.

Eksempel 2.2. Lad $\mathbf{I} = \langle x + 2y, 3y^2 + z, y^2 \rangle \subset \mathbb{F}[x, y, z]$ hvor $x >_{\text{leks}} y >_{\text{leks}} z$.[1] For at bestemme LT($\mathbf{I}$) vælges et $f \in \mathbf{I}$, som er givet ved

$$\begin{aligned} f &= a(x + 2y) + b(3y^2 + z) + cy^2 \\ &= ax + (3b + c)y^2 + 2ay + bz \ , \end{aligned}$$

hvor $a, b, c \in \mathbb{F}[x, y, z]$. Alt efter om a, b, c er nulpolynomier eller ej opnås forskellige ledende led for f. Hvis $a \neq 0$ og $b, c = 0$ fås at $\text{LT}(f) = \text{LT}(a)x$. I tabel 2.1 ses de ledende led for alle mulige tilfælde. Desuden illustrerer tabellen, at der ikke findes monomier med mindre grad end de angivne, som kan være ledende led for en funktion $f \in \mathbf{I}$. Bemærk specielt at i de tilfælde

	LT(f)
$a \neq 0, b, c = 0$	LT(a)x
$b \neq 0, a, c = 0$	LT($3b$)y^2
$c \neq 0, a, b = 0$	LT(c)y^2
$a, b \neq 0, c = 0$	LT($ax + 3by^2$)
$b, c \neq 0, a = 0$	LT($(3b + c)y^2 + bz$)
$a, c \neq 0, b = 0$	LT($ax + cy^2$)
$a, b, c \neq 0$	LT($ax + (3b + c)y^2 + bz$)

Tabel 2.1: Mulige ledende led af $f \in \mathbf{I}$.

hvor $3b + c = 0$ for $b, c \neq 0$ og $a = 0$ fås at det ledende led af f er LT(b)z. Samlet giver dette at mængden af ledende led af elementer i $\mathbf{I}$ er givet ved

$$\text{LT}(\mathbf{I}) = \{d_1 x, d_2 y^2, d_3 z | d_1, d_2, d_3 \text{ er monomier i } \mathbb{F}[x, y, z]\} \ .$$

Idealet som frembringer LT($\mathbf{I}$) er derfor givet ved $\langle x, y^2, z \rangle \subset \mathbb{F}[x, y, z]$. ▲

Bemærkning 2.3. Metoden, som er anvendt i eksempel 2.2, er generelt ikke en velegnet metode til at bestemme de ledende led af et ideal. Den primære grund til succes i det ovenstående er, at polynomierne som frembringer $\mathbf{I}$ indeholder få led, og vi kan derfor hurtigt udtømme alle mulige tilfælde.

Ved at indføre Gröbner-baser opnår vi en lettere metode til at løse ovenstående problem, da en frembringende mængde for $\mathbf{I}$, som er en Gröbner-basis, har den egenskab, at LT($\mathbf{I}$) kan aflæses direkte.

[1] Se bilag A.1 for definition af den Leksikografiske orden.

Definition 2.4 (Gröbner-basis)**.** Lad en monomiel ordning være givet og lad $\mathbf{I}$ være et ideal. En endelig delmængde $G = \{g_1, \ldots, g_t\}$ er en Gröbner-basis for $\mathbf{I}$ hvis

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

[CLO92, s.77]

En given basis, som opfylder definition 2.4, er ikke nødvendigvis den mindste eller mest optimale Gröbner-basis for det frembringende ideal, hvilket følgende eksempel illustrerer.

Eksempel 2.5. Lad $G = \{x, y-z, z^3+z, y^3+z\}$ være en Gröbner-basis for $\mathbf{I}$ hvor $x >_{\text{leks}} y >_{\text{leks}} z$.[2] Da G er en Gröbner-basis er definition 2.4 opfyldt, og derfor gælder at

$$\langle \mathrm{LT}(\mathbf{I}) \rangle = \Big\langle \mathrm{LT}(x), \mathrm{LT}(y-z), \mathrm{LT}(z^3+z), \mathrm{LT}(y^3+z) \Big\rangle = \Big\langle x, y, z^3, y^3 \Big\rangle \ .$$

Bemærk at $\mathrm{LT}(y^3+z) = y^3 = y^2 \cdot y = y^2 \,\mathrm{LT}(y-z) \in \langle x, y, z^3 \rangle$. Så idealet frembragt af de ledende led af G kan derfor frembringes af den mindre mængde, hvorfor $\langle \mathrm{LT}(\mathbf{I}) \rangle = \langle x, y, z^3 \rangle$. Ligeledes kan G reduceres til $G' = G - \{y^3+z\}$, og samtidig forblive en Gröbner-basis da G' også opfylder definition 2.4 for $\mathbf{I}$.

$$\langle \mathrm{LT}(G') \rangle = \Big\langle x, y, z^3 \Big\rangle = \langle \mathrm{LT}(\mathbf{I}) \rangle \ .$$

Desuden gælder at polynomiet y^3+z kan frembringes af elementerne i G';

$$\begin{aligned} & 0 \cdot x + (y^2 + yz + z^2) \cdot (y-z) + 1 \cdot (z^3+z) \\ = \ & y^3 - y^2 z + y^2 z - y z^2 + y z^2 - z^3 + z^3 + z \\ = \ & y^3 + z \ . \end{aligned}$$

Mængden G' er heraf en ny Gröbner-basis for $\mathbf{I}$. ▲

Der gælder generelt, at G' fra ovenstående eksempel er en Gröbner-basis ses i det næste lemma.

Lemma 2.6. *Lad G være en Gröbner-basis for et ideal $\mathbf{I}$. Lad $p \in G$ være et polynomium hvorom der gælder, at $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$. Da er $G - \{p\}$ også en Gröbner-basis. [CLO92, s.91]*

Bevis. Da G er en Gröbner-basis gælder at

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(\mathbf{I}) \rangle \ . \tag{2.1}$$

Hvis $\mathrm{LT}(p) \in \langle \mathrm{LT}(G - \{p\}) \rangle$ så gælder at $\langle \mathrm{LT}(G - \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle$. Fra (2.1) og definition 2.4 følger at $G - \{p\}$ er en Gröbner-basis. □

[2] Ved anvendelse af algoritme 1 fra afsnit 2.3 ses at G er en Gröbner-basis.

En reduceret Gröbner-basis kan derfor defineres.

Definition 2.7 (Reduceret Gröbner-basis)**.** En reduceret Gröbner-basis for et ideal $\mathbf{I}$ er en Gröbner-basis G for $\mathbf{I}$, hvorom der gælder at

(*i*) $\mathrm{LC}(p) = 1$ for alle $p \in G$.

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

[CLO92, s.92]

Senere i kapitlet præsenteres Buchbergers algoritme, som konstruerer Gröbner-baser. Disse baser kan være vilkårligt store, så i visse tilfælde ville det være praktisk at kunne reducere den konstruerede basis. Næste afsnit danner baggrund for Buchbergers algoritme.

2.2 Metode til Konstruktion af Gröbner-Baser

Lad i det følgende afsnit et ideal $\mathbf{I} = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}[\mathbf{x}]$ være givet, hvor $F = \{f_1, \ldots, f_s\}$ ikke er en Gröbner-basis. Det vil sige at der findes minimum et monomium a, hvorom der gælder, at $a \in \langle \mathrm{LT}(\mathbf{I}) \rangle$, men $a \notin \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s) \rangle$. Hvis F skal udvides til en Gröbner-basis for $\mathbf{I}$ er det nødvendigt, at ethvert monomium i $\langle \mathrm{LT}(\mathbf{I}) \rangle$ også ligger i $\langle \mathrm{LT}(F) \rangle$. Vi har altså brug for at kunne tilføje polynomier til F med egenskaben, at deres ledende led er dem, der mangler for at $\langle \mathrm{LT}(\mathbf{I}) \rangle = \langle \mathrm{LT}(F) \rangle$, hvormed F opfylder definition 2.4. Følgende definition af S-polynomier giver en metode til at "finde" de manglende ledende led i en basis F, således at F kan udvides til en Gröbner-basis.

Definition 2.8 (S-polynomium)**.** Lad $f, g \in \mathbb{F}[\mathbf{x}]$ være ikke-nulpolynomier.

(*i*) Hvis $\mathrm{multigrad}(f) = \alpha$ og $\mathrm{multigrad}(g) = \beta$ så lad $\gamma = (\gamma_1, \ldots, \gamma_n)$, hvor $\gamma_i = \max\{\alpha_i, \beta_i\}$ for $i \in \{1, \ldots, n\}$. Det mindste fælles multiplum af $\mathrm{LM}(f)$ og $\mathrm{LM}(g)$ betegnes $\mathbf{x}^\gamma$ og skrives $\mathbf{x}^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

(*ii*) S-polynomiet af f og g er givet ved

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

[CLO92, s.97]

Polynomiet $S(f,g)$ er et polynomium, som har den egenskab, at det frembringes af polynomierne f og g, men det indeholder hverken det ledende led fra f eller g. Følgende er et eksempel på hvorledes et S-polynomium konstrueres.

Eksempel 2.9. Lad $f,g \in \mathbb{F}[x,y,z]$ med den monomielle ordning $x >_{\text{leks}} y >_{\text{leks}} z$, hvor $f(x,y,z) = 5x^3z+x^2y+z^3$ og $g(x,y,z) = xy^2+z$. Det mindste fælles multiplum af $\text{LM}(f)$ og $\text{LM}(g)$ er givet ved $\text{lcm}(x^3z, xy^2) = x^3y^2z$, hvorfor S-polynomiet bliver

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

Bemærk at $\text{LM}(S(f,g)) = x^2y^3$ hvilket er forskellig fra $\text{LM}(f) = x^3z$ og $\text{LM}(g) = xy^2$. S-polynomiet har derfor den ønskede egenskab. ▲

Selvom $S(f,g)$ ikke indeholder det ledende led fra $f,g \in F$ kan $S(f,g)$ muligvis godt indeholde ledende monomier fra andre polynomier i den førnævnte basis F. Desuden kan det ledende monomium i $S(f,g)$ også være et multiplum af allerede eksisterende ledende monomier i F. Vi ønsker derfor at kunne reducere S-polynomiet yderligere før det tilføjes til F, således at det ledende monomium af det polynomium som tilføjes F ikke er et multiplum af nogen af de ledende monomier, som allerede findes i F. Til at reducere S-polynomiet anvendes divisionsalgoritmen fra bilag B.1. Vi definerer derfor resten ved division.

Definition 2.10. Lad F være en mængde af polynomier i $\mathbb{F}[x,y,z]$ og lad $f \in \mathbb{F}[x,y,z]$. Resten af f ved division med F betegnes $\overline{f}^F$.

I eksempel 2.9 blev S-polynomiet af f og g konstrueret. Dette kan dog reduceres yderligere ved division med g, da $\text{LM}(S(f,g)) = x^2y^3 = xy \cdot \text{LM}(g)$. Resten ved division af $S(f,g)$ med f og g giver et nyt polynomium som bestemmes følgende;

Eksempel 2.11 (Fortsættelse af eksempel 2.9)**.** Lad $F = \{f,g\}$ fra eksempel 2.9. Resten af S-polynimiet $S(f,g)$ ved division med F udregnes ved hjælp af divisionsalgoritmen (jævnfør algoritme 6);

$$\overline{S(f,g)}^F = -x^2z^2 - \frac{1}{5}xyz + \frac{1}{5}y^2z^3 \ .$$

Det ses heraf, at $\text{LT}(\overline{S(f,g)}^F)) \notin \langle \text{LT}(f), \text{LT}(g) \rangle$. Resten giver derfor mulighed for at udvide F, således at F stadig er en basis for $\mathbf{I}$ og samtidig er tættere på at opfylde definitionen for at være en Gröbner-basis. ▲

Når en basis F for idealet $\mathbf{I}$ er blevet udvidet tilstrækkeligt, således at udvidelsen er en Gröbner-basis G, opnås entydighed ved division med G. Følgende proposition udtaler sig om dette.

Proposition 2.12. *Lad $G = \{g_1, \ldots, g_t\}$ være en Gröbner-basis for et ideal $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ og lad $f \in \mathbb{F}[\mathbf{x}]$. Der eksisterer et entydigt $r \in \mathbb{F}[\mathbf{x}]$ med følgende egenskaber;*

(*i*) *Intet led i r er dividerbart med* $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.

(*ii*) *Der findes et $g \in \mathbf{I}$ således at $f = g + r$.*

Specielt gælder at r er resten ved division af f med G ved anvendelse af divisionsalgoritmen, algoritme 6, uanset divisionsrækkefølgen af elementerne i G. [CLO92, s.82]

Bevis. Anvendes divisionsalgoritmen, algoritme 6 fra bilag B, på f ved division med G haves, at $f = a_1 g_1 + \cdots + a_t g_t + r$. Sætning B.1 giver at r opfylder (*i*). Ved at vælge $g = a_1 g_1 + \cdots + a_t g_t$ fås at $g \in \mathbf{I}$ og at $f = g + r$, hvorfor (*ii*) er opfyldt. Eksistensen af r er derfor opfyldt.

Antag at $f = g + r = g' + r'$ opfylder (*i*) og (*ii*) og antag modsætningsvist at $r \neq r'$. Så gælder at $r - r' = g' - g$ er indeholdt i $\mathbf{I}$ og derfor at $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(\mathbf{I}) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle$. Da $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$ frembringer alle elementer i $\langle \mathrm{LT}(\mathbf{I}) \rangle$, og da $\mathrm{LT}(r - r')$ er et monomium gælder, at $\mathrm{LT}(r - r')$ er dividerbar med mindst et af $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$. Dette er dog ikke muligt da hverken r eller r' er dividerbar med nogen af $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$, hvorfor $r - r' = 0$. Dette er en modstrid med antagelsen og resten r er derfor entydig. □

Entydigheden ved division med en Gröbner-basis G kan udnyttes til at afgøre om et givent polynomium er indeholdt i idealet frembragt af G.

Korollar 2.13. *Lad $G = \{g_1, \ldots, g_t\}$ være en Gröbner-basis for et ideal $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ og lad $f \in \mathbb{F}[\mathbf{x}]$. Da gælder at $f \in \mathbf{I}$ hvis og kun hvis resten ved division af f med G er nul. [CLO92, s.82]*

Bevis. Antag at $f \in \mathbf{I}$. Så haves at $f = f + 0$ opfylder begge egenskaber i proposition 2.12. Herved er resten af f ved division med G lig nul. Antag omvendt at resten ved division af f med G er lig nul. Så følger direkte af proposion 2.12 (*ii*) at $f \in \mathbf{I}$. □

Baseret på det foregående teori indeholder det følgende afsnit Buchbergers algoritme som er velegnet til at konstruere en Gröbner-basis.

2.3 Buchbergers Algoritme

Buchbergers Algoritme tager udgangspunkt i en på forhånd defineret basis for et ideal $\mathbf{I}$. Denne basis udvides løbende i algoritmen, indtil der haves en Gröbner-basis for idealet. For at kunne afgøre hvornår algoritmen har udvidet basen tilstrækkeligt, giver den følgende sætning et kriterium for, hvornår der haves en Gröbner-basis.

Sætning 2.14 (Buchbergers Kriterium)**.** *Lad* $\mathbf{I}$ *være et ideal. En basis* $G = \{g_1, \ldots, g_t\}$ *er en Gröbner-basis for* $\mathbf{I}$ *hvis og kun hvis der for alle par* $i \neq j$ *for* $i, j \in \{1, \ldots, t\}$ *gælder, at resten af* $S(g_i, g_j)$ *ved division med* G *er nul. [CLO92, s.85]*

Bevis. Antag at G er en Gröbner-basis for $\mathbf{I}$. Fra definition 2.8 haves at S-polynomier antager formen $S(g_i, g_j) = a_i g_i + a_j g_j$, hvor $a_i, a_j \in \mathbb{F}[\mathbf{x}]$. Da $g_i, g_j \in \mathbf{I}$ så gælder at $S(g_i, g_j) \in \mathbf{I}$. Fra korollar 2.13 haves derfor, at resten ved division af $S(g_i, g_j)$ med G er nul.

Antag omvendt at alle S-polynomier har en rest på nul ved division med G. Vi ønsker at fastsætte, at G er en Gröbner-basis ved at vise, at definition 2.4 er opfyldt. Da $\mathbf{I}$ frembringes af $g_1, \ldots, g_t$ gælder direkte at $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle \subseteq \langle \mathrm{LT}(\mathbf{I}) \rangle$.

Til at bevise den omvendte inklusion vælges et vilkårligt $f \in \mathbf{I}$ som fastholdes i det følgende. Polynomiet f kan udtrykkes på formen

$$f = \sum_{i=1}^{t} h_i g_i \ , \tag{2.2}$$

hvor $h_i \in \mathbb{F}[\mathbf{x}]$ for $i = 1, \ldots, t$. Fra lemma A.12 haves at

$$\mathrm{multigrad}(f) \leq \max_i(\mathrm{multigrad}(h_i g_i)) \ . \tag{2.3}$$

Vi lader $m(i) = \mathrm{multigrad}(h_i g_i)$ og definerer $\delta = \max(m(1), \ldots, m(t))$, så haves fra (2.3) at $\mathrm{multigrad}(f) \leq \delta$. Selvom $f \in \mathbf{I}$ er fast kan polynomiet muligvis skrives på forskellige måder på formen (2.2). Ved at betragte alle disse mulige måder opnås forskellige δ'er. For en given monomiel ordning vælges et f, hvor δ er minimal. Da vi ønsker at vise, at $\mathrm{multigrad}(f) = \delta$ antages modsætningsvist at $\mathrm{multigrad}(f) < \delta$. Det haves så at

$$\begin{aligned} f &= \sum_{i=1}^{t} h_i g_i = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i \ . \end{aligned} \tag{2.4}$$

Da f samt anden og tredje sum på højre siden af lighedstegnet i (2.4) har multigrad skarpt mindre end δ, må første sum også have multigrad skarpt mindre end δ. Dette er kun tilfældet hvis $\mathrm{LC}(\mathrm{LT}(\sum \mathrm{LT}(h_i)g_i)) = 0$ for ellers ville multigrad$(f) = \delta$.

Lad $\mathrm{LT}(h_i) = c_i\mathbf{x}^{\alpha(i)}$. Så kan den første sum i (2.4) skrives som

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i = \sum_{m(i)=\delta} c_i\mathbf{x}^{\alpha(i)}g_i \ . \tag{2.5}$$

Da multigrad$(h_ig_i) = \delta$ i (2.5) og multigrad$(\sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i) < \delta$, pr. antagelse omkring f og (2.4), kan lemma A.13 anvendes. Så gælder at (2.5) er en sum af linear kombination af S-polynomier $S(\mathbf{x}^{\alpha(j)}g_j, \mathbf{x}^{\alpha(k)}g_k)$, hvor hvert S-polynomium har multigrad mindre end δ. Per definition haves at

$$\begin{aligned} S(\mathbf{x}^{\alpha(j)}g_j, \mathbf{x}^{\alpha(k)}g_k) &= \frac{\mathbf{x}^{\delta}}{\mathbf{x}^{\alpha(j)}\,\mathrm{LT}(g_j)}\mathbf{x}^{\alpha(j)}g_j - \frac{\mathbf{x}^{\delta}}{\mathbf{x}^{\alpha(k)}\,\mathrm{LT}(g_k)}\mathbf{x}^{\alpha(k)}g_k \\ &= \mathbf{x}^{\delta}\left(\frac{g_j}{\mathrm{LT}(g_j)} - \frac{g_k}{\mathrm{LT}(g_k)}\right) \\ &= \mathbf{x}^{\delta-\gamma_{jk}}\left(\frac{\mathbf{x}^{\gamma_{jk}}}{\mathrm{LT}(g_j)}g_j - \frac{\mathbf{x}^{\gamma_{jk}}}{\mathrm{LT}(g_k)}g_k\right) \\ &= \mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k) \ , \end{aligned} \tag{2.6}$$

hvor $\mathbf{x}^{\gamma_{jk}} = \mathrm{lcm}(\mathrm{LM}(g_j), \mathrm{LM}(g_k))$. Der findes altså konstanter $c_{jk} \in \mathbb{F}$ således at

$$\begin{aligned} \sum_{m(i)=\delta} \mathrm{LT}(h_i)g_i &= \sum_{j,k} c_{jk}S(\mathbf{x}^{\alpha(j)}g_j, \mathbf{x}^{\alpha(k)}g_k) \\ &= \sum_{j,k} c_{jk}\mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k) \ . \end{aligned} \tag{2.7}$$

Da $\overline{S(g_j, g_k)}^{G} = 0$ per antagelse følger af divisionsalgoritmen at $S(g_j, g_k)$ kan skrives på formen

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk}g_i \ ,$$

hvor $a_{ijk} \in \mathbb{F}[\mathbf{x}]$. Fra ligning (B.5) korollar B.2 haves at

$$\mathrm{multigrad}(a_{ijk}g_i) \leq \mathrm{multigrad}(S(g_j, g_k)) \ .$$

Dette betyder også at

$$\mathrm{multigrad}(\mathbf{x}^{\delta-\gamma_{jk}}a_{ijk}g_i) \leq \mathrm{multigrad}(\mathbf{x}^{\delta-\gamma_{jk}}S(g_j, g_k)) < \delta \ ,$$

hvor den sidste ulighed følger af (2.6). Bemærk at

$$\begin{aligned}\sum_{j,k} c_{jk}\mathbf{x}^{\delta-\gamma_{jk}}S(g_j,g_k) &= \sum_{j,k} c_{jk}\mathbf{x}^{\delta-\gamma_{jk}}\left(\sum_{i=1}^{t} a_{ijk}g_i\right)\\ &= \sum_{j,k} c_{jk}\left(\sum_{i=1}^{t} \mathbf{x}^{\delta-\gamma_{jk}}a_{ijk}g_i\right)\end{aligned}$$

fra (2.7) er givet ved en sum hvor alle led har multigrad mindre end δ. Det vil sige, at f i (2.4) på højresiden kan omskrives til summer af multigrad mindre end δ. Heraf er der opnået en modstrid med antagelsen om minimalitet af δ, og derfor må multigrad$(f) = \delta$. Dette giver lighed i (2.3), hvorfor der gælder for mindst et $i \in \{1,\ldots,t\}$ at $\mathrm{LM}(f) = \mathrm{LM}(h_i g_i)$ og da $\mathrm{LM}(g_i)|\,\mathrm{LM}(h_i g_i)$ følger at $\mathrm{LM}(g_i)|\,\mathrm{LM}(f)$ hvorfor $\mathrm{LM}(f)$ er dividerbar med $\mathrm{LM}(g_i)$. Heraf følger at $\mathrm{LT}(f) \in \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle$. □

Buchbergers Kriterium udtaler sig om hvorvidt en given basis for et ideal også er en Gröbner-basis. Denne egenskab bliver udnyttet i Buchbergers Algoritme, der er præsenteret i algoritme 1. Algoritmen udvider en given mængde af frembringere for et ideal til en Gröbner-basis.

Algoritme 1 Buchbergers Algoritme.

Input: Et ideal $\mathbf{I} = \langle f_1,\ldots,f_s\rangle$.
Lad $G := \{f_1,\ldots,f_s\}$ og $G' = \emptyset$;
while $G\backslash\{G'\} \neq \emptyset$ **do**
  Lad $G' := G$;
  for hvert par $\{f_i, f_j\}$ hvor $f_i \neq f_j$ i G' **do**
    Lad $S := \overline{S(f_i,f_j)}^{G'}$;
    if $S \neq 0$ **then**
      Lad $G := G \cup \{S\}$;
    end if
  end for
end while
Output: En Gröbner-basis $G = \{g_1,\ldots,g_t\}$ hvor $\mathbf{I} = \langle g_1,\ldots,g_t\rangle$.

Følgende sætning beviser at Buchbergers Algoritme giver en Gröbner-basis i et endeligt antal skridt.

Sætning 2.15 (Buchbergers Algoritme)**.** *Lad* $\mathbf{I} = \{f_1,\ldots,f_s\} \neq \{0\}$ *være et ideal. Der gælder for* $\mathbf{I}$ *at Buchbergers Algoritme 1 i et endeligt antal skridt konstruerer en Gröbner-basis for* $\mathbf{I}$*. [CLO92, s.90]*

Bevis. Vi viser først, at algoritmen konstruerer en Gröbner-basis, hvorfor det kræves at $G \subseteq \mathbf{I}$ i alle af algoritmens etaper. Fra algoritmens begyndelse

er dette sandt, da G sættes lig den frembringende mængde for $\mathbf{I}$. Mængden G udvides herefter ved hvert gennemløb af while-løkken indtil en Gröbner-basis for $\mathbf{I}$ er konstrueret. Ved hver udvidelse af G tilføjes en rest $S = \overline{S(p,q)}^{G'}$ hvor $p, q \in G$. Da $G \subset I$ før udvidelsen er $p, q \in \mathbf{I}$ og heraf er $S(p,q) \in \mathbf{I}$. Da $S(p,q)$ divideres med $G' \subset \mathbf{I}$ fås at $G \cup \{S\} \subset \mathbf{I}$, hvorfor G også er indeholdt i $\mathbf{I}$ efter udvidelsen. Bemærk desuden at G faktisk fra begyndelsen indeholder en basis for $\mathbf{I}$, hvorfor G stadig efter udvidelsen er en basis for $\mathbf{I}$. Ved algoritmens afslutning er $G = G'$ hvilket er tilfældet når $S = \overline{S(p,q)}^{G'} = 0$ for alle $p, q \in G$. Fra sætning 2.14 haves da at G er en Gröbner-basis.

Vi skal også sikre os at algoritmen afslutter. Dette sker efter et gennemløb af while-løkken hvor $G = G'$. Efter et vilkårligt gennemløb består mængden G af G' sammen med nogle ikke-nul rester af S-polynomier af elementer fra G'. Da $G' \subset G$ følger at

$$\langle \mathrm{LT}(G') \rangle \subset \langle \mathrm{LT}(G) \rangle \ . \tag{2.8}$$

Hvis $G' \neq G$ så er mindst en rest $r \neq 0$ blevet tilføjet G. Da r er opnået ved division med G' er $\mathrm{LT}(r)$ ikke dividerbart med noget ledende led af elementerne i G' hvorfor $\mathrm{LT}(r) \notin \langle \mathrm{LT}(G') \rangle$. Da $r \in G$ haves derimod at $\mathrm{LT}(r) \in \langle \mathrm{LT}(G) \rangle$ så heraf er $\langle \mathrm{LT}(G') \rangle$ strengt mindre end $\langle \mathrm{LT}(G) \rangle$. Fra (2.8) haves da at de på hinanden konstrueret idealer $\langle \mathrm{LT}(G') \rangle$ former en stigende kæde af idealer i $\mathbb{F}[\mathbf{x}]$. Fra den Stigende Kæde Sætning (se bilag sætning B.5) haves at efter et endeligt antal iterationer vil kæden stabiliseres, således at $\langle \mathrm{LT}(G') \rangle = \langle \mathrm{LT}(G) \rangle$. Heraf er $G' = G$ og algoritmen afslutter efter et endeligt antal skridt. □

I det følgende eksempel anvendes Buchbergers Algoritme til at bestemme en Gröbner-basis for et givet ideal.

Eksempel 2.16. Lad $\mathbf{I} = \langle x^2y - 1, xy^2 - x \rangle$ med den monomielle ordning $x >_{\text{leks}} y$. Før første gennemløb af while-løkken haves at $G = \{x^2y - 1, xy^2 - x\}$ og $G' = \emptyset$.

- Da $G \backslash \{G'\} = G \neq \emptyset$ sættes $G' := \{x^2y - 1, xy^2 - x\}$.
  - For $\{x^2y - 1, xy^2 - x\}$ fås at $\overline{S(x^2y - 1, xy^2 - x)}^{G'} = x^2 - y$ og heraf $G = \{x^2y - 1, xy^2 - x, x^2 - y\}$.
- Da $G \backslash \{G'\} = \{x^2 - y\} \neq \emptyset$ sættes $G' = \{x^2y - 1, xy^2 - x, x^2 - y\}$.
  - For $\{x^2y - 1, xy^2 - x\}$ fås at $\overline{S(x^2y - 1, xy^2 - x)}^{G'} = 0$.

  - For $\{xy^2-x, x^2-y\}$ fås at $\overline{S(xy^2-x, x^2-y)}^{G'} = y^3-y$ og heraf $G = \{x^2y-1, xy^2-x, x^2-y, y^3-y\}$.
  - For $\{x^2y-1, x^2-y\}$ fås at $\overline{S(x^2y-1, x^2-y)}^{G'} = y^2-1$ og heraf $G = \{x^2y-1, xy^2-x, x^2-y, y^3-y, y^2-1\}$.

- Da $G\backslash\{G'\} = \{y^3-y, y^2-1\} \neq \emptyset$ sættes $G' = \{x^2y-1, xy^2-x, x^2-y, y^3-y, y^2-1\}$.
  - For $\{x^2y-1, xy^2-x\}$ fås at $\overline{S(x^2y-1, xy^2-x)}^{G'} = 0$.
  - For $\{xy^2-x, x^2-y\}$ fås at $\overline{S(xy^2-x, x^2-y)}^{G'} = 0$.
  - For $\{x^2y-1, x^2-y\}$ fås at $\overline{S(x^2y-1, x^2-y)}^{G'} = 0$.
  - For $\{x^2y-1, y^3-y\}$ fås at $\overline{S(x^2y-1, y^3-y)}^{G'} = 0$.
  - For $\{x^2y-1, y^2-1\}$ fås at $\overline{S(x^2y-1, y^2-1)}^{G'} = 0$.
  - For $\{xy^2-x, y^3-y\}$ fås at $\overline{S(xy^2-x, y^3-y)}^{G'} = 0$.
  - For $\{xy^2-x, y^2-1\}$ fås at $\overline{S(xy^2-x, y^2-1)}^{G'} = 0$.
  - For $\{x^2-y, y^3-y\}$ fås at $\overline{S(x^2-y, y^3-y)}^{G'} = 0$.
  - For $\{x^2-y, y^2-1\}$ fås at $\overline{S(x^2-y, y^2-1)}^{G'} = 0$.
  - For $\{y^3-y, y^2-1\}$ fås at $\overline{S(y^3-y, y^2-1)}^{G'} = 0$.

- Da $G\backslash\{G'\} = \emptyset$ er $G = \{x^2y-1, xy^2-x, x^2-y, y^3-y, y^2-1\}$ en Gröbner-basis.

Bemærk dog at G ikke er en reduceret Gröbner-basis for $\mathbf{I}$, idet det ses direkte at $y^3-y = y(y^2-1)$, hvorfor G kan reduceres. ▲

Bemærkning 2.17. Buchbergers Algoritme er meget tidskrævende, hvilket også fremgår tydeligt af ovenstående eksempel, da algoritmen gennemregner de sammen udsagn flere gange. En optimering af algoritmen er derfor at foretrække, så snart man er interesseret i at udregne større Gröbner-baser.

2.4 Fodaftryksgrænsen

I dette afsnit betragtes Fodaftryksgrænsen, som fortæller hvor mange ikke-nulpunkter et polynomium mindst har i $\mathbb{F}_q^n$. Dette kan anvendes til at bestemme det højeste antal af fælles nulpunkter et ideal kan have, når der er endeligt mange af disse. For endelige legemer $\mathbb{F}_q$ haves at der er q elementer. Det vil sige at for vektorrummet $\mathbb{F}_q^n$ gælder, der at $|\mathbb{F}_q^n| = q^n$ og mængden

af fælles nulpunkter for en mængde af polynomier i $\mathbb{F}_q[\mathbf{x}]$ må derfor være endelig. Som nævnt tidligere i afsnit 1.1.2 er det imidlertidig muligt at finde polynomier $f \in \mathbb{F}_q[\mathbf{x}]$ som ingen rod har i $\mathbb{F}_q^n$. Hvis ethvert polynomium skal have en rod er det nødvendigt at udvide legemet, hvilket gøres ved den algebraiske aflukning, jævnfør definition 1.2. Mængden af fælles nulpunkter for et ideal kaldes varietet og defineres ved følgende.

Definition 2.18 (Varietet af ideal)**.** Lad $\mathbf{I} \subset \mathbb{F}[x_1, \ldots, x_n]$ være et ideal. Da kaldes mængden

$$\mathbf{V}(\mathbf{I}) = \{\mathbf{p} = (p_1, \ldots, p_n) \in \mathbb{F}^n \mid f(\mathbf{p}) = 0 \text{ for alle } f \in \mathbf{I}\}$$

varieteten af idealet $\mathbf{I}$. [CLO92, s.79]

Bemærkning 2.19. Idet ethvert ideal $\mathbf{I} \in \mathbb{F}[\mathbf{x}]$ har en endelig frembringende mængde ifølge Hilberts Basis Sætning, sætning B.4, haves at $\mathbf{I} = \langle g_1, \ldots, g_t \rangle$. Det vil sige at ethvert polynomium $f(\mathbf{x}) \in \mathbf{I}$ kan skrives som

$$f(\mathbf{x}) = \sum_{i=1}^{t} h_i(\mathbf{x}) g_i(\mathbf{x}),$$

hvor $g_i \in \mathbf{I}$ og $h_i \in \mathbb{F}[\mathbf{x}]$. Det er derfor kun nødvendigt at finde fælles nulpunkter for de frembringende elementer, og varieteten af et ideal kan derfor skrives

$$\mathbf{V}(\mathbf{I}) = \mathbf{V}(\langle g_1, \ldots, g_t \rangle) = \{\mathbf{p} \in \mathbb{F}^n \mid g_i(\mathbf{p}) = 0 \text{ for } i \in \{1, \ldots, t\}\}.$$

Følgende defineres fodaftrykket.

Definition 2.20 (Fodaftryk)**.** Lad $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ være et ideal og en monomiel ordning $<$ på $\mathbb{F}[\mathbf{x}]$ være givet. Fodaftrykket af $\mathbf{I}$ under $<$ er da mængden

$$\Delta_<(\mathbf{I}) = \{\mathbf{x}^\alpha \in \mathbb{F}[\mathbf{x}] \mid \mathbf{x}^\alpha \text{ ikke er ledende monomium for } f \in \mathbf{I}\}.$$

[GT10, Definition 1.1]

I det følgende proposition gives en øvre grænse for antallet af punkter i varieteten af et ideal, når det vides at denne er endelig. Dette resultat benyttes i det efterfølgende til at vise Fodaftryksgrænsen.

Proposition 2.21. *Lad* $\mathbf{I} \subset \overline{\mathbb{F}}_q[\mathbf{x}]$ *være et ideal, hvor* $\mathbf{V}(\mathbf{I})$ *er endelig. Så er antallet af punkter i* $\mathbf{V}(\mathbf{I})$ *højest* $\dim(\overline{\mathbb{F}}_q[\mathbf{x}]/\mathbf{I})$*. [CLO92, s.235]*

Bevis. Antag at $\mathbf{V}(\mathbf{I}) = \{\mathbf{p}_1, \ldots, \mathbf{p}_m\}$ hvor $\mathbf{p}_1, \ldots, \mathbf{p}_m$ er punkter i $\overline{\mathbb{F}}_q^n$. Vi ønsker at bestemme polynomier $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}) \in \overline{\mathbb{F}}_q[\mathbf{x}]$, hvor $f_i(\mathbf{p}_i) = 1$

og $f_i(\mathbf{p}_j) = 0$ for $i \neq j$. Da ingen punkter i $\mathbf{V}(\mathbf{I})$ er ens gælder der, at $\mathbf{p}_i$ og $\mathbf{p}_j$ er forskellige i mindst en position når $i \neq j$. Det antages derfor at $\mathbf{p}_i$ og $\mathbf{p}_j$ er forskellige i den ℓ'te position. For alle par $\mathbf{p}_i, \mathbf{p}_j$ hvor $i \neq j$ defineres

$$h_{i,j}(\mathbf{x}) = \frac{x_\ell - p_{j_\ell}}{p_{i_\ell} - p_{j_\ell}},$$

som opfylder at $h_{i,j}(\mathbf{p}_i) = 1$ og $h_{i,j}(\mathbf{p}_j) = 0$. Vi kan heraf konstruere polynomierne $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})$ med de ønskede egenskaber ved at lade

$$f_i(\mathbf{x}) = \prod_{j \neq i} h_{i,j}(\mathbf{x}),$$

for $i \in \{1, \ldots, m\}$. Hvis det kan vises, at ækvivalensklasserne $[f_1], \ldots, [f_m] \in \overline{\mathbb{F}}_q[\mathbf{x}]/\mathbf{I}$ er lineært uafhængige følger det, at

$$m \leq \dim(\overline{\mathbb{F}}_q[\mathbf{x}]/\mathbf{I}),$$

hvilket vil sige at antallet af punkter i $\mathbf{V}(\mathbf{I})$ er højest $\dim(\overline{\mathbb{F}}_q[\mathbf{x}]/\mathbf{I})$.

Antag at $\sum_{i=1}^m a_i[f_i] = [0]$ i $\overline{\mathbb{F}}_q[\mathbf{x}]/\mathbf{I}$ for $a_i \in \overline{\mathbb{F}}_q$. Lad $h = \sum_{i=1}^m a_i f_i \in \overline{\mathbb{F}}_q[\mathbf{x}]$. Der gælder så af definition A.3, at

$$[h] = \sum_{i=1}^m a_i[f_i] = [0] = \{g \in \mathbb{F}_q[\mathbf{x}] \mid g \equiv 0 \mod \mathbf{I}\}.$$

Det vil sige at $h - 0 = h \in \mathbf{I}$, og for alle $\mathbf{p}_i \in \mathbf{V}(\mathbf{I})$ følger heraf, at $h(\mathbf{p}_i) = 0$. Derfor fås for $1 \leq j \leq m$, at

$$0 = h(\mathbf{p}_j) = \sum_{i=1}^m a_i f_i(\mathbf{p}_j) = 0 + \cdots + 0 + a_j f_j(\mathbf{p}_j) + 0 + \cdots + 0 = a_j.$$

Dette giver at ækvivalensklasserne $[f_1], \ldots, [f_m]$ er lineært uafhængige og hermed gælder der, at

$$|\mathbf{V}(\mathbf{I})| \leq \dim(\overline{\mathbb{F}}_q[\mathbf{x}]/\mathbf{I}).$$

□

Bemærkning 2.22. Dimensionen af kvotienten af $\mathbb{F}_q[\mathbf{x}]$ modulo $\mathbf{I}$ bestemmes ud fra antallet af monomier indeholdt i fodaftrykket for $\mathbf{I}$. Det vil sige

$$\dim\left(\overline{\mathbb{F}}_q[x_1, \ldots, x_n]/\mathbf{I}\right) = |\Delta_<(\mathbf{I})|.$$

Det er herved muligt at give Fodaftryksgrænsen som fortæller hvor mange ikke-nulpunkter et polynomium $f(\mathbf{x})$ mindst har i $\mathbb{F}_q^n$ når det ledende monomium er kendt.

Sætning 2.23 (Fodaftryksgrænsen)**.** *Lad $\overline{\mathbb{F}}_q$ være den algebraiske aflukning af $\mathbb{F}_q$ og $f(x_1,\ldots,x_n) \in \overline{\mathbb{F}}_q[x_1,\ldots,x_n]$ være et ikke-nulpolynomium. Fastsæt en monomiel ordning $>$ på $\overline{\mathbb{F}}_q[x_1,\ldots,x_n]$, og antag, at $x_1^{m_1}\cdots x_n^{m_n}$ med $0 \leq m_1,\ldots,m_n < q$ er ledende monomium i f. Så er antallet af ikke-nulpunkter for $f(x_1,\ldots,x_n)$ i $\mathbb{F}_q^n$ mindst $(q-m_1)\cdots(q-m_n)$. [GT10, s.11]*

Bevis. Idet der kun ønskes punkter i $\mathbb{F}_q^n$ betragtes først $h_i(x_1,\ldots,x_n) = x_i^q - x_i$ for $i \in \{1,\ldots,n\}$, som er definerende polynomier for $\mathbb{F}_q^n$. Det vil sige at $\mathbf{V}(\langle h_1,\ldots,h_n\rangle) = \mathbb{F}_q^n$. Lad

$$\mathbf{I} = \langle f, h_1,\ldots,h_n\rangle,$$

så gælder der, at $\mathbf{V}(\mathbf{I})$ er endelig og består af nulpunkterne for f i $\mathbb{F}_q^n$. Af proposition 2.21 fås at $|\mathbf{V}(\mathbf{I})| \leq \dim(\mathbb{F}_q[x_1,\ldots,x_n]/\mathbf{I}) = |\Delta_<(\mathbf{I})|$. Da $x_1^{m_1}\cdots x_n^{m_n}$ er ledende monomium for f fås, at ethvert monomium $\mathbf{x}^\alpha \in \mathbb{F}_q[\mathbf{x}]$, hvorom der gælder, at $\alpha_i < m_i$ for et eller andet $i \in \{1,\ldots,n\}$, vil ligge i $\Delta_<(\mathbf{I})$. Heraf fås, at det maksimale antal nulpunkter for f er

$$|\Delta_<(\mathbf{I})| = q^n - (q-m_1)\cdots(q-m_n),$$

da der i alt haves q^n punkter i $\mathbb{F}_q^n$. Det vil sige at f minimum har

$$q^n - (q^n - (q-m_1)\cdots(q-m_n)) = (q-m_1)\cdots(q-m_n)$$

ikke-nulpunkter i $\mathbb{F}_q^n$. □

Kapitel 3

Netværkskodningsproblemet

Givet et netværk bestående af et antal enheder og kanaler, hvor nogle af enhederne er kilder og/eller modtagere, kan en grafrepræsentation af netværket konstrueres. Grafrepræsentationen kan benyttes til en vurdering af, om det er muligt at optimere forsendelsen af meddelelser ved at kode netværket. Altså om flere meddelelser kan sendes til alle modtagere på en gang i stedet for at sende meddelelserne af sted til en modtager ad gangen. For at se hvorvidt det er muligt at kode meddelelserne på en sådan måde, at der kan dekodes ved modtageren, opstilles et netværkskodningsproblem. Et netværkskodningsproblem består i at bestemme om de nødvendige kommunikationsveje er tilgængelige i et netværk, hvis modtagerne skal kunne dekode de modtaget meddelelser. I dette kapitel præsenteres det kreds- og forsinkelsesfrie multicast netværkskodningsproblem, samt afgøres hvornår det har en løsning.

3.1 Lineær Netværkskodning

I dette afsnit defineres netværkskodningsproblemet. Her betragtes specielt multicast netværket og herunder bestemmes netværksovergange, samt under hvilke forudsætninger netværkskodningsproblemet har en løsning.

3.1.1 Præsentation af Netværkskodningsproblemet

Grafrepræsentationen af et givent netværk er en orienteret graf $G = (V, E)$ hvor enhederne giver punktmængden V og kanalerne kantmængden E. Kilderne samles i en kildemængde $\mathcal{S} = \{s_1, \ldots, s_{|\mathcal{S}|}\} \subseteq V$, og modtagerne angives i modtagermængden $\mathcal{R} = \{r_1, \ldots, r_{|\mathcal{R}|}\} \subseteq V$. Informationen

som ønskes sendt gennem netværket udtrykkes ved en meddelelsesmængde $\mathcal{X} = \{X_1, \ldots, X_h\}$, hvor X_j er en variabel, der antager værdier i $\mathbb{F}_q$. Ud fra disse meddelelser konstueres en meddelelsesvektor $\mathbf{X} = (X_1, \ldots, X_h)$, dvs. $\mathbf{X} \in \mathbb{F}_q^h$.

Til at definere hvilke kilder der skal generere meddelelser X_j for $j \in \{1, \ldots, h\}$ haves kildefunktionen $K : \mathcal{X} \to \mathcal{S}$. Det vil sige at hvis $K(X_j) = s_i$ så genereres meddelelse X_j ved kilde s_i. Kildefunktionen er surjektiv, da alle punkter i kildemængden nødvendigvis må generere minimum en meddelelse for at kunne betragtes som kilde. Antallet af beskeder $X_j \in \mathcal{X}$, som er genereret ved kilde s_i, betegnes i det følgende som $\nu(s_i)$. Demandfunktionen $D : \mathcal{R} \to \mathcal{X}$ angiver hvilke meddelelser en modtager kræver fra $\mathcal{X}$. Det vil sige at hvis der for en modtager $r_i \in \mathcal{R}$ haves at $D(r_i) = \mathcal{X}_{r_i} = \{X_{j_1}, \ldots, X_{j_l}\}$ så kræver r_i meddelelserne $X_{j_1}, \ldots, X_{j_l}$. I de tilfælde hvor $D(r_i) = \mathcal{X}$ for alle $r_i \in \mathcal{R}$, altså alle modtagere kræver alle meddelelser, tales der om multicast.

Ud fra ovenstående er det muligt opstille et netværkskodningsproblem.

Definition 3.1 (Netværkskodningsproblem)**.** Et givent netværk repræsenteret ved en orienteret graf $G = (V, E)$, en kildemængde $\mathcal{S}$, en modtagermængde $\mathcal{R}$, en meddelelsesmængde $\mathcal{X}$, en kildefunktion K og en demandfunktion D kaldes et netværkskodningsproblem.

Netværkskodningsproblemet siges at have en løsning hvis enhver modtager $r_k \in \mathcal{R}$ kan dekode meddelelserne givet ved demandfunktionen $D(r_k)$ korrekt.

Bemærkning 3.2. Et netværkskodningsproblem siges at være lineært, hvis meddelelsernes adfærd gennem netværket kan skrives som lineære polynomier over $\mathbb{F}_q$. Dette beskrives yderligere i afsnit 3.1.3.

For at et multicast netværkskodningsproblemet, som indeholder h meddelelser, har mulighed for at have en løsning, erdet nødvendigt, at der er minimum h disjunkte veje i netværket til hver modtager $r_k \in \mathcal{R}$. For disse disjunkte veje skal der desuden gælde, at $\nu(s_i)$ af disse veje starter i kilde s_i. I tilfælde hvor der ikke er tale om et multicast netværkskodningsproblem skal der være $|D(r_k)| \leq h$ disjunkte veje til modtager $r_k \in \mathcal{R}$. Her skal der gælde at $\nu_{r_k}(s_i)$ af disse veje starter i s_i, hvor $\nu_{r_k}(s_i)$ betegner antallet af meddelelser r_k kræver som er genereret ved kilde s_i. Kravet om h disjunkte veje i netværket kommer af, at en modtager $r_k \in \mathcal{R}$ kræver h meddelelser fra kildemængden. Hvis der konstrueres en udvidelse af netværket, så kan Minimum Snit Maximum Flow sætningen, jævnfør sætning C.3, anvendes til at fastsætte antallet af disjunkte veje fra s til $r_k \in \mathcal{R}$. Dette er lig antallet af meddelelser, der maksimalt kan sendes til r_k. Udvidelsen konstrueres ved at tilføje et imaginært punkt s til punktmængden V, hvorfra der haves $\nu(s_i)$

kanter fra s til hvert $s_i \in \mathcal{S}$. Når der ønskes at sendes h meddelelser til r_k skal der altså være h disjunkte veje, og da alle modtagere i $\mathcal{R}$ ønsker h meddelelser ved multicast, skal der være h disjunkte veje til hver modtager $r_k \in \mathcal{R}$.

De disjunkte veje for en modtager r_k samles i et flow F_k og alle sådanne flows samles i et flowsystem $\mathcal{F} = \{F_1, F_2, \ldots, F_{|\mathcal{R}|}\}$. Hvordan flowsystemet fastsættes vil vi ikke komme ind på i denne rapport, der henvises i stedet til Ford-Fulkersons Maximum Flow algoritme i [Sch09].

Inden der ses på hvornår et netværkskodningsproblem har en løsning beskrives meddelelsernes adfærd igennem netværket først ved hjælp af overgangskoefficienter. I det følgende betragtes kun multicast tilfældet, for det generelle tilfælde henvises til kapitel 4.

3.1.2 Netværksovergange

Det er nødvendigt at kende ind- og udgående kanter af et punkt samt andre kanter, dette defineres ved følgende.

Definition 3.3. Lad u og v være punkter i en orienteret graf $G = (V, E)$ hvor $e = (u, v)$ er en kant mellem u og v. Da er $\text{ind}(v) = \{(u, v) \mid (u, v) \in E\}$ og $\text{ud}(u) = \{(u, v) \mid (u, v) \in E\}$. For en kant $e = (u, v)$ gælder der, at $\text{ind}(e) = \text{ind}(v)$ og $\text{ud}(e) = \text{ud}(v)$.

I det følgende vil en ordning på kanterne også være nødvendig.

Definition 3.4. Lad $G = (V, E)$ være en graf. For en orienteret vej P i G, hvor der gælder at kant e_1 besøges før kant e_2 haves ordningen $e_1 \prec e_2$. Denne ordning kaldes en ancestral ordning.

Som tidligere nævnt genereres meddelelserne X_i ved kilderne $s_k \in \mathcal{S}$. Til at beskrive overgang fra kilde til kanal haves indkodningskoefficienter, a_{ij}. For disse koefficienter angiver indekset i hvilken meddelelse fra $\mathcal{X}$ der er tale om, dvs. $i \in \{1, \ldots, h\}$, mens indekset j angiver hvilken kant der ses på i kantmængden E, altså $j \in \{1, \ldots, |E|\}$. For indkodningskoefficienterne gælder der, at $a_{ij} = 0$ hvis $j \notin \text{ud}(s_k)$ eller $K(X_i) \neq s_k$. Indkodningskoefficienterne samles i en indkodningsmatrix A af størrelsen $h \times |E|$.

Når en meddelelse passerer en enhed sker der en overgang mellem kanalerne i netværket, og disse overgange beskrives med kantovergangskoefficienter f_{ij}. Det vil sige at f_{ij} beskriver overgangen fra kant(kanal) i til

kant(kanal) j, hvor der gælder, at $i, j \in \{1, \ldots, |E|\}$. Kantovergangskoefficienterne samles i en kantovergangsmatrix F, som har størrelsen $|E| \times |E|$. Hvis $i \notin \text{ind}(j)$ så sættes f_{ij} til at være nul, da det ikke er muligt at kode mellem to kanter, der ikke er forbundet. Heraf beskriver koefficienten f_{ij} om der er en vej i grafen fra kant i til kant j, og overgangsmatricen F fortæller derfor hvilke veje af længde to netværket har. (Det vil sige at der er brugt to kanter, men kun en punkt er passeret). Betragt F^2 så fås, at den ik'te komponent er givet ved

$$[F^2]_{ik} = \sum_{j=1}^{|E|} f_{ij} f_{jk}.$$

Der haves derfor at en komponent i F^2 kun kan være ikke-nul hvis der er en vej fra kant i til j og fra kant j til k for mindst et $j \in \{1, \ldots, |E|\}$. Således beskriver F^2 veje af længde tre i netværket. Dette argument kan fortsættes således at F^m beskriver veje af længde $m+1$ i netværket. Idet der betragtes kredsfrie netværket har enhver vej i den orienteret graf $G = (V, E)$ en endelig længde. Der eksisterer derfor et $N \in \mathbb{N}$, således at $F^N = \mathbf{O}$, hvor $\mathbf{O}$ er nulmatricen, hvilket vil sige, at N er længden af netværkets længste vej. For matricen

$$Q = I + F + F^2 + \cdots + F^{N-1} \tag{3.1}$$

haves ud fra ovenstående at Q indeholder information om vejene i netværket. Her gælder at komponent Q_{ij} er en sum, hvor ethvert led beskriver en vej fra kant i til kant j, og desuden er alle veje fra i til j beskrevet i denne sum. For udtrykket i (3.1) haves følgende lemma.

Lemma 3.5. *Lad F være en kantovergangsmatrix til et netværk, $G = (V, E)$ og $N \in \mathbb{N}$ være valgt således at $F^N = \mathbf{O}$ så gælder der, at*

$$I + F + F^2 + \cdots + F^{N-1} = (I - F)^{-1}.$$

Bevis. Betragt

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

Heraf haves, at

$$I + F + F^2 + \cdots + F^{N-1} = (I - F)^{-1}.$$

□

Ved overgange fra en kanal til en modtager $r_k \in \mathcal{R}$ haves dekodningskoefficienter $b_{ij}^{r_k}$. Her angiver i kanten så $i \in \{1, \ldots, |E|\}$, j beskeden der betragtes, altså $j \in \{1, \ldots, h\}$ og $r_k \in \mathcal{R}$ modtageren. Koefficienten $b_{ij}^{r_k}$

sættes lig nul hvis der gælder, at $i \notin \text{ind}(r_k)$. Dekoningskoefficienterne $b_{ij}^{r_k}$ samles i en dekodningsmatrix matrix B^{r_k} af størrelsen $|E| \times h$, hvilket vil sige, at der konstrueres en matrix B^{r_k} til hver modtager r_k i $\mathcal{R}$.

For et netværkskodningsproblem defineres følgende en variabelvektor som samler netværkets overgangskoefficienter.

Definition 3.6. Lad et netværk med overgangskoefficienterne a_{ij}, f_{ij} og $b_{ij}^{r_k}$ være givet. Da er en fælles variabelvektor for netværket defineret ved

$$\xi = (a_{11}, \ldots, a_{h|E|}, f_{11}, \ldots, f_{|E||E|}, b_{11}^{r_1}, \ldots, b_{|E|h}^{r_{|\mathcal{R}|}}).$$

Antallet af elementer i ξ betegnes n.

Da komponenterne i ξ benyttes til at beskrive overgange følger af bemærkning 3.2, at enhver komponent i ξ er et element fra $\mathbb{F}_q$.

Ved hjælp af overgangskoefficienterne er det muligt at bestemme hvorvidt der findes en løsning til et netværkskodningsproblem, givet i definition 3.1. Først defineres imidlertid kant- og outputpolynomier.

3.1.3 Løsning til Netværkskodningsproblemet

Meddelelsernes adfærd igennem netværket kan beskrives vha. overgangskoefficienterne ved brug af kantpolynomier $Y(j)$ og outputpolynomier $Z_j^{r_k}$. Kantpolynomiet $Y(j)$ er et udtryk for de beskeder, som løber på kanten j. Outputpolynomiet $Z_j^{r_k}$ udtrykker en kombination af de beskeder, som det er muligt for modtageren $r_k \in \mathcal{R}$ at modtage, når denne ønsker at betragte beskeden X_j. Disse er defineret ved

$$Y(j) = \sum_{i=1}^{h} a_{ij} X_i + \sum_{i \in \text{ind}(j)} f_{ij} Y(i) \,, \tag{3.2}$$

$$Z_j^{r_k} = \sum_{i \in \text{ind}(r_k)} b_{ij}^{r_k} Y(i) \,, \tag{3.3}$$

hvor h er antallet af meddelelser i $\mathcal{X}$. Kantpolynomiet $Y(j)$ i (3.2) er veldefineret ud fra en ancestral ordning på kanterne. Dette skyldes, at $Y(j)$ kun kan afhænge af $Y(i)$ hvis kant i og j optræder på den samme orienteret vej i netværket, altså er $Y(i)$ blevet defineret, før $Y(j)$ skal bestemmes.

Ud fra (3.2) kan kantpolynomierne samles i en rækkevektor, og heraf skrives vha. meddelelsesvektoren $\mathbf{X}$, indkodningsmatricen A og kantovergangsmatricen F;

$$\begin{aligned}
(Y(1) \;\; Y(2) \;\; \cdots \;\; Y(|E|)) &= (X_1 \;\; X_2 \;\; \cdots \;\; X_h)(A + AF + AF^2 + AF^{N-1}) \\
&= (X_1 \;\; X_2 \;\; \cdots \;\; X_h)A(I + F + F^2 + F^{N-1}) \\
&= (X_1 \;\; X_2 \;\; \cdots \;\; X_h)A(I - F)^{-1}. \qquad (3.4)
\end{aligned}$$

Her følger omskrivningen til (3.4) af lemma 3.5. Tilsvarende kan outputpolynomierne samles i en rækkevektor og skrives som

$$(Z_1^{r_k} \;\; Z_2^{r_k} \;\; \cdots \;\; Z_h^{r_k}) = (Y(1) \;\; Y(2) \;\; \cdots \;\; Y(|E|))B^{r_k}. \tag{3.5}$$

Ved brug af (3.4) kan (3.5) desuden omskrives til

$$(Z_1^{r_k} \;\; Z_2^{r_k} \;\; \cdots \;\; Z_h^{r_k}) = (X_1 \;\; X_2 \;\; \cdots \;\; X_h)A(I-F)^{-1}B^{r_k}. \tag{3.6}$$

Ud fra (3.6) er det muligt at definere overgangsmatricen for en modtager $r_k \in \mathcal{R}$ i et netværk.

Definition 3.7 (Overgangsmatrix)**.** Lad et multicast netværk med indkodningsmatrix A, kantovergangsmatrix F og dekodningsmatrix B^{r_k} være givet. Så er overgangsmatricen for modtager $r_k \in \mathcal{R}$ givet ved

$$\begin{aligned} M^{r_k} &= A(I + F + F^2 + \cdots + F^{N-1})B^{r_k} \\ &= A(I-F)^{-1}B^{r_k}, \end{aligned}$$

som har størrelsen $h \times h$.

Her beskriver matricen $(I-F)^{-1}$ alle veje i netværket, samt A kan siges at beskrive indkodningsvejene og B dekodningsvejene. Det vil sige enhver komponent $m_{ij}^{r_k}$ i M^{r_k} er en sum af vejene fra meddelelsen i til output af meddelelsen j. Bestemmes determinanten af M^{r_k} fås derfor et polynomium, hvor hvert led er et produkt mellem veje fra de forskellige input i til de forskellige output j, for $i, j \in \{1, \ldots, h\}$. I et led i $\det(M^{r_k})$ kan ethvert input og output kun optræde én gang, således optræder en overgangskoefficient kun én gang i hvert led i determinanten. Heraf beskriver et led i determinanten $\det(M^{r_k})$ de disjunkte veje der er i netværket som meddelelserne kan tage gennem netværket fra input til output. Dette svarer til at hvert led i $\det(M^{r_k})$ beskriver et flow i netværket fra kildemængden $\mathcal{S}$ til modtager $r_k \in \mathcal{R}$.

Ud fra definition 3.7 haves for (3.6) at

$$(Z_1^{r_k} \;\; Z_2^{r_k} \;\; \cdots \;\; Z_h^{r_k}) = (X_1 \;\; X_2 \;\; \cdots \;\; X_h)M^{r_k}, \tag{3.7}$$

og heraf ses at hvis overgangsmatricen M^{r_k} er regulær, så kan outputvektoren $\mathbf{Z}^{r_k} = (Z_1^{r_k} \;\; Z_2^{r_k} \;\; \cdots \;\; Z_h^{r_k})$ for modtager $r_k \in \mathcal{R}$ dekodes til meddelelsesvektoren $\mathbf{X}$. Fra lineær algebra haves at hvis alle overgangskoefficienter i M^{r_k} er fastsatte værdier i et legeme $\mathbb{F}_q$, så er M^{r_k} regulær hvis og kun hvis $\det(M^{r_k}) \neq 0$.

Det vil sige at skal det være muligt at løse netværkskodningsproblemet, så skal der for hver modtager $r_k \in \mathcal{R}$, $k \in \{1, \ldots, |\mathcal{R}|\}$ gælde, at overgangsmatricen er regulær. Derfor defineres overgangspolynomiet til at være

$$T(\xi) = \prod_{r_k \in \mathcal{R}} \det(M^{r_k}). \tag{3.8}$$

Da hvert led i $\det(M^{r_k})$ beskriver et flow F_k fås at et led i $T(\xi)$ beskriver et flowsystem $\mathcal{F} = \{F_1, \ldots, F_{|\mathcal{R}|}\}$ for netværket. Der gælder fra (3.8) at hvis alle $\det(M^{r_k}) \neq 0$ for fastsatte værdier i $\mathbb{F}_q$ så er $T(\xi) \neq 0$ for disse værdier, hvilket giver at T ikke er nulpolynomiet. Omvendt gælder der, at hvis T ikke er nulpolynomiet, eksisterer der et ξ med værdier i et legeme $\mathbb{F}_q$, således at $\det(M^{r_k}) \neq 0$ for alle $r_k \in \mathcal{R}$. Overgangspolynomiet $T(\xi)$ benyttes til at afgøre hvorvidt et netværkskodningsproblem har en løsning.

Sætning 3.8. *Et multicast netværkskodningsproblem har en løsning hvis og kun hvis det tilsvarende overgangspolynomium er ikke-nul. Hvis netværkskodningsproblemet har en løsning, da vil lineær netværkskodning over $\mathbb{F}_q$, hvor $q > |\mathcal{R}|$, være tilstrækkeligt. [GT10, s.12]*

Bevis. Antag at T ikke er nulpolynomiet. Da eksisterer et ξ med værdier i et tilstrækkeligt stort legeme $\mathbb{F}_q$, således at der kan dekodes for netværket. Altså netværkskodningsproblemet har en løsning.

Antag, at netværkskodningsproblemet har en løsning, hvilket vil sige der findes overgangskoefficienter, så det er muligt at dekode ved alle modtagere. Lad disse værdier ligge i ξ, da er $T(\xi) \neq 0$, heraf er T ikke-nulpolynomiet.

Når et netværkskodningsproblem har en løsning, gælder der, at enhver overgangskoefficient maksimalt kan have potens $|\mathcal{R}|$ i overgangspolynomiet $T(\xi)$. Dette skyldes at hver koefficient kun kan optræde en gang i $\det(M^{r_k})$ for hver modtager $r_k \in \mathcal{R}$. Det følger så af fodaftrykgrænsen sætning 2.23 at $T(\xi)$ har en ikke-nulløsning over $\mathbb{F}_q$ for $q > |R|$. □

Sætning 3.8 angiver under hvilke forhold et givent netværkskodningsproblem har en løsning, men siger intet om hvorledes en sådan løsning kan bestemmes. Der eksisterer algoritmer til at konstruere løsninger, disse vil imidlertid ikke blive betragtet i dette projekt, jvf. [GT10]. I stedet betragtes i det følgende vilkårlig netværkskodning.

3.2 Vilkårlig Netværkskodning

Ved lineær netværkskodning findes en løsning ved at se på, hvilke overgangskoefficienter der kan opfylde kant- og outputpolynomier således at enhver modtager $r_k \in \mathcal{R}$ kan dekode. Det kan imidlertid godt være komplekst og tidskrævende at finde sådanne koefficienter. Derfor kan det være en fordel at vælge koefficienterne tilfældigt i et fastsat legeme $\mathbb{F}_q$ og for bagefter at undersøge om den fundne løsning er brugbar. Når koefficienterne vælges vilkårligt tales der om vilkårlig netværkskodning, men kodningen foregår

stadig ved lineære operationer over $\mathbb{F}_q$. I dette afsnit undersøges sandsynligheden for at finde en brugbar løsning til et netværkskodningsproblem når kodningen foretages vilkårligt.

3.2.1 Sandsynlighed for en Løsning til Netværkskodningsproblemet

Som nævnt i sætning 3.8 skal der gælde, at overgangspolynomiet $T(\xi)$ er ikke-nul for at netværkskodningsproblemet har en løsning, hvor ξ indeholder alle indkodnings-, kantovergangs- og dekodningskoefficienter. Ved brug af Fodaftryksgrænsen er det muligt at give en sandsynlighed for at der vælges en brugbar løsning til netværkskodningsproblemet i legemet $\mathbb{F}_q^n$. Der ses først på tilfældet hvor netværket er kendt, hvilket vil sige at monomierne i $T(\xi)$ er kendte. Herefter ses der på sandsynligheden for succes ved et netværk hvor vejene fra kilderne $s \in \mathcal{S}$ til modtagere $r \in \mathcal{R}$ ikke er kendte.

Lad $\xi = (x_1, \ldots, x_n)$ repræsenterer overgangskoefficienterne i det givne netværket, pånær dekodningskoefficienterne $b_{ij}^{r_k}$ der betragtes som konstanter i det følgende. Lad $T(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ være givet med en monomiel ordning på de variable $x_1, \ldots, x_n$. Antag, at $x_1^{m_1} \cdots x_n^{m_n}$ er det ledende monomium i $T(x_1, \ldots, x_n)$, så haves det fra Fodaftryksgrænsen, sætning 2.23, at der for overgangspolynomiet T findes mindst $(q - m_1) \cdots (q - m_n)$ ikke-nulpunkter i $\mathbb{F}_q^n$. Dette betyder, at overgangskoefficienterne kan vælges på mindst $(q-m_1) \cdots (q-m_n)$ måder således at overgangspolynomiet T vil give ikke-nul, hvorved der er fundet en løsning til netværkskodningsproblemet. Der er i alt q^n måder at vælge overgangskoefficienterne på. Ud fra dette er det muligt at give en nedre grænse for successandsynligheden i tilfælde hvor netværket er kendt. Denne kaldes Footprint-grænsen og er givet ved;

$$P_{\mathrm{FP}\,2} := \prod_{i=1}^{n} \frac{q - m_i}{q}. \tag{3.9}$$

I tilfælde hvor det ledende monomium ikke er kendt for overgangspolynomiet $T(x_1, \ldots, x_n)$ gives en svagere nedre grænse;

$$P_{\mathrm{FP}\,1} := \min \left\{ \prod_{i=1}^{n} \frac{q - m_i}{q} \;\middle|\; x_1^{m_1} \cdots x_n^{m_n} \text{ er et monomium i } T \right\}. \tag{3.10}$$

Der gælder lighed imellem $P_{\mathrm{FP}\,2}$ og $P_{\mathrm{FP}\,1}$ i de tilfælde, hvor det ledende monomium i overgangspolynomiet også er det monomium der giver den mindste sandsynlighed.

Bemærkning 3.9. I det ovenstående er det muligt at opnå en højere sandsynlighed for succes ved at lade nogle af koefficienterne være valgt på forhånd,

hvorved antallet af variable falder. Dette gøres ved at lade koefficienterne, der beskriver tilfælde, hvor der kun er én kant der går ind i et punkt være lig en, da der ikke er brug for kodning i disse tilfælde. Samtidig vælges alle overgangskoefficienter f_{ij} til nul hvis j kommer før i i en ancestral ordning af kanterne. Indkodningskoefficienterne a_{ij} vælges til nul, hvis der gælder at $j \notin \mathrm{ud}(s)$ for $s \in \mathcal{S}$ eller at X_i ikke genereres i kilde s hvor $j \in \mathrm{ud}(s)$.

For Footprint-grænsen gælder der, at vejene i netværket skal være kendte, da det ellers ikke er muligt at bestemme monomierne i overgangspolynomiet $T(\xi)$. Hvis monomierne i overgangspolynomiet hørende til et netværkskodningsproblem ikke er kendte, så haves følgende grænse for successandsynligheden.

Proposition 3.10. *Successandsynligheden for at finde en løsning til et netværkskodningsproblem med en løsning er nedre afgrænset af*

$$P_{\mathrm{succ}} \geq P_{\mathrm{Ho}\,0} := \left(\frac{q - |\mathcal{R}|}{q}\right)^{\eta}, \tag{3.11}$$

for $q \geq |\mathcal{R}|$, hvor η er antallet af variable i overgangspolynomiet hørende til netværkskodningsproblemet. [HMK+06, Theorem 2]

Bevis. Betragt overgangspolynomiet $T(\xi) = \prod_{r\in\mathcal{R}} \det(M^r)$, hvor ξ indeholder alle indkodnings-, kantovergangs- og dekodningskoefficienter. Lad overgangskoefficienter f_{ij} være nul, hvis j kommer før i i en ancestral ordning af kanterne. Desuden lades indkodningskoefficienterne a_{ij} være nul, hvis der gælder at $j \notin \mathrm{ud}(s)$ for $s \in \mathcal{S}$ eller at X_i ikke genereres i kilde s hvor $j \in \mathrm{ud}(s)$. Betragt dekodningskoefficienterne b^r_{ij} som konstanter. Det vil sige polynomiet $T(\xi)$ har η variable, som højest kan optræde én gang i hvert monomium i hver af de $|\mathcal{R}|$ determinanter $\det(M^r)$. Af dette fås at hver af de η variable højest kan have potens $|\mathcal{R}|$ i $T(\xi)$. Ved fodaftryksgrænsen, sætning 2.23, fås herved at der findes mindst $(q - |\mathcal{R}|)^\eta$ ikke-nulpunkter for $T(\xi)$ ud af de q^η mulige. Heraf fås at sandsynligheden for at vælge en ikke-nulløsning er

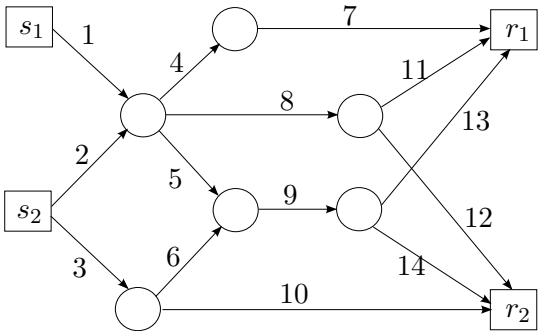
$$P_{\mathrm{succ}} \geq P_{\mathrm{Ho}\,0} := \left(\frac{q - |\mathcal{R}|}{q}\right)^{\eta}. \tag{3.12}$$

Af (3.12) ses det at der nødvendigvis må gælde at $q \geq |\mathcal{R}|$, da den nedre grænse for successandsynligheden ellers ville blive negativ, hvilket ikke er muligt. □

Sandsynlighederne fra (3.9), (3.10) og (3.11) giver at successandsynligheden er nedre afgrænset ved følgende

$$P_{\mathrm{succ}} \geq P_{\mathrm{FP}\,2} \geq P_{\mathrm{FP}\,1} \geq P_{\mathrm{Ho}\,0}.$$

Dette skyldes, at en større viden om netværkets opbygning medfører et bedre beslutningsgrundlag vedrørende valget af koefficienterne.



Figur 3.1: Netværk hørende til eksempel 3.11.

3.3 Eksempel på Multicast Netværkskodningsproblem

I dette afsnit anvendes teorien fra de to foregående afsnit til at løse et konkret kreds- og forsinkelsesfrit multicast netværkskodningsproblem. Dette gøres ved et eksempel, hvor netværket er konstrueret således at de forskellige aspekter af teorien illustreres bedst muligt.

Eksempel 3.11. Først opstilles netværkskodningsproblemet fra definition 3.1, som vi ønsker at løse.

Lad et netværk med grafrepræsentationen $G = (V, E)$ være givet, se figur 3.1. Punktmængden er $V = \{s_1, s_2, \ldots, r_2\}$ og kantmængden er $E = \{1, 2, \ldots, 14\}$. For kanterne haves en ancestral ordning $1 \prec 2 \prec \cdots \prec 14$. Desuden haves kildemængden $\mathcal{S} = \{s_1, s_2\}$, modtagermængden $\mathcal{R} = \{r_1, r_2\}$ samt meddelelsesmængden $\mathcal{X} = \{X_1, X_2, X_2\}$. Kildefunktionen er givet ved

$$K(X) = \begin{cases} s_1 \text{ for } X = X_1 \\ s_2 \text{ for } X \in \{X_2, X_3\} \end{cases} .$$

Da der ses på et multicast netværk haves, at $D(r_1) = \{X_1, X_2, X_3\} = D(r_2)$, altså begge modtagere kræver alle meddelelser i meddelelsesvektoren $\mathbf{X} = [X_1 \;\; X_2 \;\; X_3]$.

Flowsystemet for netværket er $\mathcal{F} = \{F_1, F_2\}$. Her kræves at F_1 og F_2 indeholder 3 disjunkte veje hver og desuden skal $\nu(s_1) = 1$ vej starte i s_1 og $\nu(s_2) = 2$ veje starte i s_2. De to flow er givet ved

$$\begin{aligned} F_1 &= \{(1,4,7),(2,8,11),(3,6,9,13)\} , \\ F_2 &= \{(1,8,12),(2,5,9,14),(3,10)\} , \end{aligned}$$

som har de ønskede egenskaber, da $\mathrm{ud}(s_1) = \{1\}$ og $\mathrm{ud}(s_2) = \{2, 3\}$.

Ud fra netværket givet i figur 3.1 er det muligt at lave indkodnings- og kantovergangsmatricen;

$$A = \begin{bmatrix} a_{11} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & a_{22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_{33} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

og

$$F = \begin{bmatrix} 0 & 0 & 0 & f_{14} & f_{15} & 0 & 0 & f_{18} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_{24} & f_{25} & 0 & 0 & f_{28} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & f_{36} & 0 & 0 & 0 & f_{3,10} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & f_{47} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{59} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{69} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{8,11} & f_{8,12} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{9,13} & f_{9,14} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

For kantovergangsmatricen gælder der, at $F^4 = \mathbf{O}$, hvilket svarer til at den længste vej i netværket har længden 4. Ved at betragte netværket i figur 3.1 ses at dette også er tilfældet. Det vil sige at $I + F + F^2 + F^3 = (I - F)^{-1}$ beskriver alle veje i netværket. For de to modtagere $r_1, r_2 \in \mathcal{R}$ haves dekodningsmatricer

$$B^{r_1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_{71} & b_{72} & b_{73} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_{11,1} & b_{11,2} & b_{11,3} \\ 0 & 0 & 0 \\ b_{13,1} & b_{13,2} & b_{13,3} \\ 0 & 0 & 0 \end{bmatrix} \text{ og } B^{r_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_{10,1} & b_{10,2} & b_{10,3} \\ 0 & 0 & 0 \\ b_{12,1} & b_{12,2} & b_{12,3} \\ 0 & 0 & 0 \\ b_{14,1} & b_{14,2} & b_{14,3} \end{bmatrix}.$$

Kant- og outputpolynomierne bestemmes for indgående kanter i r_1 ved

at benytte (3.2) og (3.3). Der haves, at $\text{ind}(r_1) = \{7, 11, 13\}$, og kantpolynomierne bliver

$$\begin{aligned} Y(7) &= f_{47}Y(4) = f_{14}f_{47}Y(1) = a_{11}f_{14}f_{47}X_1 \ , \\ Y(11) &= f_{8,11}Y(8) = f_{18}f_{8,11}Y(1) + f_{28}f_{8,11}Y(2) \\ &= a_{11}f_{18}f_{8,11}X_1 + a_{22}f_{28}f_{8,11}X_2 \ , \\ Y(13) &= f_{9,13}Y(9) = f_{59}f_{9,13}Y(5) + f_{69}f_{9,13}Y(5) \\ &= f_{15}f_{59}f_{9,13}Y(1) + f_{25}f_{59}f_{9,13}Y(2) + f_{36}f_{69}f_{9,13}Y(3) \\ &= a_{11}f_{15}f_{59}f_{9,13}X_1 + a_{22}f_{25}f_{59}f_{9,13}X_2 + a_{33}f_{36}f_{69}f_{9,13}X_3 \ . \end{aligned}$$

Heraf bestemmes outputpolynomierne til at være

$$\begin{aligned} Z_1^{r_1} &= b_{71}Y(7) + b_{11,1}Y(11) + b_{13,1}Y(13) \ , \\ Z_2^{r_1} &= b_{72}Y(7) + b_{11,2}Y(11) + b_{13,2}Y(13) \ , \\ Z_3^{r_1} &= b_{73}Y(7) + b_{11,3}Y(11) + b_{13,3}Y(13) \ . \end{aligned}$$

Outputpolynomierne til modtagerne $r_1, r_2 \in \mathcal{R}$ kan også bestemmes vha. overgangsmatricerne, M^{r_1} og M^{r_2}, til netværket. I M^{r_1} er komponenterne (j, i) givet ved

$$\begin{aligned} &\text{for } j = 1: && a_{11}f_{14}f_{47}b_{7i} + a_{11}f_{18}f_{8,11}b_{11,i} + a_{11}f_{15}f_{59}f_{9,13}b_{13,i} \ , \\ &\text{for } j = 2: && a_{22}f_{24}f_{47}b_{7i} + a_{22}f_{28}f_{8,11}b_{11,i} + a_{22}f_{25}f_{59}f_{9,13}b_{13,i} \ , \\ &\text{for } j = 3: && a_{33}f_{36}f_{69}f_{9,13}b_{13,i} \ , \end{aligned}$$

hvor $i \in \{1, 2, 3\}$. For M^{r_2} haves komponent (j, i) til at være

$$\begin{aligned} &\text{for } j = 1: && a_{11}f_{18}f_{8,12}b_{12,i} + a_{11}f_{15}f_{59}f_{9,14}b_{14,i} \ , \\ &\text{for } j = 2: && a_{22}f_{28}f_{8,12}b_{12,i} + a_{22}f_{25}f_{59}f_{9,14}b_{14,i} \ , \\ &\text{for } j = 3: && a_{33}f_{3,10}b_{10,i} + a_{33}f_{36}f_{69}f_{9,14}b_{14,i} \ , \end{aligned}$$

for $i \in \{1, 2, 3\}$. Der gælder så af (3.7) at

$$\mathbf{Z}^{r_1} = \mathbf{X}M^{r_1} \text{ og } \mathbf{Z}^{r_2} = \mathbf{X}M^{r_2}.$$

For at se om netværkskodningsproblemet har en løsning bestemmes overgangspolynomiet

$$T(\xi) = \det(M^{r_1}) \det(M^{r_2}),$$

som er forskelligt fra nul, hvis koefficienterne i ξ bestemmes korrekt. Der gælder derfor fra sætning 3.8, at netværkskodningsproblemet har en løsning, hvis koefficienterne er indeholdt i $\mathbb{F}_3$.

Som tidligere nævnt findes der algoritmer til at bestemme en løsning, men da netværket her har en begrænset størrelse er det muligt at bestemme

en løsning manuelt inden for rimelig tid. Vi bestemmer overgangskoefficienterne til at være følgende;

$$\begin{aligned}
a_{11} &= a_{22} = a_{33} = 1 \\
f_{14} &= f_{18} = f_{25} = f_{28} = f_{36} = f_{3,10} = f_{47} = f_{59} = f_{69} = f_{8,11} = f_{8,12} \\
&= f_{9,13} = f_{9,14} = 1 \\
b_{71}^{r_1} &= b_{72}^{r_1} = b_{11,2}^{r_1} = b_{11,3}^{r_1} = b_{13,3}^{r_1} = b_{10,2}^{r_2} = b_{10,3}^{r_2} = b_{12,1}^{r_2} = b_{14,1}^{r_2} = b_{14,2}^{r_2} = 1 \\
f_{15} &= f_{24} = 0 \\
b_{73}^{r_1} &= b_{11,1}^{r_1} = b_{13,1}^{r_1} = b_{13,2}^{r_1} = b_{10,1}^{r_2} = b_{12,2}^{r_2} = b_{12,3}^{r_2} = b_{14,3}^{r_2} = 0
\end{aligned}$$

Af dette fås overgangsmatricer

$$M^{r_1} = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{og} \quad M^{r_2} = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 2 & 1 \end{bmatrix}, \tag{3.13}$$

og overgangspolynomium

$$T(\xi) = 1 \cdot 1 = 1 \neq 0.$$

Heraf ses at de valgte koefficienter giver en løsning til netværkkodningsproblemet.

Ud fra overgangsmatricerne fås at

$$[Z_1^{r_1} \;\; Z_2^{r_1} \;\; Z_3^{r_1}] = [X_1 \;\; X_2 \;\; X_3]M^{r_1} = [X_1 \;\; 2X_1 + X_2 \;\; X_1 + 2X_2 + X_3],$$

og

$$[Z_1^{r_2} \;\; Z_2^{r_2} \;\; Z_3^{r_2}] = [X_1 \;\; X_2 \;\; X_3]M^{r_2} = [X_1 + 2X_2 + X_3 \;\; X_2 + 2X_3 \;\; X_3].$$

De inverse til overgangsmatricerne i (3.13) bestemmes til

$$(M^{r_1})^{-1} = \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{og} \quad (M^{r_2})^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & -2 & 1 \end{bmatrix}.$$

Ud fra dette burde der gælde, at

$$\mathbf{Z}^{r_k}(M^{r_1})^{-1} = \mathbf{X} \quad \text{og} \quad \mathbf{Z}^{r_2}(M^{r_2})^{-1} = \mathbf{X}.$$

For r_1 fås at

$$\begin{aligned}
\mathbf{Z}^{r_1}(M^{r_1})^{-1} &= [X_1 \;\; -2X_1 + 2X_1 + X_2 \;\; -X_1 - 2X_2 + X_1 + 2X_2 + X_3] \\
&= [X_1 \;\; X_2 \;\; X_3],
\end{aligned}$$

og for r_2

$$\begin{aligned}\mathbf{Z}^{r_2}(M^{r_2})^{-1} &= [X_1 + 2X_2 + X_3 - 2X_2 - X_3 \;\; X_2 + 2X_3 - 2X_3 \;\; X_3] \\ &= [X_1 \;\; X_2 \;\; X_3].\end{aligned}$$

Herved ses at der ved den fundne løsning dekodes korrekt ved begge modtagere. Ved denne løsning er koefficienterne bestemt således at det vides, at der er en løsning til netværket, men hvis der vælges at foretages vilkålig kodning kan vi udregne sandsynligheden for at finde en brugbar løsning.

Først bestemmes Footprint-grænserne $P_{\mathrm{FP}\,1}$ og $P_{\mathrm{FP}\,2}$, herefter ses der på $P_{\mathrm{Ho}\,0}$. Fra bemærkning 3.9 vides at nogle overgangskoefficienter kan vælges på forhånd. Fra netværket i figur 3.1 fås derfor, at $a_{11} = a_{22} = a_{33} = f_{36} = f_{3,10} = f_{47} = f_{8,11} = f_{8,12} = f_{9,13} = f_{9,14} = 1$, desuden gælder der, at dekodningskoefficienterne ses som konstanter. Overgangskoefficienterne der skal bestemmes er så

$$f_{14} = a,\; f_{15} = b,\; f_{18} = c,\; f_{24} = d,\; f_{25} = e,\; f_{28} = f,\; f_{59} = g,\; f_{69} = h.$$

Alle andre koefficienter vælges til at være nul. For de vilkårligt valgte koefficienter haves en monomiel ordning hvor $e > a > b > d > c > f > g > h$. Determinanterne af overgangsmatricerne bestemmes som ovenfor og der fås at

$$\det(M^{r_1}) = afhk_1 + dchk_2 \quad \text{og} \quad \det(M^{r_2}) = ecfk_3 + bfgk_4\,,$$

hvorfor overgangspolynomiet bliver

$$T(\xi) = eacfgh\tilde{k}_1 + abf^2gh\tilde{k}_2 + edc^2gh\tilde{k}_3 + bdcfgh\tilde{k}_4.$$

Her afhænger $k_1, k_2, k_3, k_4, \tilde{k}_1, \tilde{k}_2, \tilde{k}_3$ og $\tilde{k}_4$ kun af dekodningskoefficienterne. Det ledende monomium i T er $eacfhg$ og derfor fås Footprint-grænsen

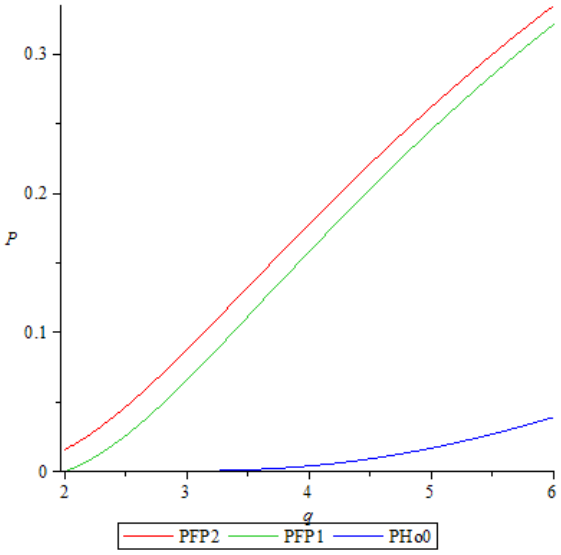
$$P_{\mathrm{FP}\,2} = \frac{(q-1)^6}{q^6}\,.$$

I tilfælde hvor den monomielle ordning ikke er kendt fås Footprint-grænsen

$$P_{\mathrm{FP}\,1} = \frac{(q-2)(q-1)^4}{q^5}\,.$$

Her ses at $P_{\mathrm{FP}\,2}$ er positiv for $q \geq 2$, mens $P_{\mathrm{FP}\,1}$ er positiv for $q \geq 3$, jvf. figur 3.2.

Fra proposition 3.10 haves at når monomierne i overgangspolynomiet ikke er kendte, kan sandsynligheden for at bestemme en brugbar løsning ved vilkårlig kodning stadig findes. Her bestemmes antallet af variable i overgangspolynomiet. For netværket i dette eksempel haves der 8 variable,



Figur 3.2: Plot af Footprint-grænserne og $P_{\mathrm{Ho}\,0}$ til forskellige værdier af q.

hvis de samme koefficienter som før vælges på forhånd. Desuden anses dekodningskoefficienterne stadig som konstanter. Af dette fås en grænse for successandsynligheden til at være

$$P_{\mathrm{Ho}\,0} = \frac{(q-2)^8}{q^8}.$$

Også denne sandsynlighed er illusteret på figur 3.2 og det ses, at der haves en ikke-nul sandsynlighed hvis $q \geq 3$. ▲

Kapitel 4

Det Generelle Netværkskodningsproblem

I kapitel 3 beskæftigede vi os med multicast netværkskodningsproblemet, der kan betragtes som et særtilfælde af det generelle netværkskodningsproblem. I modsætning til multicast netværkskodningsproblemet kan der her haves tilfælde, hvor alle modtagere $r \in \mathcal{R}$ ikke kræver alle meddelelser i meddelelsesvektoren $\mathbf{X}$. Dette betyder at der måske findes kilder $s \in \mathcal{S}$, hvorfra en modtager $r \in \mathcal{R}$ intet kræver. Inden der ses på, hvornår et generelt netværkskodningsproblem har en løsning betragtes overgangsmatricen M.

Overgangsmatricen M for det generelle netværkskodningsproblem kan konstrueres ud fra indkodnings-, kantovergangs- og dekodningsmatricer ligesom ved multicast netværker. Ved det generelle netværkskodningsproblem gælder der, at indkodning- og kantovergangsmatricen konstrueres på samme måde som ved multicast netværket. Det vil sige at for indkodningsmatricen A gælder der, at komponent a_{ij} er nul, når der gælder, at meddelelse X_i ikke genereres i en kilde $s \in \mathcal{S}$ eller $j \notin \text{ud}(s)$. Indkodningsmatricen A er en $h \times |E|$ matrix. For kantovergangsmatricen F gælder der, at komponent f_{ij} er nul når $i \notin \text{ind}(j)$, samt at $F^N = \mathbf{O}$ for $N \in \mathbb{N}$, hvor N er længden af den længste vej. Kantovergangsmatricen F har størrelsen $|E| \times |E|$. For dekodningsmatricen B gælder der, at denne beskriver alle modtagere $r \in \mathcal{R}$ samtidig, i modsætning til multicast netværkskodningsproblemet hvor modtagerne betragtes enkeltvis. Altså her beskriver de første h søjler dekodningen til r_1, de næste h søjler dekodningen til r_2, osv. Desuden gælder der for matricen B, at en komponent hørende til modtager $r \in \mathcal{R}$ er nul, hvis meddelelse $X_j \notin \mathcal{X}_r = D(r)$, hvor $D(\cdot)$ er demandfunktionen, eller

$i \notin \text{ind}(r)$. Dekodningsmatricen B er en matrix af størrelse $|E| \times (|\mathcal{R}| \cdot h)$. Ud fra dette fås at overgangsmatricen M er givet ved

$$M = A \cdot (I - F)^{-1} \cdot B, \tag{4.1}$$

og har størrelsen $h \times (|\mathcal{R}| \cdot h)$. I overgangsmatricen M beskriver de første h søjler forholdet mellem meddelelserne i $\mathcal{X}$ og modtager r_1, de næste h søjler forholdet mellem $\mathcal{X}$ og r_2 osv. For at beskrive hvilken meddelelse der ses på i forhold til hver modtager $r_k \in \mathcal{R}$ indføres følgende notation.

> For en komponent M_{ij^k} i M beskriver indekset ij^k at der ses på række i og søjle $((k-1)h + j)$ i M. Udtrykket for søjlenumret kommer af at det er den k'te modtager r_k der betragtes og den j'te meddelelse. Det vil sige at $i, j \in \{1, \ldots, h\}$ og $k \in \{1, \ldots, |\mathcal{R}|\}$.

Som ved multicast netværkskodningsproblemet lader vi

$$\xi = (a_{1,1}, \ldots, a_{h,|E|}, f_{1,1}, \ldots, f_{|E|,|E|}, b_{1,1}, \ldots, b_{|E|,|\mathcal{R}|h}),$$

være en vektor indeholdende alle overgangskoefficienter. I det følgende antages at antallet af komponenter i ξ er n.

Hvis en eventuel løsning til et givent netværkskodningsproblem skal findes er det nødvendigt sikre, at de ønskede forbindelser eksisterer i netværket. Det vil sige at der skal være $|D(r)|$ disjunkte veje fra kildemængden $\mathcal{S}$ til modtager $r \in \mathcal{R}$, samt at disse veje skal have begyndelse i de korrekte kilder. Altså når $r \in \mathcal{R}$ kræver $\nu_r(s)$ meddelelser fra $s \in \mathcal{S}$, skal der gælde, at der er $\nu_r(s)$ disjunkte veje fra s til r. Herudover må en forbindelse mellem kildemængden $\mathcal{S}$ og modtager $r_i \in \mathcal{R}$ ikke påvirke forbindelsen mellem $\mathcal{S}$ og modtager $r_j \in \mathcal{R}$, hvor $i \neq j$. Dette kan også betragtes som situationen hvor en modtager r_i modtager noget information som ikke er krævet, så skal r_i kunne ignorere den information uden at miste noget af den krævede information. Ud fra dette fås følgende sætning vedrørende hvornår et generelt netværkskodningsproblem har en løsning.

Sætning 4.1. *Lad et kreds- og forsinkelsesfrit netværk $G = (V, E)$ med overgangsmatrix M være givet. Det lineære netværkskodningsproblem har en løsning hvis og kun hvis variablerne i ξ kan vælges, således at*

1. *Komponent $M_{ij^k} = 0$ hvis modtager r_k ikke kræver meddelelse i eller j.*
2. *Komponenter M_{ij^k} hvor modtager r_k kræver både meddelelse i og j kan samles i en kvadratisk matrix M_k af størrelsen $|D(r_k)| \times |D(r_k)|$ som er regulær.*

[KM03, Theorem 6]

Bevis. Antag at betingelse *1.* og *2.* er opfyldt. Betingelse *1.* sikrer at modtager r_k kan ignorere meddelelser som den ikke kræver. Fra betingelse *2.* gælder der at modtager r_k kan inverterer M_k, og hermed genskabe de krævede meddelelser. Fra dette fås at en løsning til netværkskodningsproblemet er fundet.

Antag at netværket har en løsning, men at betingelse *1.* eller *2.* ikke er opfyldt. Hvis betingelse *1.* ikke er opfyldt vil der gælde at en modtager r_k ikke kan ignorere modtaget meddelelser, som ikke er krævet. Så vil output ved modtager r_k være påvirket af de uønskede meddelelser, da de optræder som fejlinformation. Da det ikke muligt at se forskel på fejlmeddelelser og ønskede meddelelser ved modtager r_k, så vil r_k ikke kunne dekode korrekt. Hermed er der en modstrid med at netværkskodningsproblemet har en løsning.

Idet M_k fra betingelse *2.* kan ses som et multicast netværk med kun en kilde og en modtager gælder der fra sætning 3.8, at hvis betingelse *2.* ikke er opfyldt kan netværkskodningsproblemet ikke løses. Hermed har netværkskodningsproblemet en løsning hvis og kun hvis betingelse *1.* og *2.* er opfyldt. □

Afgørelsen af om der findes en løsning ξ' som kan opfylde betingelse *1.* og *2.* fra sætning 4.1 kan være en omstændig proces. Dog, ved en omskrivning af problemet bliver det lettere at sige, om der kan findes en løsning ξ'. Lad $p_1(\xi), p_2(\xi), \ldots, p_\kappa(\xi)$ betegne komponenterne M_{ij^k}, hvor modtager $r_k \in \mathcal{R}$ ikke kræver meddelelse i eller j. Det vil sige, at hvis der findes et ξ, hvorom der gælder, at $p_k(\xi) = 0$ for alle $k \in \{1, \ldots, \kappa\}$ vil betingelse *1.* være opfyldt. I tilfælde hvor modtager $r_k \in \mathcal{R}$ kræver meddelelserne i og j sættes $g_k(\xi) = \det(M_k)$, for $k \in \{1, \ldots, |\mathcal{R}|\}$. Lad ξ_0 være en ny variable og definer

$$g(\xi, \xi_0) = 1 - \xi_0 \prod_{k=1}^{|\mathcal{R}|} g_k(\xi).$$

Der gælder således at hvis der kan findes et ξ og ξ_0, hvorom der gælder, at $g(\xi, \xi_0) = 0$ så er $g_k(\xi) \neq 0$ for alle $k \in \{1, \ldots, |\mathcal{R}|\}$ for dette ξ. Det vil sige at $g(\xi, \xi_0)$ beskriver hvorvidt betingelse *2.* er opfyldt.

Ud fra ovenstående beskrivelse af betingelse *1.* og *2.* defineres idealet for det lineære netværkskodningsproblem ved

$$\mathbf{I}(G) = \langle p_1, \ldots, p_\kappa, g \rangle .$$

Herved bliver varieteten af idealet, iflg. definition 2.18,

$$\mathbf{V}(\mathbf{I}(G)) = \{(\xi, \xi_0) \in \mathbb{F}_q^{n+1} \mid f(\xi, \xi_0) = 0 \text{ for alle } f \in \mathbf{I}(G)\},$$

som er ikke-tom, hvis der findes et ξ der opfylder betingelse *1.* og *2.* i sætning 4.1. Det er derfor muligt at omskrive sætning 4.1 til følgende:

Sætning 4.2. *Lad et kreds- og forsinkelsesfrit netværk $G = (V, E)$ være givet. Det lineære netværkskodningsproblem har en løsning hvis og kun hvis $\mathbf{V}(\mathbf{I}(G))$ er ikke-tom, og heraf at $\mathbf{I}(G) \subset \mathbb{F}_q[\xi, \xi_0]$. [KM03, Theorem 7]*

Bevis. Antag, at $\mathbf{I}(G) \subset \mathbb{F}_q[\xi, \xi_0]$. Der gælder så fra sætning B.7, at $\mathbf{V}(\mathbf{I}(G))$ er en ikke-tom mængde, da $1 \notin \mathbf{I}(G)$. Det vil sige at der findes minimum et ξ og ξ_0 så $p_1(\xi), \ldots, p_\kappa(\xi) = 0$ og hermed er betingelse *1.* fra sætning 4.1 opfyldt. Der gælder desuden at $g(\xi, \xi_0) = 0$, hvilket vil sige at $\xi_0 \neq 0$, og at

$$\prod_{k=1}^{|\mathcal{R}|} g_k(\xi) \neq 0.$$

Af ovenstående gælder der derfor, at $g_k(\xi) \neq 0$ for alle $k \in \{1, \ldots, |\mathcal{R}|\}$, hvilket vil sige, at betingelse *2.* fra sætning 4.1 er opfyldt, og netværkskodningsproblemet har en løsning.

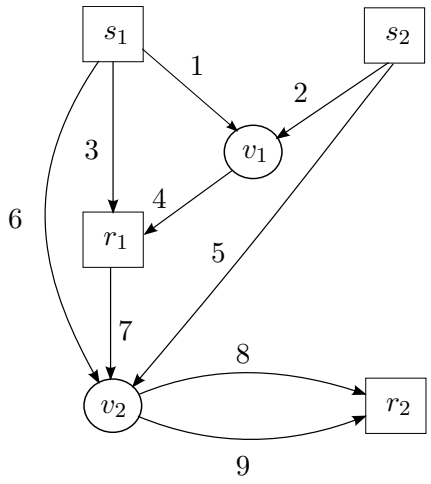
Antag, at netværkskodningsproblemet har en løsning, men at $\mathbf{I}(G) = \mathbb{F}_q[\xi, \xi_0]$. Der fås fra sætning B.7, at $\mathbf{V}(\mathbf{I}(G)) = \emptyset$, og der findes ingen ξ og ξ_0 der opfylder betingelserne fra sætning 4.1, hvilket er imodstrid med at netværkskodningsproblemet har en løsning.

Fra ovenstående fås altså at $1 \notin \mathbf{I}(G)$, og hermed at $\mathbf{V}(\mathbf{I}(G)) \neq \emptyset$, for at netværkskodningsproblemet har en løsning. □

Ved brug af sætning 4.2 er det muligt at afgøre om et lineært netværkskodningsproblem har en løsning ved at konstruere idealet $\mathbf{I}(G)$ og herefter bestemme en basis for $\mathbf{I}(G)$. Denne Gröbner-basis kan fastsættes ved hjælp af Buchbergers Algoritme, algoritme 1, og reduceres ved at bruge definition 2.7. Hvis den reducerede Gröbner-basis er forskellig fra $\{1\}$ vil der gælde at der findes en løsning til det lineære netværksproblem.

4.1 Eksempler på Generelle Netværkskodningsproblemer

I det følgende illustreres teorien omkring det generelle netværkskodningsproblem gennem to eksempler. I disse eksempler ses der på det samme netværk,



Figur 4.1: Netværk hørende til eksemplerne 4.3 og 4.4.

men med to forskellige netværkskodningsproblemer. I det ene vil der ikke være en løsning, mens der ved det andet eksisterer en løsning.

Det følgende eksempel illustrerer netværkskodningsproblemet uden løsning.

Eksempel 4.3. Lad det lineære netværk med orienteret graf i figur 4.1 være givet, hvor $V = \{s_1, s_2, \ldots, r_2\}$ og $E = \{1, \ldots, 9\}$. Lad meddelelsesrummet være givet ved $\mathcal{X} = \{X_1, X_2, X_3, X_4\}$, modtagermængden er $\mathcal{R} = \{r_1, r_2\}$ og kildemængden er $\mathcal{S} = \{s_1, s_2\}$. Kildefunktion er givet ved

$$K(X) = \begin{cases} s_1 \text{ for } X \in \{X_1, X_2\} \\ s_2 \text{ for } X \in \{X_3, X_4\} \end{cases} . \tag{4.2}$$

For demandfunktionen, D, haves at

$$\begin{aligned} D(r_1) &= \mathcal{X}_{r_1} = \{X_1, X_2\}, \\ D(r_2) &= \mathcal{X}_{r_2} = \{X_3, X_4\}. \end{aligned} \tag{4.3}$$

Før overgangsmatricen M konstrueres for netværkskodningsproblemet sikres der, at der eksisterer 2 disjunkte veje i netværket fra $\mathcal{S}$ til hver modtager i $\mathcal{R}$. Hvis ikke dette er tilfældet kan det direkte siges at netværket ikke har en løsning. For netværket givet i figur 4.1 er det muligt at finde 4 disjunkte veje, hvor to går til r_1 og to går til r_2, et eksempel på sådanne veje er $\{(1,4),(3),(5,8),(6,9)\}$. Her går $(1,4)$ og (3) til r_1, mens $(5,8)$ og $(6,9)$ går til r_2. Heraf har netværkskodningsproblemet måske en løsning. For at bestemme overgangsmatricen M konstrueres indkodnings-, kantovergangs- og

dekodningsmatricen. Disse bestemmes ud fra netværket og der fås indkodningsmatrix

$$A = \begin{bmatrix} a_{11} & 0 & a_{13} & 0 & 0 & a_{16} & 0 & 0 & 0 \\ a_{21} & 0 & a_{23} & 0 & 0 & a_{26} & 0 & 0 & 0 \\ 0 & a_{32} & 0 & 0 & a_{35} & 0 & 0 & 0 & 0 \\ 0 & a_{42} & 0 & 0 & a_{45} & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{4.4}$$

kantovergangsmatrix

$$F = \begin{bmatrix} 0 & 0 & 0 & f_{14} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & f_{24} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & f_{37} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & f_{47} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{58} & f_{59} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{68} & f_{69} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & f_{78} & f_{79} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{4.5}$$

og dekodingsmatrix

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b_{31} & b_{32} & 0 & 0 & 0 & 0 & 0 & 0 \\ b_{41} & b_{42} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & b_{87} & b_{88} \\ 0 & 0 & 0 & 0 & 0 & 0 & b_{97} & b_{98} \end{bmatrix}. \tag{4.6}$$

Ud fra overgangsmatricerne fås

$$\xi = (a_{11}, a_{22}, \ldots, a_{26}, f_{14}, f_{24}, \ldots, f_{79}, b_{31}, b_{32}, \ldots, b_{98}) .$$

Af (4.1) skal $(I-F)^{-1}$ bestemmes inden overgangsmatricen M kan bestemmes. Dette er gjort i Maple, og her fås at

$$(I-F)^{-1} = \begin{bmatrix} 1 & 0 & 0 & f_{14} & 0 & 0 & f_{14}f_{47} & f_{14}f_{47}f_{78} & f_{14}f_{47}f_{79} \\ 0 & 1 & 0 & f_{24} & 0 & 0 & f_{24}f_{47} & f_{24}f_{47}f_{78} & f_{24}f_{47}f_{79} \\ 0 & 0 & 1 & 0 & 0 & 0 & f_{37} & f_{37}f_{78} & f_{37}f_{79} \\ 0 & 0 & 0 & 1 & 0 & 0 & f_{47} & f_{47}f_{78} & f_{47}f_{79} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & f_{58} & f_{59} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & f_{68} & f_{69} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & f_{78} & f_{79} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{4.7}$$

Ved brug af (4.4), (4.7) og (4.6) konstrueres overgangsmatricen

$$M = \begin{bmatrix} \star & \star & 0 & 0 & 0 & 0 & \bullet & \bullet \\ \star & \star & 0 & 0 & 0 & 0 & \bullet & \bullet \\ \bullet & \bullet & 0 & 0 & 0 & 0 & \star & \star \\ \bullet & \bullet & 0 & 0 & 0 & 0 & \star & \star \end{bmatrix}, \tag{4.8}$$

hvor $\star$ og $\bullet$ repræsenterer komponenterne, der ikke direkte er nul ud fra konstruktionen. Komponenterne $\bullet$ skal evaluere til nul, dvs. at disse giver polynomierne $p_1(\xi), \ldots, p_8(\xi)$. Komponenterne $\star$ samles i matricer M_1 og M_2. Her gælder der, at de fire komponenter i øverste venstre hjørne angiver M_1 da de fire første søjler hører til modtager r_1. Tilsvarende angiver komponenterne i nederste højre hjørne M_2. Der gælder at M_1 og M_2 skal være regulære. Lad $g_1(\xi) = \det(M_1)$ og $g_2(\xi) = \det(M_2)$, så fås at $g(\xi) = 1 - \xi_0 \det(M_1)\det(M_2)$.

Af sætning 4.2 gælder der så, at det lineære netværkskodningsproblem har en løsning, hvis

$$\mathbf{V}(\mathbf{I}(G)) = \mathbf{V}\left(\langle p_1, \ldots, p_8, g\rangle\right) \neq \emptyset\,.$$

Dette afgøres ved at bestemme en Gröbner-basis til $\mathbf{I}(G)$, hvor den monomielle ordning er valgt til at være den leksikografiske ordning med $a_{11} >_{\text{leks}} a_{22} >_{\text{leks}} \cdots >_{\text{leks}} b_{98} >_{\text{leks}} \xi_0$. Den reducerede Gröbner-basis for idealet $\mathbf{I}(G)$ findes ved hjælp af Maple efter samme metode som brugt i eksempel D.1 i bilag D. Der fås at Gröbner-basen for $\mathbf{I}(G)$ er $\{1\}$ og hermed gælder der, at $\mathbf{V}(\mathbf{I}(G)) = \emptyset$ og netværkskodningsproblemet har derfor ikke en løsning. ▲

Ved at lave en lille ændring i netværkskodningsproblemet givet i eksempel 4.3 er det muligt at få en løsning til det givne netværk. Dette illustreres i følgende eksempel.

Eksempel 4.4. Vi lader netværket, V, E, $\mathcal{S}$, $\mathcal{R}$ og kildefunktionen, K, være ligesom i eksempel 4.3, men demandfunktionerne givet i (4.3) ændres til

$$\begin{aligned} D(r_1) &= \mathcal{X}_{r_1} = \{X_1, X_3\}\,, \\ D(r_2) &= \mathcal{X}_{r_2} = \{X_2, X_4\}\,. \end{aligned}$$

Idet netværket og kildefunktionen ikke er ændret, er indkodnings- og kantovergangsmatricen fra foregående eksempel uændret, så A er givet ved (4.4) og F ved (4.5). Heraf fås også at $(I - F)^{-1}$ stadig er givet ved (4.7). For

dekodningsmatricen fås

$$\tilde{B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ b_{31} & 0 & b_{33} & 0 & 0 & 0 & 0 & 0 \\ b_{41} & 0 & b_{43} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & b_{86} & 0 & b_{88} \\ 0 & 0 & 0 & 0 & 0 & b_{96} & 0 & b_{98} \end{bmatrix}.$$

For dette netværkskodningsproblem bliver overgangsmatricen

$$\tilde{M} = \begin{bmatrix} \star & 0 & \star & 0 & 0 & \bullet & 0 & \bullet \\ \bullet & 0 & \bullet & 0 & 0 & \star & 0 & \star \\ \star & 0 & \star & 0 & 0 & \bullet & 0 & \bullet \\ \bullet & 0 & \bullet & 0 & 0 & \star & 0 & \star \end{bmatrix}, \tag{4.9}$$

hvor $\star$ og $\bullet$ har samme betydning som i eksempel 4.3. Det vil sige at der igen haves otte polynomier $\tilde{p}_1(\xi), \ldots, \tilde{p}_8(\xi)$ fra $\bullet$ - komponenterne, som skal evaluere til nul. Desuden fås

$$\tilde{M}_1 = \begin{bmatrix} M_{11^1} & M_{13^1} \\ M_{31^1} & M_{33^1} \end{bmatrix} \text{ og } \tilde{M}_2 = \begin{bmatrix} M_{22^2} & M_{24^2} \\ M_{42^2} & M_{44^2} \end{bmatrix},$$

som skal være regulære. Heraf bestemmes $\tilde{g}_1 = \det(\tilde{M}_1)$, $\tilde{g}_2 = \det(\tilde{M}_2)$ og $\tilde{g} = 1 - \xi_0 \det(\tilde{M}_1)\det(\tilde{M}_2)$.

Idealet for netværkskodningsproblemet bliver så

$$\mathbf{I}(G) = \langle \tilde{p}_1, \ldots, \tilde{p}_8, \tilde{g} \rangle,$$

som vi ønsker skal have en varietet forskellig fra den tomme mængde. Dette bestemmes igen vha. af Maple og der fås, at Gröbner-basen er forskellig fra $\langle 1 \rangle$. Det vil sige at $\mathbf{V}(\mathbf{I}(G))$ er forskellig fra den tomme mængde. Gröbner-basen består af 34 polynomier over ringen $\mathbb{F}_q[\xi]$. Disse polynomier er vedlagt i Bilag D. Altså haves der en løsning til netværkskodningsproblemet. Dog er denne løsning imidlertid ikke fundet, men det vides at den eksisterer. ▲

Del II

Fejlkorrigerende Netværkskodning

Del I indeholdt en grundlæggende gennemgang af netværkskodningsproblemet både i det multicast og det generelle tilfælde. Her var fokus især rettet imod, hvornår et netværk havde en løsning, hvilket var muligt at bestemme ud fra netværkets topologi vha. Gröbner-basis teori. Resultatet om eksistensen af en løsning byggede på antagelsen om, at der blev sendt over en støjfri kanal, da det ikke var muligt at fejlkorrigere. I anden del af rapporten betragtes, i modsætning til del I, netværker hvor det er muligt at foretage fejlkorrigering. Vi antager i denne del, at netværkets topologi er ukendt, hvilket vil sige at overgangskoefficienter, kantpolynomier og lignende fra kapitel 3 ikke kan bestemmes, desuden foretages alt kodning vilkårligt. Netværket betragtes derfor som én stor kanal, betegnet operatorkanalen, som giver anledning til fejl og sletninger i transmission. Fejlene kan opstå ved at forstyrrende information tilføres det oprindelige data, enten ved en fejl i netværket eller en bevidst tilførsel fra en udenforstående kilde. Sletninger kan opstå, hvis den vilkårlige kodning ikke udføres optimalt. Altså at en eller flere koefficienter vælges forkert, således at output ved modtageren ikke er en uafhængig mængde af information. En anden årsag til sletninger er, at flowet til en modtager er mindre end antallet af informationsbeskeder, der ønskes transmitteret, hvorved output ved modtageren vil være mindre end input i kanalen.

I denne del betragtes to fejlkorrigeringsmetoder; Minimumsafstandsdekodning samt liste-L-dekodning. I kapitel 6 defineres en kode kaldet KK-koden, som anvender minimumsafstandsdekodning og som tilnærmelsesvis når Singleton Grænsen. Denne kode udvides i kapitel 9 til en kode kaldet MV-koden som er anvendelig ved liste-L-dekodning. Fundamentet for begge kodekonstruktioner er lineariserede polynomier som præsenteres i kapitel 5. Sidst i del II betragtes KK-kodens og MV-kodens fejlretningsevner i forhold til pakkehastigheden R^*.

Kapitel 5

Lineariserede Polynomier

Dette kapitel omhandler lineariserede polynomier, som senere benyttes i konstruktionen af koder hvis kodeord er underrum af et vektorrum. Vi indleder med en definition af lineariserede polynomier.

Definition 5.1 (Lineariseret polynomium)**.** Lad $\mathbb{F}_{q^m}$ være givet. Et polynomium $L(x)$ over $\mathbb{F}_{q^m}$ på formen

$$L(x) = \sum_{i=0}^{d} a_i x^{q^i} \ , \tag{5.1}$$

med koefficienterne $a_1, \ldots, a_d \in \mathbb{F}_{q^m}$ betegnes et linearseret polynomium. Hvis alle koefficienter er nul, således at $L(x)$ er nulpolynomiet, så skrives $L(x) = 0$. Desuden, hvis $L_1(x) - L_2(x) = 0$ så skrives at $L_1(x) = L_2(x)$.

Mængden af lineariserede polynomier over $\mathbb{F}_{q^m}$ betegnes $\mathscr{L}_{q^m}[x]$, mens $\mathscr{L}^k_{q^m}[x]$ betegner mængden af lineariserede polynomier over $\mathbb{F}_{q^m}$ af grad højest q^{k-1}.

Lemma 5.2. *Lad $L_1(x), L_2(x) \in \mathscr{L}_{q^m}[x]$ og $\alpha_1, \alpha_2 \in \mathbb{F}_{q^m}$, så gælder at*

i. For $\lambda_1, \lambda_2 \in \mathbb{F}_q$ opfylder $L_1(x)$ linearitetsbetingelsen.

$$L_1(\lambda_1\alpha_1 + \lambda_2\alpha_2) = \lambda_1 L_1(\alpha_1) + \lambda_2 L_1(\alpha_2) \ .$$

ii. Enhver $\mathbb{F}_{q^m}$-linear kombination $\alpha_1 L_1(x) + \alpha_2 L_2(x)$ er et lineariseret polynomium over $\mathbb{F}_{q^m}$.

iii. Det sammensatte polynomium af to lineariserede polynomier; $L_1 \circ L_2(x) = L_1(L_2(x))$ *er et lineariseret polynomium over* $\mathbb{F}_{q^m}$.

Bevis. Lad

$$L_1(x) = \sum_{i=0}^{d_1} a_i x^{q^i} \quad \text{og} \quad L_2(x) = \sum_{j=0}^{d_2} b_j x^{q^j} \ , \tag{5.2}$$

og lad $\alpha_1, \alpha_2 \in \mathbb{F}_{q^m}$.

i. Da $\lambda_1, \lambda_2 \in \mathbb{F}_q$ gælder at $\lambda_1^{q^j} = \lambda_1$ og $\lambda_2^{q^j} = \lambda_2$. For et lineariseret polynomium fås derfor at

$$\begin{aligned} L_1(\lambda_1\alpha_1 + \lambda_2\alpha_2) &= \sum_{i=0}^{d_1} a_i(\lambda_1\alpha_1 + \lambda_2\alpha_2)^{q^i} \\ &= \sum_{i=0}^{d_1} a_i\lambda_1\alpha_1^{q^i} + \sum_{i=0}^{d_1} a_i\lambda_1\alpha_1^{q^i} = \lambda_1 L_1(\alpha_1) + \lambda_2 L_1(\alpha_2) \ . \end{aligned}$$

ii. For en $\mathbb{F}_{q^m}$-linear kombination fås

$$\begin{aligned} \alpha_1 L_1(x) + \alpha_2 L_2(x) &= \alpha_1 \sum_{i=0}^{d_1} a_i x^{q^i} + \alpha_2 \sum_{j=0}^{d_2} b_j x^{q^j} \\ &= \sum_{i=0}^{d_1} \alpha_1 a_i x^{q^i} + \sum_{j=0}^{d_2} \alpha_2 b_j x^{q^j} \\ &= \sum_{k=0}^{d} (\alpha_1 a_k + \alpha_2 b_k) x^{q^k} \ , \end{aligned} \tag{5.3}$$

hvor $d = \max\{d_1, d_2\}$ og $a_{d_1+1}, \ldots, a_d = 0$ hvis $d = d_2$ eller $b_{d_2+1}, \ldots, b_d = 0$ hvis $d = d_1$.

iii. Det sammensatte polynomium giver

$$\begin{aligned} L_1 \circ L_2(x) &= \sum_{i=0}^{d_1} a_i \left(\sum_{j=0}^{d_2} b_j x^{q^j} \right)^{q^i} \\ &= \sum_{i=0}^{d_1} \sum_{j=0}^{d_2} a_i b_j^{q^i} x^{q^{j+i}} = \sum_{k=0}^{d_1+d_2} c_k x^{q^k} \text{ hvor} \\ c_k &= \sum_{i=0}^{k} a_i b_{k-i}^{q^i} \ . \end{aligned} \tag{5.4}$$

Specielt ses at det sammensatte polynomium har grad $q^{d_1+d_2}$. □

Det, at et lineariseret polynomium opfylder ovenstående lemma er netop bevæggrunden for betegnelsen "et lineariseret polynomium". Produktet af to linearisered polynomier er derimod ikke nødvendigvis et lineariseret polynomium. Lad $L_1(x)$ og $L_2(x)$ være givet som i (5.2), så fås at

$$\begin{aligned} L_1(x)L_2(x) &= \left(\sum_{i=0}^{d_1} a_i x^{q^i}\right)\left(\sum_{j=0}^{d_2} b_j x^{q^j}\right) \\ &= a_0b_0x^{q^0+q^0} + a_0b_1x^{q^0+q^1} + a_1b_0x^{q^1+q^0} + \cdots + a_{d_1}b_{d_2}x^{q^{d_1}+q^{d_2}} \\ &= \sum_{h=0}^{d_1+d_2} \sum_{\substack{i+j=h \\ i\leq d_1, j\leq d_2}} a_1b_jx^{q^i+q^j} \ , \end{aligned}$$

hvilket ikke altid kan omskrives til formen (5.1).

Sætning 5.3. *Mængden $\mathscr{L}_{q^m}[x]$ med de to binære operationer addition $+$ og kompositionen $\circ$ giver en ikke-kommutativ ring.*

Bevis. Lad $L_1, L_2, L_3 \in \mathscr{L}_{q^m}[x]$ hvor $L_1(x) = \sum_{i=0}^{d_1} a_i x^{q^i}$, $L_2(x) = \sum_{j=0}^{d_2} b_j x^{q^j}$ og $L_3(x) = \sum_{h=0}^{d_3} c_h x^{q^h}$. Ligning (5.3) giver at $(\mathscr{L}_{q^m}, +)$ er lukket under addition, mens ligning (5.4) giver at $(\mathscr{L}_{q^m}, \circ)$ er lukket under kompositionen. At $(\mathscr{L}_{q^m}, +)$ er associativ følger ligeledes af (5.3) da

$$\begin{aligned} (L_1(x) + L_2(x)) + L_3(x) &= \sum_{k=0}^{d}(a_k + b_k)x^{q^k} + \sum_{h=0}^{d_3} c_h x^{q^h} \\ &= \sum_{k=0}^{d'}(a_k + b_k + c_k)x^{q^k} = \sum_{i=0}^{d_1} a_i x^{q^i} + \sum_{k=0}^{d''}(b_k + c_k)x^{q^k} \\ &= L_1(x) + (L_2(x) + L_1(x)) \ , \end{aligned}$$

hvor $d = \max\{d_1, d_2\}$, $d' = \max\{d_1, d_2, d_3\}$ og $d'' = \max\{d_2, d_3\}$. Dette er et velkendt resultat for polynomier over en polynomiumsring. Desuden gælder fra (5.4) at

$$
\begin{aligned}
(L_1 \circ L_2(x)) \circ L_3(x) &= \left(\sum_{i=0}^{d_1} a_i \left(\sum_{j=0}^{d_2} b_j x^{q^j}\right)^{q^i}\right) \circ \left(\sum_{h=0}^{d_3} c_h x^{q^h}\right) \\
&= \sum_{i=0}^{d_1}\sum_{j=0}^{d_2} a_i b_j^{q^i} \left(\sum_{h=0}^{d_3} c_h x^{q^h}\right)^{q^{i+j}} \\
&= \sum_{i=0}^{d_1}\sum_{j=0}^{d_2}\sum_{h=0}^{d_3} a_i b_j^{q^i} c_h^{q^{i+j}} x^{q^{i+j+h}} \\
&= \sum_{i=0}^{d_1} a_i \left(\sum_{j=0}^{d_2}\sum_{h=0}^{d_3} b_j c_h^{q^j} x^{q^{j+h}}\right)^{q^i} \\
&= \left(\sum_{i=0}^{d_1} a_i x^{q^i}\right) \circ \left(\sum_{j=0}^{d_2}\sum_{h=0}^{d_3} b_j c_h^{q^j} x^{q^{j+h}}\right) \\
&= \left(\sum_{i=0}^{d_1} a_i x^{q^i}\right) \circ \left(\sum_{j=0}^{d_2} b_j \left(\sum_{h=0}^{d_3} c_h x^{q^h}\right)^{q^j}\right) \\
&= L_1 \circ (L_2 \circ L_3(x)) \ ,
\end{aligned}
$$

hvorfor $(\mathscr{L}_{q^m}, \circ)$ også er associativ.

Betragt $L_1(x)$. Om koefficienterne i $L_1(x)$ gælder $a_i \in \mathbb{F}_{q^m}$ for $i \in \{1, \ldots, d_1\}$, så der findes et neutralt element $e_i \in \mathbb{F}_{q^m}$, således at $a_i + e_i = a_i$ for alle i. Ligeledes findes et element $g_i \in \mathbb{F}_{q^m}$ hvorom der gælder at $a_i + g_i = 0$ for alle i. Konstruer $L_e(x) = \sum_{i=0}^{d_1} e_i x^{q^i}$ og $L_g(x) = \sum_{i=0}^{d_1} g_i x^{q^i}$. Heraf fås

$$
\begin{aligned}
L_1(x) + L_e(x) &= \sum_{i=0}^{d_1} a_i x^{q^i} + \sum_{i=0}^{d_1} e_i x^{q^i} \\
&= \sum_{i=0}^{d_1} (a_i + e_i) x^{q^i} = \sum_{i=0}^{d_1} a_i x^{q^i} = L_1(x) \quad \text{og} \\
L_1(x) + L_g(x) &= \sum_{i=0}^{d_1} a_i x^{q^i} + \sum_{i=0}^{d_1} g_i x^{q^i} \\
&= \sum_{i=0}^{d_1} (a_i + g_i) x^{q^i} = \sum_{i=0}^{d_1} 0 x^{q^i} = 0 \ ,
\end{aligned}
$$

så der findes en additiv identitet og invers for $\mathscr{L}_{q^m}[x]$.

Definer et lineariseret polynomium ved $L_i(x) = 1x^{q^0} + \sum_{i=1}^{d_1} 0x^{q^i}$, hvor 0 er nul-elementet i $\mathbb{F}_{q^m}$. Desuden gælder at $a_i \cdot 1 = a_i$ for alle $i \in \{1, \ldots, d_1\}$.

Heraf

$$\begin{aligned} L_1 \circ L_i(x) &= \sum_{i=0}^{d_1} a_i \left(1x^{q^0} + \sum_{i=1}^{d_1} 0x^{q^i} \right)^{q^i} \\ &= \sum_{i=0}^{d_1} a_i 1x^{q^i} + \sum_{i=1}^{d_1} a_i 0^{qi} x^{q^{i+i}} = L_1(x) \ , \end{aligned}$$

hvorfor der findes en identitet for $(\mathscr{L}_{q^m}, \circ)$.

De distributive love gælder også, hvilket ses følgende;

$$\begin{aligned} L_1 \circ (L_2(x) + L_3(x)) &= \sum_{i=0}^{d_1} a_i \left(\sum_{j=0}^{d_2} b_j x^{q^j} + \sum_{h=0}^{d_3} c_h x^{q^h} \right)^{q^i} \\ &= \sum_{i=0}^{d_1} a_i \left(\sum_{k=0}^{d} (b_k + c_k) x^{q^k} \right)^{q^i} \\ &= \sum_{i=0}^{d_1} \sum_{k=0}^{d} (a_i b_k^{q^i} + a_i c_k^{q^i}) x^{q^{k+i}} \\ &= \sum_{i=0}^{d_1} \sum_{k=0}^{d_2} a_i b_k^{q^i} x^{q^{k+i}} + \sum_{i=0}^{d_1} \sum_{k=0}^{d_3} a_i c_k^{q^i} x^{q^{k+i}} \\ &= L_1 \circ L_2(x) + L_1 \circ L_3(x) \ , \end{aligned}$$

hvor $d = \max\{d_2, d_3\}$.

Sammenlagt giver det ovenstående, at mængden $\mathscr{L}_{q^m}$ former en ikke-kommutativ ring under addition og komposition. □

Lemma 5.4. *Lad d være et positivt heltal, og lad $f, g \in \mathscr{L}_{q^m}^d[x]$. Hvis $\alpha_1, \ldots, \alpha_d$ er lineært uafhængige elementer i et udvidelelseslegeme af $\mathbb{F}_{q^m}$, hvorom der gælder, at $f(\alpha_i) = g(\alpha_i)$ for $i \in \{1, \ldots, d\}$ så er $f(x) = g(x)$. [KK08, Lemma 11]*

Bevis. Definer $h(x) = f(x) - g(x)$, så har $h(x)$ elementerne $\alpha_1, \ldots, \alpha_d$ som nulpunkter. Desuden er alle lineære kombinationer af $\alpha_1, \ldots, \alpha_d$ også nulpunkter for $h(x)$, da $h(x)$ er et lineariseret polynomium. Heraf har $h(x)$ mindst q^d forskellige nulpunkter. Dog er graden af $h(x)$ mindre end q^d, så $h(x)$ her flere nulpunkter end dets grad. Dette er kun muligt hvis $h(x) = 0$, hvorfor $f(x) = g(x)$. □

5.1 Divisionsalgoritme for Lineariserede Polynomier

Vi har til tider behov for at kunne dividere lineariserede polynomier med hinanden. Lad $L_1(x)$ og $L_2(x)$ være lineariserede polynomier, så findes entydige lineariserede polynomier $q_R(x), q_L(x)$ og $r_R(x), r_L(x)$ således at

$$L_1(x) = L_2(q_R(x)) + r_R(x) = q_L(L_2(x)) + r_L(x) \ ,$$

hvor $r_L(x) = 0$ eller $\deg(r_L(x)) < \deg(L_2(x))$ og $r_R(x) = 0$ eller $\deg(r_R(x)) < \deg(L_2(x))$. For at bestemme $q_R(x), q_L(x)$ og $r_R(x), r_L(x)$ anvendes den højre divisionsalgoritme eller den venstre divisionsalgoritme. Begge algoritmer er rekursive. Nedenstående algoritme fra [KK08] er den højre divisionsalgoritme. Den venstre divisionsalgoritme **vdiv**$(a(x), b(x))$ er tilsvarende med den forskel, at polynomiet $t(x)$ defineres til

$$t(x) := \frac{a_d}{b_e^{q^{d-e}}} x^{q^{d-e}} \ ,$$

og $a'(x), b'(x)$ defineres til

$$a'(x) := a(x) - t(b(x)); \qquad b'(x) := b(x) \ .$$

Vi benytter ikke den venstre divisionsalgoritme i denne rapport, men da dens funktion er lignende den højre divisionsalgoritme er dette blot er spørgsmål om valg af metode.

Algoritme 2 Højre division af lineariserede polynomier; **hdiv**$(a(x), b(x))$.

Input: Et par $a(x), b(x)$ af lineariserede polynomier over $\mathbb{F}_{q^m}$, hvor $b(x) \neq 0$.
Lad $q(x) := 0$;
if $\deg(a(x)) < \deg(b(x))$ **then**
    $r(x) := a(x)$;
else
    $d := \deg(a(x))$; $e := \deg(b(x))$;
    $a_d := \mathrm{LC}(a(x))$; $b_e := \mathrm{LC}(b(x))$;
    $t(x) := \frac{a_d}{b_e} q^{m-e} x^{q^{d-e}}$;
    $a'(x) := a(x) - b(t(x))$; $b'(x) := b(x)$;
    Lad $\{q'(x), r'(x)\} :=$ **hdiv**$(a'(x), b'(x))$;
    $q(x) := q'(x) + t(x)$; $r(x) := r'(x)$;
end if
Output: Et par $q(x), r(x)$ af lineariserede polynomier over $\mathbb{F}_{q^m}$.

Sætning 5.5. *Lad $L_1(x), L_2(x)$ være lineariserede polynomier over $\mathbb{F}_{q^m}$. Så gælder at Algoritme 2 med $L_1(x), L_2(x)$ som input konstruerer lineariserede polynomier $q, r \in \mathbb{F}_{q^m}[x]$, således at*

$$L_1(x) = L_2(q(x)) + r(x) \ ,$$

hvor $r(x) = 0$ eller $\deg(r(x)) < \deg(L_2(x))$.

Bevis. Vi viser ved induktion efter graden af $L_1(x)$, at $q(x)$ og $r(x)$ eksisterer. Lad $L_1(x) = \sum_{i=0}^{d_1} a_i x^{q^i}$ og $L_2(x) = \sum_{j=0}^{d_2} b_j x^{q^j}$.

Basisskridt: For $d_1 = 0$ haves at

$$L_1(x) = a_0 x^{q^0} = a_0 x \ .$$

Hvis $\deg(L_1(x)) < \deg(L_2(x))$ fås at $r(x) = L_1(x)$ og $q(x) = 0$ hvorfor

$$L_1(x) = L_2(0) + L_1(x) \ .$$

Hvis $\deg(L_1(x)) \geq \deg(L_2(x))$, så må graden af $L_2(x)$ være $q^{d_2} = q^0 = 1$ og i dette tilfælde er $L_2(x) = b_0 x^{q^0}$. Algoritmen definerer da

$$t(x) := \left(\frac{a_0}{b_0}\right)^{q^m} x^{q^0} = \frac{a_0}{b_0} x \ ,$$

hvorved $L_1'(x) = a_0 x - b_0 \left(\frac{a_0}{b_0} x\right)^{q^0} = 0$. Heraf er $r(x) = r'(x) = 0$ og $q(x) = t(x) = \frac{a_0}{b_0} x$. Dette giver at

$$L_1(x) = L_2(q(x)) + r(x) = b_0 \left(\frac{a_0}{b_0} x\right)^{q^0} + 0 = a_0 x \ ,$$

hvorfor $q(x)$ er et lineariseret polynomium konstrueret fra $L_1(x)$ og $L_2(x)$ mens $r(x) = 0$.

Induktionsantagelse: Vi antager at algoritme 2 producerer lineariserede polynomier $q(x)$ og $r(x)$, således at $L_1(x) = L_2(q(x)) + r(x)$ for $d_1 \leq n$.

Induktionsskridt: Antag at $d_1 = n + 1$. Det vil sige at $L_1(x) = \sum_{i=1}^{n+1} a_i x^{q^i}$, hvor $a_{n+1} \neq 0$. Hvis $\deg(L_1(x)) < \deg(L_2(x))$ følger tilsvarende basisskridtet, at $r(x) = L_1(x)$ og $q(x) = 0$, hvorfor $q(x)$ og $r(x)$ er lineariserede polynomier. Så vi antager at $\deg(L_1(x)) \geq \deg(L_2(x))$. Algoritme 2 bestemmer

$$t(x) := \left(\frac{a_{n+1}}{b_{d_2}}\right)^{q^{m-d_2}} x^{q^{n+1-d_2}}; \quad q(x) = t(x) + q'(x); \quad r(x) = r'(x); \ (5.5)$$

hvor $q'(x)$ og $r'(x)$ er output fra algoritme 2 med $L_1'(x)$ og $L_2'(x)$ som input. Der gælder fra konstruktionen af $L_1'(x)$ at $\deg(L_1'(x)) < \deg(L_1(x)) = n+1$. Dette ses ved

$$\begin{aligned}
L_1'(x) &= L_1(x) - L_2(t(x)) = L_1(x) - L_2\left(\left(\frac{a_{n+1}}{b_{d_2}}\right)^{q^{m-d_2}} x^{q^{n+1-d_2}}\right) \\
&= \sum_{i=0}^{n+1} a_i x^{q^i} - \sum_{j=0}^{d_2-1} b_j \left(\left(\frac{a_{n+1}}{b_{d_2}}\right)^{q^{m-d_2}} x^{q^{n+1-d_2}}\right)^{q^j} - b_{d_2}\left(\frac{a_{n+1}}{b_{d_2}}\right)^{q^m} x^{q^{n+1}} \\
&= a_{n+1}x^{q^{n+1}} + \sum_{i=0}^{n} a_i x^{q^i} - \sum_{j=0}^{d_2-1} b_j \left(\frac{a_{n+1}}{b_{d_2}}\right)^{q^{m-d_2+j}} x^{q^{n+1-d_2+j}} - a_{n+1}x^{q^{n+1}} \\
&= \sum_{i=0}^{n} a_i x^{q^i} - \sum_{j=0}^{d_2-1} b_j \left(\frac{a_{n+1}}{b_{d_2}}\right)^{q^{m-d_2+j}} x^{q^{n+1-d_2+j}},
\end{aligned}$$

så $L_1'(x)$ har højest grad n. Fra induktionsantagelsen følger så at $q'(x)$ og $r'(x)$ er lineariserede polynomier. Da $t(x)$ i (5.5) er et lineariseret polynomium og da en sum af to lineariserede polynomier er et nyt lineariseret polynomium, fås at $q(x)$ og $r(x)$ i (5.5) også bliver lineariserede polynomier.

For at være sikre på at algoritme 2 giver et output, skal algoritmen afslutte på et tidspunkt. Lad $a(x), b(x)$ være input. Hvis $\deg(a(x)) < \deg(b(x))$ allerede ved algoritmens start, så afslutter algoritmen med det samme ved at definere $q(x) := 0$ og $r(x) := a(x)$. Ellers defineres $a'(x)$ og $b'(x)$ og disse polynomier behandles som input ved endnu et gennemløb af algoritme 2. Som vist ovenfor er graden af $a'(x)$ mindre end graden af $a(x)$, så ved hver rekursivt gennemløb falder graden af input polynomiet $a(x)$. Desuden er $b'(x) := b(x)$ så $b'(x)$ har samme grad som $b(x)$. Heraf ændres graden af $b'(x)$ ikke ved det rekursive gennemløb og algoritmen vil på et tidspunkt opnå at $\deg(a(x)) < \deg(b(x))$, hvorved algoritmen afsluttes. □

Proposition 5.6. *Lad $L_1(x)L_2(x) \in \mathscr{L}_{q^m}[x]$ være givet. Der eksisterer entydige lineariserede polynomier $q(x), r(x)$ således at*

$$L_1(x) = L_2(q(x)) + r(x) ,$$

hvor $r(x) = 0$ eller $\deg(r(x)) < \deg(L_2(x))$.

Bevis. Eksistenen af $q(x)$ og $r(x)$ følger af sætning 5.5, så følgende vises kun entydigheden. Lad $q(x), r(x)$ og $q'(x), r'(x)$ være output fra algoritme 2 med input $L_1(x), L_2(x)$ således at

$$L_1(x) = L_2(q(x)) + r(x) = L_2(q'(x)) + r'(x) ,$$

hvor $\deg(r(x)) = 0$ eller $\deg(r(x)) < \deg(L_2(x))$ og $\deg(r'(x)) = 0$ eller $\deg(r'(x)) < \deg(L_2(x))$. Ved omskrivning ses

$$\begin{aligned} r'(x) - r(x) &= L_2(q(x)) - L_2(q'(x)) \\ &= L_2(q(x) - q'(x)) \ . \end{aligned}$$

Da både $r(x)$ og $r'(x)$ har grad mindre end $\deg(L_2(x))$, så gælder at $r'(x) - r(x)$ har grad mindre end $\deg(L_2(x))$. Men konstruktionen af sammensatte polynomier giver at $\deg(L_2\left(q(x) - q'(x)\right)) \geq \deg(L_2(x))$, hvorfor der må gælde at $r'(x) - r(x) = 0$. Heraf er $r'(x) = r(x)$. Desuden er $L_2(q(x) - q'(x)) = 0$ kun muligt hvis alle koefficienterne er nul-elementer og da $L_2(x) \neq 0$ pr. antagelse, må $q(x) - q'(x) = 0$, hvorfor $q(x) = q'(x)$. □

Bemærkning 5.7. Hvis et lineariseret polynomium over $\mathbb{F}_k$, hvor $k = q^m$, er givet med koefficienter i $\mathbb{F}_k$, er det ud fra koefficienterne muligt at definere værdierne for q og m. I nogle tilfælde kan der være flere muligheder, f.eks. hvis de benyttede koefficienterne alle ligger i $\mathbb{F}_q$, så kan legemet betragtes både som $\mathbb{F}_{q^m}$ eller $\mathbb{F}_{(q^j)^{\frac{m}{j}}}$ hvor $j|m$. Da algoritme 2 bestemmer lineariserede polynomier $q(x)$ og $r(x)$ på en entydig måde, har det ingen betydning for det endelige resultat hvorvidt legemet i disse tilfælde betragtes som $\mathbb{F}_{q^m}$ eller $\mathbb{F}_{(q^j)^{\frac{m}{j}}}$.

Eksempel 5.8. Lad $L_1(x)$ og $L_2(x)$ være lineariserede polynomier over $\mathbb{F}_{q^m}$ med $q = 2$ givet ved

$$\begin{aligned} L_1(x) &= x^{q^0} + x^{q^1} + x^{q^3} \ , \\ L_2(x) &= x^{q^0} + x^{q^1} \ . \end{aligned}$$

Vi ønsker at dividere $L_1(x)$ med $L_2(x)$ og anvender algoritme 2. Det ses at $\deg(L_1(x)) = 3$ og $\deg(L_2(x)) = 1$, så i første omgang springer algoritmen direkte til **else** i **if**-løkken. Algoritmen giver

$$\begin{aligned} d := 3; \quad e := 1; \qquad a_d := 1; \quad b_e := 1; \\ t(x) &= \frac{1}{1}^{q^{m-1}} x^{q^2} = x^{q^2} \ . \end{aligned}$$

Da det er en rekursiv algoritme gennemløbes denne igen, med

$$\begin{aligned} L_1'(x) &:= L_1(x) - L_2(t(x)) = x^{q^0} + x^{q^1} + x^{q^3} - (x^{q^2} + x^{q^3}) = x^{q^0} + x^{q^1} - x^{q^2} \ , \\ L_2'(x) &:= L_2(x) = x^{q^0} + x^{q^1} \ . \end{aligned}$$

Her er $\deg(L_1'(x)) = 2 \geq \deg(L_2'(x)) = 1$, så igen springes direkte til konstruktion af $t'(x)$. Algoritmen giver

$$\begin{aligned} d := 2; \quad e := 1; \qquad a_d := -1; \quad b_e := 1; \\ t'(x) &= \frac{-1}{1}^{q^{m-1}} x^{q^1} = x^{q^1} \ , \end{aligned}$$

hvorefter de to polynomier igen redefineres;

$$\begin{aligned} L_1''(x) &= L_1'(x) - L_2'(t'(x)) = x^{q^0} + x^{q^1} - x^{q^2} - \left(x^{q^1} + x^{q^2}\right) = x^{q^0} \ , \\ L_2''(x) &= L_2'(x) = x^{q^0} + x^{q^1} \ . \end{aligned}$$

Endnu en gang gennemløbes algoritme 2, men denne gang er $\deg(L_1''(x)) = 0 < \deg(L_2''(x)) = 1$, hvorfor resten bestemmes;

$$r''(x) = L_1''(x) = x^{q^0} \ .$$

Output af dette gennemløb er derfor $q''(x) = 0$ og $r''(x) = x^{q^0}$. Output af anden gennemløb af algoritmen giver så

$$q'(x) = q''(x) + t'(x) = 0 + x^{q^1} = x^{q^1} \quad \text{og} \quad r'(x) = r''(x) = x^{q^0} \ .$$

Første gennemløb af algoritmen bestemmer heraf de endelige værdier for q og r til at være

$$q(x) = q'(x) + t(x) = x^{q^1} + x^{q^2}; \qquad r(x) = r'(x) = x^{q^0} \ .$$

Vi har derfor at

$$L_1(x) = L_2(q(x)) + r(x) \ .$$

For kontrol ses let at

$$\begin{aligned} x^{q^0} + x^{q^1} + x^{q^3} &= \left(x^{q^1} + x^{q^2}\right)^{q^0} + \left(x^{q^1} + x^{q^2}\right)^{q^1} + x^{q^0} \\ &= x^{q^1} + x^{q^2} + x^{q^2} + x^{q^3} + x^{q^0} = x^{q^0} + x^{q^1} + x^{q^3} \ . \end{aligned}$$

▲

5.2 Konstruktion af Bivariat Lineariseret Polynomium

I dette afsnit præsenteres en algoritme fra [KK08], som kan konstruere et bivariat lineariseret polynomium $Q(x, y)$.

Definition 5.9 (Bivariat lineariseret polynomium)**.** Et bivariat lineariseret polynomium er et polynomium $Q(x, y)$ på formen

$$Q(x, y) = Q_x(x) + Q_y(y) \ , \tag{5.6}$$

hvor $Q_x(x)$ og $Q_y(y)$ er lineariserede polynomier over $\mathbb{F}_{q^m}$. Et bivariat lineariseret polynomium med et enkelt led og med ledende koefficient 1 kaldes et bivariat lineariseret monomium.

5.2. KONSTRUKTION AF BIVARIAT LINEARISERET POLYNOMIUM

Et bivariat lineariseret monomium kan antage formen x^{q^i} eller y^{q^j} for $i, j \in \mathbb{Z}_{\geq 0}$.

Til at konstruere $Q(x, y)$ benyttes den $(1, k-1)$-vægtet grad af et bivariat lineariseret polynomium, som er defineret ved følgende.

Definition 5.10 ($(1, k-1)$-vægtet grad.)**.** Lad $h(x, y) = h_x(x) + h_y(y)$ være et bivariat lineariseret polynomium, hvor $h_x(x)$ og $h_y(y)$ er lineariserede polynomier med grad henholdsvis $q^{d_x(h)}$ og $q^{d_y(h)}$. Den $(1, k-1)$-vægtet grad af $h(x, y)$ er defineret ved

$$\deg_{1,k-1}(h(x, y)) := \max\{d_x(h), k - 1 + d_y(h)\} .$$

I tilfælde hvor $h_x(x) = 0$ eller $h_y(y) = 0$ defineres graden af $h_x(x)$ og $h_y(y)$ til henholdsvis $q^{d_x(h)} = -\infty$ eller $q^{d_y(y)} = -\infty$. [KK08]

Lad en lineært uafhængig mængde $B = \{(x_1, y_1), \ldots, (x_r, y_r)\}$ over $\mathbb{F}_q$ være givet, hvor $(x_i, y_i) \in \mathbb{F}_{q^m}^2$ for $i \in \{1, \ldots, r\}$. Algoritme 3 på side 57 tager B som input og giver $Q(x, y)$ som output. Dette polynomium er konstrueret således at $Q(x_i, y_i) = 0$ for alle $(x_i, y_i) \in \text{span}\{B\}$. Følgende redegøres for baggrunden for algoritmens opbygning.

Idéen er at der sideløbende konstrueres to forskellige bivariate lineariserede polynomier, $h_0(x, y)$ og $h_1(x, y)$, som begge to opfylder, at

$$h_0(x_i, y_i) = 0 = h_1(x_i, y_i) , \tag{5.7}$$

for alle $(x_i, y_i) \in \text{span}\{B\}$. Da vi senere ønsker at anvende $Q(x, y)$ til dekodning stilles der krav om, at graden af $Q(x, y)$ er begrænset opadtil, hvorfor der løbende tilstræbes at holde graden af $h_0(x, y)$ og $h_1(x, y)$ så lille som mulig i algoritmen. Som udgangspunkt defineres $h_0(x, y) = x$ og $h_1(x, y) = y$. Dette sikrer at polynomierne allerede antager en lineariseret form ved algoritmens begyndelse, og at de samtidig har minimal grad. For hver vektor $(x_i, y_i) \in B$ redefineres $h_0(x, y)$ og $h_1(x, y)$, således at de opfylder (5.7) for denne vektor.

Lad (x_i, y_i) være en given vektor i B. Værdierne af $h_0(x_i, y_i)$ og $h_1(x_i, y_i)$ bestemmes og defineres ved henholdsvis Δ_0 og Δ_1. Dette giver information om hvorvidt polynomierne allerede opfylder (5.7). Såfremt $\Delta_0 = 0$ behøves $h_0(x, y)$ ikke at redefineres for denne vektor, og ligeledes gælder for $h_1(x, y)$ hvis $\Delta_1 = 0$. Begyndelsesdefinitionen af $h_0(x, y)$ og $h_1(x, y)$, samt det faktum at nulvektoren ikke kan være en vektor i B, da B består af lineære uafhængige vektorer over $\mathbb{F}_q$, medfører at vi aldrig har tilfældet at både $\Delta_0 = 0$ og $\Delta_1 = 0$. Antag at $\Delta_0 = 0$. Vi har da kun brug for at redefinere $h_1(x, y)$. Denne defineres til

$$h_1(x, y) := (h_1(x, y))^q - (\Delta_1)^{q-1} h_1(x, y) . \tag{5.8}$$

Ved indsættelse af (x_i, y_i) i (5.8) ses at $h_1(x_i, y_i) = 0$. Tilsvarende redefinering af $h_0(x, y)$ benyttes ved $\Delta_1 = 0$.

Hvis både Δ_0 og Δ_1 er forskellige fra nul er det nødvendigt at redefinere begge polynomier på en sådan måde at de stadig har så lille en grad som muligt, men samtidig er forskellige. Den $(1, k-1)$-vægtede grad af $h_0(x, y)$ og $h_1(x, y)$ sammenlignes. Hvis $\deg_{1,k-1}(h_0) \leq \deg_{1,k-1}(h_1)$ har $h_1(x, y)$ den højeste $(1, k-1)$-vægtet grad, så dennes grad ændres ikke, mens graden af $h_0(x, y)$ stiger;

$$h_1(x, y) := \Delta_1 h_0(x, y) - \Delta_0 h_1(x, y) \,, \tag{5.9}$$

$$h_0(x, y) := (h_0(x, y))^q - (\Delta_0)^{q-1} h_0(x, y) \,. \tag{5.10}$$

Ved indsættelse af (x_i, y_i) i $h_0(x, y)$ og $h_1(x, y)$ fås at (5.7) er opfyldt for redefineringen af $h_0(x, y)$ og $h_1(x, y)$. Såfremt $\deg_{1,k-1}(h_0) > \deg_{1,k-1}(h_1)$ redefineres $h_0(x, y)$ og $h_1(x, y)$ på tilsvarende måde ved at erstatte h_1 med h_0 og h_0 med h_1 i (5.9) og (5.10).

Bemærk at måden hvorpå $h_0(x, y)$ og $h_1(x, y)$ redefineres medfører, at de forbliver bivariate polynomier med den egenskab, at de ikke indeholder monomier af formen $x^{m_1} y^{m_2}$ for $m_1, m_2 \geq 1$.

Når $h_0(x, y)$ og $h_1(x, y)$ opfylder (5.7) for alle $i \in \{1, \ldots, r\}$ undersøges afsluttende hvilket polynomium der har den mindste $(1, k-1)$-vægtet grad. Dette polynomium bliver output af algoritmen og et bivariat lineariseret polynomium $Q(x, y)$ er konstrueret.

I sætning 5.15, som følger på side 58, vises, at algoritme 3 konstruerer $Q(x, y)$ som ønsket. Dog definerer vi først en orden på de bivariate lineariserede polynomier ud fra den $(1, k-1)$-vægtet grad.

Definition 5.11 (Orden på bivariate lineariserede polynomier.)**.** Lad $f(x, y)$ og $g(x, y)$ være bivariate lineariserede polynomier. Hvis

$$\deg_{1,k-1}(f) < \deg_{1,k-1}(g) \,,$$

så siges $f(x, y) \prec g(x, y)$. I tilfælde hvor $\deg_{1,k-1}(f) = \deg_{1,k-1}(g)$ gælder at $f(x, y) \prec g(x, y)$ hvis $d_y(f) + k - 1 < \deg_{1,k-1}(f)$ og $d_y(g) + k - 1 = \deg_{1,k-1}(g)$. Hvis ingen af disse tilfælde er gældende så siges $f(x, y)$ og $g(x, y)$ at være ikke-sammenlignelige. [KK08]

Ovenstående definition giver at i de tilfældet, hvor den $(1, k-1)$-vægtede grad af to bivariate lineariserede polynomier er ens, så er det kun muligt at ordne polynomierne, hvis det ene polynomium $f(x, y)$ opfylder at $d_x(f) > k - 1 + d_y(f)$ og det andet polynomium $g(x, y)$ opfylder at $k - 1 + d_y(g) \geq d_x(g)$.

Algoritme 3 Konstruktion af et bivariat lineariseret polynomium; **biv**(B).

Input: En linear uafhængig mængde $B = \{(x_1, y_1), \ldots, (x_r, y_r)\} \in W$.
Lad $h_0(x, y) = x$; $h_1(x, y) = y$;
for $i = 1, \ldots, r$ **do**
  $\Delta_0 := h_0(x_i, y_i)$; $\Delta_1 := h_1(x_i, y_i)$;
  if $\Delta_0 = 0$ **then**
    $h_1(x, y) := (h_1(x, y))^q - (\Delta_1)^{q-1} h_1(x, y)$;
  else if $\Delta_1 = 0$ **then**
    $h_0(x, y) := (h_0(x, y))^q - (\Delta_0)^{q-1} h_0(x, y)$;
  else
    if $\deg_{1,k-1}(h_0) \leq \deg_{1,k-1}(h_1)$ **then**
      $h_1(x, y) := \Delta_1 h_0(x, y) - \Delta_0 h_1(x, y)$;
      $h_0(x, y) := (h_0(x, y))^q - (\Delta_0)^{q-1} h_0(x, y)$;
    else
      $h_0(x, y) := \Delta_1 h_0(x, y) - \Delta_0 h_1(x, y)$;
      $h_1(x, y) := (h_1(x, y))^q - (\Delta_1)^{q-1} h_1(x, y)$;
    end if
  end if
end for
if $\deg_{1,k-1}(h_1) < \deg_{1,k-1}(h_0)$ **then**
  $Q(x, y) := h_1(x, y)$;
else
  $Q(x, y) := h_0(x, y)$;
end if
Output: Et bivariat lineariseret polynomium $Q(x, y) = Q_x(x) + Q_y(y)$.

Proposition 5.12. *Ordnen $\prec$ på bivariate lineariserede polynomier inducere en total ordning på bivariate lineariserede monomier.*

Bevis. Det er nødvendigt at betragte tre tilfælde;

i. $f(x, y) = x^{q^i}$ og $g(x, y) = x^{q^j}$,

ii. $f(x, y) = x^{q^i}$ og $g(x, y) = y^{q^j}$ og

iii. $f(x, y) = y^{q^i}$ og $g(x, y) = y^{q^j}$.

Lad tilfælde *i.* være givet, så gælder at $\deg_{1,k-1}(f) = i$ og $\deg_{1,k-1}(g) = j$. Hvis $i < j$ eller $i > j$ så giver definition 5.11 henholdsvis at $x^{q^i} \prec x^{q^j}$ og $x^{q^j} \prec x^{q^i}$. I tilfælde hvor $i = j$ er $f(x, y)$ og $g(x, y)$ identiske og der er ikke noget at vise.

Lad tilfælde *ii.* være givet, så haves at $\deg_{1,k-1}(f) = i$ og $\deg_{1,k-1}(g) = k-1+j$. Tilfælde hvor $i \leq j$ giver at $x^{q^i} \prec y^{q^j}$. Hvis $i > j$ definer da $h = i-j$. Så følger at $y^{q^j} \prec x^{q^i}$ hvis $k-1 < h$ og at $x^{q^i} \prec y^{q^j}$ hvis $k-1 \geq h$.

Hvis tilfælde *iii.* er givet så er $\deg_{1,k-1}(f) = k-1+i$ og $\deg_{1,k-1}(g) = k-1+j$. Hvis $i < j$ eller $i > j$ så haves henholdsvis at $y^{q^i} \prec y^{q^j}$ eller $y^{q^j} \prec y^{q^i}$. Hvis $i = j$ er $f(x,y)$ og $g(x,y)$ identiske.

I alle de tre ovenstående tilfælde opnås en total ordning på de bivariate lineariserede monomier. □

Hvis der konstrueres et polynomium $h(x,y) = f(x,y) + g(x,y)$ fra de tre tilfælde i ovenstående bevis, så er det i alle tre tilfælde muligt at definere det ledende monomium i $h(x,y)$. Derfor gør proposition 5.12 det muligt, at definere det ledende monomium af et bivariate lineariseret polynomium under ordenen $\prec$ som monomiet af maksimal $(1, k-1)$-vægtet grad.

Lemma 5.13. *Antag at $f(x,y)$ og $g(x,y)$ er to ikke-sammenlignelige bivariate lineariserede polynomier under $\prec$. For et passende valgt γ kan da konstrueres en linear kombination $h(x,y) = f(x,y) + \gamma g(x,y)$ hvorom det gælder at $h(x,y) \prec f(x,y)$ og $h(x,y) \prec g(x,y)$. [KK08, lemma 15]*

Bevis. I de tilfælde hvor $f(x,y)$ og $g(x,y)$ ikke er sammenlignelige må deres ledende monomium være ens, $\mathrm{LM}(f) = \mathrm{LM}(g)$. Ved at vælg $\gamma = \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)}$ fås at det ledende monomium i $h(x,y) = f(x,y) - \gamma g(x,y)$ har mindre grad end $\mathrm{LM}(f)$ og $\mathrm{LM}(g)$ under ordningen $\prec$. Heraf er $h(x,y) \prec f(x,y)$ og $h(x,y) \prec g(x,y)$. □

Definition 5.14 (x- og y-minimal.)**.** Lad A være en mængde af r lineært uafhængige elementer $(x_1, y_1), \ldots, (x_r, y_r) \in W$. Et ikke-nulpolynomium $f(x,y)$ er x-minimal med hensyn til A, hvis $f(x,y)$ er et minimal polynomium under $\prec$, således at $\mathrm{LM}(f) = x^{q^{d_x(f)}}$ og $f(x,y)$ evaluerer til nul i alle punkter i A. Desuden er $f(x,y)$ y-minimal med hensyn til A, hvis $f(x,y)$ er et minimal polynomium under $\prec$, således at $\mathrm{LM}(f) = y^{q^{d_y(f)}}$ og $f(x,y)$ evaluerer til nul i alle punkter i A. [KK08]

Sætning 5.15. *Polynomierne $h_0(x,y)$ og $h_1(x,y)$ som er output af algoritme 3, med en lineær uafhængig mængde over $\mathbb{F}_q$; $B = \{(x_1, y_1), \ldots, (x_r, y_r)\}$ som input, er henholdsvis x-minimal og y-minimal med hensyn til mængden B. [KK08, Sætning 16]*

Bevis. Vi skal vise at for ethvert skridt i algoritme 3 er polynomierne $h_0(x,y)$ og $h_1(x,y)$ henholdsvis x-minimal og y-minimal med hensyn til den mængde B de er konstrueret over. Dette gøres ved induktion.

Basisskridt: Ved algoritmens begyndelse defineres de lineariserede polynomier $h_0(x,y) = x$ og $h_1(x,y) = y$. Disse bør være x-minimale og y-minimale med hensyn til den tomme mængde. Monomiet $x^{q^{d_x(h_0)}} = x^{q^0}$ er det ledende monomium af $h_0(x,y)$ da denne kun består af et monomium. Den tomme mængde indeholder ikke nogen punkter så $h_0(x,y)$ evaluerer til nul i alle punkter i den tomme mængde. Heraf er $h_0(x,y)$ x-minimal under den tomme mængde. Tilsvarende situation for $h_1(x,y)$ medfører, at $h_1(x,y)$ er y-minimal under den tomme mængde.

Induktionsantagelse: Antag at $h_0(x,y)$ og $h_1(x,y)$ er henholdsvis x-minimal og y-minimal med hensyn til mængden $\{(x_1,y_1),\ldots,(x_j,y_j)\}$ efter j gennemløb af **for**-løkken i algoritme 3, hvor $j < r$.

Induktionsskridt: For det $j+1$'te gennemløb antages først at $\Delta_0 \neq 0$ og $\Delta_1 \neq 0$ samt at $h_1(x,y) \prec h_0(x,y)$. Da defines

$$h_0'(x,y) := \Delta_1 h_0(x,y) - \Delta_0 h_1(x,y) \ .$$

Da $\Delta_0 = h_0(x_{j+1},y_{j+1})$ og $\Delta_1 = h_1(x_{j+1},y_{j+1})$ ses det at $h_0'(x,y)$ giver nul i punktet (x_{j+1},y_{j+1}). Desuden per antagelse evaluerer $h_0(x,y)$ og $h_1(x,y)$ til nul i punkterne $\{(x_1,y_1),\ldots,(x_j,y_j)\}$ så $h_0'(x,y)$ evaluerer derfor til nul i punkterne $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$. Det ledende monomium er $\mathrm{LM}(h_0'(x,y)) = \mathrm{LM}(h_0(x,y))$ så $h_0'(x,y)$ er x-minimal da $h_0(x,y)$ er x-minimal. Polynomiet $h_1(x,y)$ redefineres til

$$h_1'(x,y) := (h_1(x,y))^q - \Delta_1^{q-1} h_1(x,y) \ . \tag{5.11}$$

Antag at $h_1'(x,y)$ ikke er y-minimal med hensyn til $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$. Så findes et andet polynomium $p(x,y) \neq h_1(x,y)$ der er y-minimal med hensyn til punkterne $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$ og hvis ledende monomium har mindre grad end graden af $\mathrm{LM}(h_1')$. Da forskellen i grad mellem $h_1'(x,y)$ og $h_1(x,y)$ er q, og da $h_1(x,y)$ per antagelsen er y-minimal med hensyn til $\{(x_1,y_1),\ldots,(x_j,y_j)\}$, følger at $p(x,y)$ har samme ledende monomium som $h_1(x,y)$. Fra lemma 5.13 følger så at der findes et polynomium $h(x,y)$ der er en linear kombination af $p(x,y)$ og $h_1(x,y)$, som har ledende monomium under $\prec$ mindre end $\mathrm{LM}(p) = \mathrm{LM}(h_1)$. Dette er en modstrid med minimaliteten af $h_0(x,y)$ og $h_1(x,y)$. Heraf må $h_1'(x,y)$ være y-minimal med hensyn til $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$.

Hvis $h_0(x,y) \prec h_1(x,y)$, $\Delta_0 \neq 0$ og $\Delta_1 \neq 0$ så følger på tilsvarendevis at $h_0(x,y)$ og $h_1(x,y)$ er henholdsvis x-minimal og y-minimal efter det $j+1$'te gennemløb af **for**-løkken.

Det antages følgende at $\Delta_0 = 0$ og $\Delta_1 \neq 0$. Da ændres $h_0(x,y)$ ikke og heraf er denne x-minimal per antagelse. Polynomiet $h_1(x,y)$ redefineres på

samme vis som i (5.11). Antag at $h_1'(x,y)$ ikke er y-minimal med hensyn til $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$. Ved samme argumentation som ovenfor så findes et andet polynomium $p(x,y) \neq h_1(x,y)$, hvorom det gælder at $\mathrm{LM}(p) = \mathrm{LM}(h_1)$, som er y-minimal med hensyn til $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$. Fra lemma 5.13 konstrueres et polynomium $h(x,y) = p(x,y) + \gamma h_1(x,y)$, hvor $\gamma \in \mathbb{F}_{q^m}$, med egenskaben at $h(x,y) \prec p(x,y)$ og $h(x,y) \prec h_1(x,y)$. Der gælder om $h(x,y)$ at:

i. Hvis $\mathrm{LM}(h) = y^{q^{d_y(h)}}$ så $h(x,y)$ y-minimal da $h(x,y)$ evaluerer til nul på $\{(x_1,y_1),\ldots,(x_j,y_j)\}$. Dette er en modtrid med antagelsen om at $h_1(x,y)$ er y-minimal på $\{(x_1,y_1),\ldots,(x_j,y_j)\}$.

ii. Hvis $h(x,y) \prec h_0(x,y)$ så haves en modstrid med antagelsen at $h_0(x,y)$ er x-minimal.

Det antages at *i.* og *ii.* ikke er tilfældet. Så er $\mathrm{LM}(h) = x^{q^{d_x(h)}}$ hvor $d_x(h) > d_x(h_0)$. Konstruktionen af $h(x,y)$ giver, at $h(x,y)$ ikke evaluerer til nul i (x_{j+1},y_{j+1}) og heraf er $h(x,y)$ ikke en sammensætning af $h_0(x,y)$ og et andet polynomium. For et passende valgt t kan vi så konstruere et polynomium $h''(x,y)$, som en linear kombination af $h(x,y)$ og $(h_0(x,y))^{q^t}$, hvorom der gælder, at $h''(x,y) \prec h(x,y)$. Polynomiet $h''(x,y)$ har samme muligheder i forhold til $h_1(x,y)$ og $h_0(x,y)$, som $h(x,y)$ havde og ovenstående konstruktion kan gentages. Fortsættende på denne måde vil vi på et tidspunkt opnå et polynomium $\tilde{h}(x,y)$ med den egenskab, at enten er $\mathrm{LM}(\tilde{h}) = y^{q^{d_y(\tilde{h})}}$ eller $\tilde{h}(x,y) \prec h_0(x,y)$, hvorved en modstrid med y-minimaliteten af $h_1(x,y)$ er opnået, eller en modstrid med x-minimaliteten af $h_0(x,y)$ er opnået. Heraf må $h_1'(x,y)$ være y-minimal med hensyn til $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$.

I tilfældet hvor $\Delta_0 \neq 0$ og $\Delta_1 = 0$ følger på samme vis som ovenfor at $h_0(x,y)$ og $h_1(x,y)$ er x-minimal og y-minimal med hensyn til mængden $\{(x_1,y_1),\ldots,(x_{j+1},y_{j+1})\}$. □

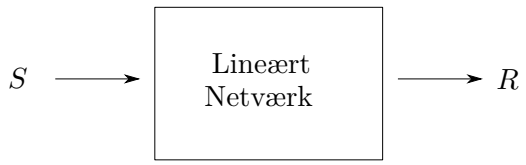
Bemærkning 5.16. Kompleksiteten af algoritme 3 er domineret af konstruktionen af $h_0(x,y)$ og $h_1(x,y)$. **For**-løkken hvori disse frembringes gennemløbes r gange. Vi definerer senere at $r = \dim(U)$, hvor $U \subseteq W$ som har dimension $\ell + m$, hvorfor $r \leq \ell + m$. For hvert gennemløb af **for**-løkken er det redefineringen af $h_i(x,y) := (h_i(x,y))^q - \Delta_i^{q-1} h_i(x,y)$ for $i \in \{0,1\}$ som er den mest krævende. Før første gennemløb af **for**-løkken er antallet af led i $h_i(x,y)$ per definition en. Ved hver redefinering øges antallet af led højest med en så i det værst tilfælde opnås at $h_i(x,y)$ har $\ell + m$ led ved sidste redefinering. Det er den situation, at koefficienterne i hvert led bliver opløftet i q, som er dominerende, og dette sker maksimalt én gang for hvert led i $h_i(x,y)$ ved hver redefinering. Heraf er kompleksiteten af algoritme 3 $O((\ell+m)^2)$.

Kapitel 6

Det Fejlkorrigerende Netværkskodningsproblem

I dette kapitel rettes fokus mod problemstillingen at kunne rette de fejl, der eventuelt måtte opstå, når information transmitteres via et netværk, hvor der undervejs udføres vilkårlig netværkskodning. Vi betragter her det givne netværk som en "sort boks", dvs. vi har ingen kendskab til netværkets topologi. Herved har vi heller ikke nogen viden om den kodning, som finder sted når informationen passerer enheder og kanaler i netværket. Netværket kan derfor ses som bestående af kun en kanal (senere betegnet operatorkanal), der kan give anledning til ændringer i den transmitterede information. Opstilling af det fejlkorrigerende netværkskodningsproblem er baseret på single unicast tilfældet. Figur 6.1 illustrerer dette. Her ses at kilden S transmittere information ind i netværket, mens enheden R modtager information fra netværket.

I multicast netværkskodningsproblemet, som blev præsenteret i kapitel 3, bestod den transmitterede information af lineært uafhængige vektorer over $\mathbb{F}_q$, og det var her muligt at dekode, hvis mængden af vektorer stadig var lineært uafhængige ved modtagerenheden. For at indføre fejlkorrigering



Figur 6.1: Betragning af netværk anvendt til fejlkorrigering.

betrages den afsendte information som et kodeord. Et kodeord er et underrum af et vektorrum og en kode består af en mængde af underrum. Lad W være et N-dimensionalt vektorrum over $\mathbb{F}_q$ og lad $\mathcal{P}(W)$ betegne mængden af alle underrum af W, mens $\mathcal{P}(W, \ell)$ betegner mængden af alle underrum af W med dimension $\ell \leq N$. En kode $\mathcal{C}$ er da defineret ved

$$\mathcal{C} = \{V_1, \ldots, V_{|\mathcal{C}|}\} \in \mathcal{P}(W) \ . \tag{6.1}$$

Denne kode har størrelsen $|\mathcal{C}|$ og dens minimumsafstand er givet ved

$$D(\mathcal{C}) = \min_{\substack{V_i, V_j \in \mathcal{C} \\ V_i \neq V_j}} d(V_i, V_j) \ ,$$

hvor d er en afstandsfunktion defineret i afsnit 6.0.1. Den maksimale dimension af koden betegnes

$$\ell(\mathcal{C}) = \max_{V \in \mathcal{C}} \dim(V) \ .$$

Hvis alle kodeord i $\mathcal{C}$ har samme dimension, så siges $\mathcal{C}$ at være en konstantdimensionskode.

En kode $\mathcal{C}$ bestående af underrum af et N-dimensionalt rum over $\mathbb{F}_q$ med de ovenfor angivet parametre siges at være af typen $[N, \ell(\mathcal{C}), \log_q |\mathcal{C}|, D(\mathcal{C})]$.

Idéen bag fejlkorrigeringen af koden $\mathcal{C}$ ligger i, at når et kodeord har gennemløbet kanalen, skal det være muligt at bestemme det transmitterede kodeord ved at sammenligne det modtaget underrum med kodeordene i $\mathcal{C}$. Vi har derfor brug for en metode til at bestemme forskellen mellem kodeordene. Dette defineres i det følgende.

6.0.1 En Metrik på Mængden af Underrum

Vi definerer en funktion d, som giver et udtryk for forskellen mellem to underrum baseret på deres dimension.

Definition 6.1. Lad $d : \mathcal{P}(W) \times \mathcal{P}(W) \to \mathbb{Z}_+$ være defineret ved

$$d(A, B) := \dim(A + B) - \dim(A \cap B) \ . \tag{6.2}$$

[KK08]

Bemærkning 6.2. Der gælder om dimensionen af en sum at

$$\dim(A + B) = \dim(A) + \dim(B) - \dim(A \cap B) \ , \tag{6.3}$$

hvorfor funktionen d kan omskrives til

$$\begin{aligned} d(A, B) &= \dim(A) + \dim(B) - 2\dim(A \cap B) && (6.4) \\ &= 2\dim(A + B) - \dim(A) - \dim(B) \ . && (6.5) \end{aligned}$$

Specielt gælder at d er en metrik på $\mathcal{P}(W)$, hvorfor d kan betragtes som en afstandsfunktion.

Proposition 6.3. *Funktionen givet i* (6.2) *er en metrik på rummet* $\mathcal{P}(W)$. *[KK08, Lemma 1]*

Bevis. Vi skal vise at for alle underrum $A, B, C \in \mathcal{P}(W)$ er definitionen for en metrik opfyldt. Dette gøres følgende i punkt *i.-iii.*

i. Positiv definit: Antag at $A = B$, så gælder fra (6.2) at

$$d(A,B) = \dim(A+B) - \dim(A \cap B) = \dim(A) - \dim(A) = 0\,.$$

Antag at $A \neq B \neq \{\mathbf{0}\}$ så haves fra (6.4) at

$$\begin{aligned} d(A,B) &= \dim(A) + \dim(B) - 2\dim(A \cap B) \\ &= \dim(A) - \dim(A \cap B) + \dim(B) - \dim(A \cap B) > 0\,. \end{aligned}$$

Den sidste ulighed i det ovenstående følger af at hvis $A \subset B$ så fås $\dim(A) - \dim(A \cap B) = 0$, men $\dim(B) - \dim(A \cap B) > 0$. Tilsvarende gælder for $B \subset A$. Hvis $A \neq A \cap B \neq B$ så gælder der, at $\dim(A) - \dim(A \cap B) > 0$ og $\dim(B) - \dim(A \cap B) > 0$.

ii. Symmetri: Der gælder at $A + B = B + A$ og $A \cap B = B \cap A$ hvorfor

$$d(A,B) = \dim(A+B) - \dim(A \cap B) = \dim(B+A) - \dim(B \cap A) = d(B,A)\,.$$

iii. Trekantsuligheden: Ligningen $d(A,B) - d(A,X) - d(X,B)$ kan omskrives til

$$\begin{aligned} & \dim(A) + \dim(B) - 2\dim(A \cap B) - \dim(A) - \dim(X) \\ & +2\dim(A \cap X) - \dim(X) - \dim(B) + 2\dim(X \cap B) \\ = \;& 2\dim(A \cap X) + 2\dim(X \cap B) - 2\dim(A \cap B) - 2\dim(X) \\ = \;& 2\left(\dim(A \cap X + X \cap B) + \dim(A \cap X \cap B) - \dim(A \cap B) - \dim(X)\right) \\ = \;& 2\left(\underbrace{\dim(A \cap X + X \cap B) - \dim(X)}_{\leq 0} + \underbrace{\dim(A \cap X \cap B) - \dim(A \cap B)}_{\leq 0}\right) \\ \leq \;& 0\,. \end{aligned}$$

Uligheden i det ovenstående følger af at $(A \cap X + X \cap B) \subset X$ og $A \cap X \cap B \subset A \cap B$. Derfor gælder at $d(A,B) \leq d(A,X) + d(X,B)$.

□

Hermed er fundamentet lagt for at kunne dekode et modtaget underrum til det kodeord som er nærmest, hvor afstanden mellem underrummet og kodeordene i $\mathcal{C}$ er fastlagt vha. funktionen d.

6.1 Sletninger og Fejl Forårsaget af Netværket

Vi lader i det følgende $V \in \mathcal{P}(W)$ betegne et afsendt kodeord, mens U betegner det modtaget ord. Når et kodeord sendes over en kanal kan der ske utilsigtede ændringer undervejs. Der er to primære årsager til dette;

- Noget af den afsendte information forsvinder. Dette betrages som sletninger, hvorfor denne ændringen kan forårsage fald i dimension mellem det afsendte kodeord V og den modtaget information udtrykt ved U.
- Noget af den afsendte information omformes. Dette betragtes som fejl i transmissionen, og kan medføre enten øget eller formindsket dimension af U i forhold til dimensionen af V.

Vi har brug for at kunne udtrykke begge tilfælde matematisk. Vi definerer derfor en stokastisk operator $\mathcal{H}_k$ som opererer på et underrum af W. Denne kaldes en sletningsoperator. Lad $V \in \mathcal{P}(W)$. Hvis $\dim(V) > k$ så returnerer $\mathcal{H}_k(V)$ et tilfældigt frembragt k-dimensionalt underrum af V. Ellers, hvis $\dim(V) \leq k$ så returneres V, hvilket er et udtryk for at der ingen sletninger finder sted under transmissionen.

Til at udtrykke fejl i transmissionen vælges et underrum E af W kaldet fejlrummet. I de tilfælde hvor $E \subset V$ sker der ingen fejl i transmissionen. En mulighed er også at $E \cap V \neq \{\mathbf{0}\}$ og at der yderligere findes noget i E som ikke ligger i V. Herved kan E tilføre fejl til kodeordet eller måske eliminere nogle sletninger frembragt af $\mathcal{H}_k(V)$. Bemærk at givet et underrum V kan der fra et fejlrum E altid konstrueres et nyt fejlrum E', som har den egenskab at $V \cap E' = \{0\}$. Der gælder så at $E = (E \cap V) \oplus E'$, hvorfor

$$\begin{aligned} U &= \mathcal{H}_k(V) + E \;=\; \mathcal{H}_k(V) + (E \cap V) \oplus E' \\ &= \{\mathbf{v}_1 | \mathbf{v}_1 \in \mathcal{H}_k(V)\} + \{\mathbf{v}_2 + \mathbf{v}_3 | \mathbf{v}_2 \in (E \cap V), \mathbf{v}_3 \in E'\} \\ &= \{\mathbf{v}_1 | \mathbf{v}_1 \in \mathcal{H}_k(V)\} + \{\mathbf{v}_2 | \mathbf{v}_2 \in (E \cap V)\} + \{\mathbf{v}_3 | \mathbf{v}_3 \in E'\} \\ &= \{\mathbf{v}_1 + \mathbf{v}_2 | \mathbf{v}_1 \in \mathcal{H}_k(V), \mathbf{v}_2 \in (E \cap V)\} + \{\mathbf{v}_3 | \mathbf{v}_3 \in E'\} \qquad (6.6) \\ &= \mathcal{H}_{k'}(V) \oplus E', \text{ hvor } k' \geq k \; . \end{aligned}$$

Da $(\mathcal{H}_k(V) \cup (E \cap V)) \cap E' = \{\mathbf{0}\}$ kan summen i (6.6) betragtes som en direkte sum. Vi får heraf at vi altid kan vælge et $k' \leq k$ og et fejlrum E', således at der findes en sletningsoperator $\mathcal{H}_{k'}(V)$ og et fejlrum E', så det modtaget ord U er givet ved $U = \mathcal{H}_{k'}(V) \oplus E'$. I det følgende betegnes k' altid ved k og E' altid ved E.

Definition 6.4. En operatorkanal med et tilhørende rum W er en kanal med input og output alfabet $\mathcal{P}(W)$. Forholdet mellem input $V \in \mathcal{P}(W)$ og output U er givet ved

$$U = \mathcal{H}_k(V) \oplus E \,, \tag{6.7}$$

hvor $k = \dim(U \cap V)$ og E er fejlrummet. Ved overførelsen af V til U siges operatorkanalen at overdrage $\rho = \dim(V) - k$ sletninger og $t = \dim(E)$ fejl. [KK08, Definition 1]

Bemærkning 6.5. Ud fra konstruktionen (6.7) fås et andet udtryk for sletningsoperatoren $\mathcal{H}_k(V)$. Dette er givet ved $\mathcal{H}_k(V) = U \cap V$. Dog er U først kendt efter gennemløb af operatorkanalen, og $\mathcal{H}_k(V)$ kan derfor ikke bestemmes direkte ved denne metode før både U og V er kendt.

6.1.1 Minimumsafstandsdekoder

Som nævnt tidligere er vi interesseret i at kunne dekode et modtaget underrum U til det afsendte kodeord $V \in \mathcal{C}$. Til dette anvendes en minimumsafstandsdekoder på output af operatorkanalen. Minimumsafstandsdekoderen har egenskaben at den tager output U fra operatorkanalen og returnerer det nærmeste kodeord $V \in \mathcal{C}$, som opfylder at for alle $V' \in \mathcal{C}$ gælder at $d(U, V) \leq d(U, V')$. Minimumsaftandsdekoderen er i stand til at dekode til det korrekt kodeord, hvis minimumsafstanden af koden er konstrueret passende i forhold til det antal fejl operatorkanalen tilfører under transmissionen. Afgrænsningen af kodens minimumsafstand er givet i følgende sætning.

Sætning 6.6. *Antag at koden $\mathcal{C}$ anvendes på operatorkanalen. Lad $V \in \mathcal{C}$ være transmitteret og lad $U = \mathcal{H}_k(V) \oplus E$ være modtaget, hvor $\dim(E) = t$. Lad $\rho = \max\{0, \ell(\mathcal{C}) - k\}$ betegne det maksimale antal af sletninger forårsaget af operatorkanalen. Hvis*

$$2(t + \rho) < D(\mathcal{C}) \,, \tag{6.8}$$

så vil minimumsafstandsdekoderen for koden $\mathcal{C}$ frembringe det afsendte rum V fra det modtaget rum U. [KK08, Sætning 2]

Bemærkning 6.7. Størrelsen $\ell(\mathcal{C})$ er den maksimale dimensionen af koden $\mathcal{C}$, mens k er dimensionen af det rum som sletningsoperatoren frembringer. Som tidligere nævnt gælder at hvis $k \geq \dim(V)$, hvor $V \in \mathcal{C}$, så tilføjer sletningsoperatoren ingen sletninger, hvorfor det maksimale antal sletninger forårsaget af operatorkanalen nødvendigvis må være nul. Heraf følger definitionen af ρ.

Bevis for sætning 6.6. Antag, at (6.8) er givet, og lad $V' = \mathcal{H}_k(V)$. Da ρ er det maksimale antal sletninger fås, at $d(V, V') \leq \rho$, og da $t = \dim(E)$ er $d(U, V') \leq t$. Heraf giver trekantsuligheden, at afstanden mellem U og V er nedre afgrænset ved

$$d(U, V) \leq d(U, V') + d(V', V) \leq t + \rho \,. \tag{6.9}$$

Lad $T \neq V$ være et andet kodeord i $\mathcal{C}$. Så er minimumsafstanden nedre afgrænset af

$$D(\mathcal{C}) \leq d(V, T) \leq d(V, U) + d(U, T) \,. \tag{6.10}$$

Ved omskrivning af (6.10) fås fra (6.9) og antagelsen, at

$$d(U, T) \geq D(\mathcal{C}) - d(V, U) > 2(t + \rho) - (t + \rho) = t + \rho \geq d(U, V) \,.$$

Heraf gælder, at minimumsafstandsdekoderen altid vil vælge at dekode til rummet V, da der ikke findes andre kodeord i $\mathcal{C}$ med samme eller mindre afstand til U. □

6.2 Konstruktion af en Fejlkorrigerende Kode; KK-Koden

I dette afsnit præsenteres en fejlkorrigerende kode som er konstrueret af Kötter og Kschischangs [KK08], heraf kaldet KK-koden. Vi indleder med en konstruktion af et rum W hørende til operatorkanalen, hvorefter vi konstruerer en fejlkorrigerende kode, som kan virke på operatorkanalen.

Lad $A = \{\alpha_1, \alpha_2, \ldots, \alpha_\ell\} \subset \mathbb{F}_{q^m}$ være en mængde af lineært uafhængige elementer over $\mathbb{F}_q$. Så udspænder disse elementer et ℓ-dimensionalt vektorrum $\text{span}\{A\} \subseteq \mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Fra dette defineres vektorrummet W over $\mathbb{F}_q$ ved den direkte sum,

$$W = \text{span}\{A\} \oplus \mathbb{F}_{q^m} = \{(\alpha, \beta) | \alpha \in \text{span}\{A\}, \beta \in \mathbb{F}_{q^m}\} \,,$$

som har dimensionen $\ell + m$.

Som angivet i ligning (6.1) består en kode $\mathcal{C}$ af en mængde underrum af W som betegnes kodeord. Et kodeord konstrueres på følgende måde;

1. For hvert kodeord som ønskes lad $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_{q^m}^k$ betegne en blok af beskedsymboler. Vektoren $\mathbf{u}$ kan betragtes som bestående af k symboler over $\mathbb{F}_{q^m}$ eller af mk symboler over $\mathbb{F}_q$.

2. For hver blok af beskedsymboler defineres et beskedpolynomium $f \in \mathscr{L}_{q^m}^k[x]$ ved

$$f(x) = \sum_{i=0}^{k-1} u_i x^{q^i} ,$$

   således at $f(x)$ er et lineariseret polynomium med koefficienter svarende til $\mathbf{u}$.

3. For hvert element i A defineres et par (α_i, β_i) hvor $\beta_i = f(\alpha_i)$ for $i \in \{1, \ldots, \ell\}$. Ethvert par (α_i, β_i) kan så betragtes som en vektor i W. Da elementerne i A danner en lineært uafhængig mængde, så er $\{(\alpha_1, \beta_1), \ldots, (\alpha_\ell, \beta_\ell)\}$ også en lineært uafhængig mængde som udspænder et ℓ dimensionelt underrum V af W. Dette underrum er et kodeord i $\mathcal{C}$.

Den afbildning som tager et beskedpolynomium $f \in \mathscr{L}_{q^m}^k[x]$ og afbilder det over i et lineært underrum $V \in \mathcal{P}(W, |A|)$ betegnes ved ev_A. Følgende lemma udtaler sig om, hvornår ev_A er injektiv.

Lemma 6.8. *Lad $A = \{\alpha_1, \alpha_2, \ldots, \alpha_\ell\} \subset \mathbb{F}_{q^m}$ være en mængde af lineært uafhængige elementer. Hvis $|A| \geq k$ så er afbildningen $\mathrm{ev}_\mathrm{A} : \mathscr{L}_{q^m}^k[x] \to \mathcal{P}(W, |A|)$ injektiv. [KK08, Lemma 12]*

Bevis. Antag at $|A| \geq k$. Vi ønsker at vise at ethvert element i $\mathscr{L}_{q^m}^k[x]$ afbildes entydigt over i et element i $\mathcal{P}(W, |A|)$. Lad $f, g \in \mathscr{L}_{q^m}^k[x]$ være givet således at $\mathrm{ev}_\mathrm{A}(f) = \mathrm{ev}_\mathrm{A}(g)$, og definer $h(x) = f(x) - g(x)$. Da gælder at $h(\alpha_i) = f(\alpha_i) - g(\alpha_i) = 0$ for alle $i \in \{1, \ldots, |A|\}$. Da $h(x)$ er et lineariseret polynomium følger, at $h(x) = 0$ for alle $x \in \mathrm{span}\{A\}$. Derfor har $h(x)$ mindst $q^{|A|}$ nulpunkter. Da $h(x)$ har grad højest q^{k-1} er dette kun muligt hvis $h(x) = 0$, hvorfor det følger at $f(x) = g(x)$. Heraf er ev_A injektiv. □

Bemærkning 6.9. Da $|A| = \ell$ per definition af A så vil tilfældet hvor $\ell \geq k$ give at afbildningen ev_A giver forskellige kodeord $V \in \mathcal{P}(W, \ell)$, når input er forskellige beskedpolynomier. Heraf kan værdimængden af afbildningen ev_A betragtes som en kode $\mathcal{C} \subset \mathcal{P}(W, \ell)$ med q^{mk} kodeord.

Lemma 6.10. *Hvis $\{(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)\} \subseteq W$ består af r lineært uafhængige elementer som opfylder at $\beta_i = f(\alpha_i)$ for et lineariseret polynomium f over $\mathbb{F}_{q^m}$, så er $\{\alpha_1, \ldots, \alpha_r\}$ en lineært uafhængig mængde. [KK08, Lemma 13]*

Bevis. Lad $\gamma_1, \ldots, \gamma_r \in \mathbb{F}_q$ være givet således at $\sum_{i=1}^{r} \gamma_i \alpha_i = 0$. Vi ønsker at vise at dette kun gælder hvis $\gamma_1 = \ldots = \gamma_r = 0$. Vi betragter

$$\begin{aligned}\sum_{i=1}^{r} \gamma_i(\alpha_i, \beta_i) &= \left(\sum_{i=1}^{r} \gamma_i \alpha_i, \sum_{i=1}^{r} \gamma_i \beta_i\right) \\ &= \left(\sum_{i=1}^{r} \gamma_i \alpha_i, \sum_{i=1}^{r} \gamma_i f(\alpha_i)\right) \\ &= \left(0, f\left(\sum_{i=1}^{r} \gamma_i \alpha_i\right)\right) = (0, f(0)) = (0,0) \ .\end{aligned}$$

Da $\{(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r)\}$ er lineært uafhængige og da $\sum_{i=1}^{r} \gamma_i(\alpha_i, \beta_i) = (0,0)$ følger det ønskede og $\{\alpha_1, \ldots, \alpha_r\}$ er derfor en lineært uafhængig mængde. □

Sætning 6.11. *Lad* $\mathrm{ev}_A : \mathscr{L}_{q^m}^k[x] \to \mathcal{P}(W, \ell)$ *være givet hvor* $\ell = |A| \geq k$ *og lad* $\mathcal{C}$ *være værdimængden af* ev_A*. Da er* $\mathcal{C}$ *en kode af typen* $[\ell+m, \ell, mk, 2(\ell - k + 1)]$*. [KK08, Sætning 14]*

Bevis. Kodeordene i $\mathcal{C}$ er underrum af W, der per konstruktion har dimension $\ell + m$. Desuden har alle kodeordene samme dimension, så den maksimale dimension af $\mathcal{C}$ er ℓ. Da antallet af forskellige lineariserede polynomier i $\mathscr{L}_{q^m}^k[x]$ er q^{mk} bliver antallet af kodeord i $\mathcal{C}$ også q^{mk} fra lemma 6.8. Heraf er $\log_q(|\mathcal{C}|) = mk$.

For at bestemme kodens minimumsafstand undersøges afstanden mellem to kodeord i $\mathcal{C}$. Lad $f(x)$ og $g(x)$ være forskellige polynomier i $\mathscr{L}_{q^m}^k[x]$ og definer kodeordene $V_1 = \mathrm{ev}_A(f)$ og $V_2 = \mathrm{ev}_A(g)$. Antag at $\dim(V_1 \cap V_2) = r$. Så må der findes r lineært uafhængige elementer $(\alpha_1', \beta_1'), \ldots, (\alpha_r', \beta_r')$, hvorom der gælder at $f(\alpha_i') = \beta_i' = g(\alpha_i')$ for $i \in \{1, \ldots, r\}$. Fra lemma 6.10 følger at $\alpha_1', \ldots, \alpha_r'$ er lineært uafhængige. Lad $B = \mathrm{span}\{\alpha_1', \ldots, \alpha_r'\}$ så gælder at for alle $b \in B$ at $f(b) - g(b) = 0$. Antag at $r \geq k$. Da er f og g lineariserede polynomier af grad mindre end q^k, som har mindst k lineært uafhængige fælles punkter. Fra lemma 5.4 fås så at $f(x) = g(x)$. Dette er en modstrid med konstruktionen af f og g, så heraf må $r \leq k - 1$. Afstanden mellem V_1 og V_2 bliver så

$$d(V_1, V_2) = \dim(V_1) + \dim(V_2) - 2\dim(V_1 \cap V_2) = 2\ell - 2r \geq 2(\ell - k + 1) \ ,$$

hvorfor kodens minimumsafstand er $D(\mathcal{C}) = 2(\ell - k + 1)$. □

I det følgende eksempel konstrueres en fejlkorrigerende kode over $\mathbb{F}_{2^5}$.

Eksempel 6.12. Definer $A = \{a_1, a_2, a_3\} = \{(10000), (01000), (00100)\} \subset \mathbb{F}_{2^5}$ over $\mathbb{F}_2$. Vektorrummet W er da givet ved

$$W = \text{span}\{(10000), (01000), (00100)\} \oplus \mathbb{F}_{2^5} \tag{6.11}$$

Dimensionen af W er 8 over $\mathbb{F}_2$.

Vi ønsker at danne kodeordene i $\mathcal{C}$ ved at lade beskedpolynomierne ligge i $\mathscr{L}_{2^5}^2[x]$, således at

$$f(x) = u_0 x^{q^0} + u_1 x^{q^1} ,$$

hvor $\mathbf{u} = (u_0, u_1) \in \mathbb{F}_{2^5}^2$ er beskedsymbolerne. Dette giver $2^{5\cdot 2} = 2^{10}$ kodeord i $\mathcal{C}$. Et eksempel på en blok af beskedsymboler er

$$\mathbf{u} = ((11100), (01010)) .$$

I bilag D.1 er legemet $\mathbb{F}_{2^5}$ konstrueret over det irreducible polynomium $x^5 + x^3 + 1 \in \mathbb{F}_2[x]$. Som primitivt element er valgt $x = \alpha$. Under denne konstruktion bliver beskedpolynomiet med koefficienter fra $\mathbf{u}$

$$f(x) = (\alpha^4 + \alpha^3 + \alpha^2)x^{q^0} + (\alpha^3 + \alpha)x^{q^1} ,$$

hvorved $f(a_1)$, $f(a_2)$ og $f(a_3)$ bliver

$$\begin{aligned}
f(a_1) &= (\alpha^4 + \alpha^3 + \alpha^2)(\alpha^4)^{q^0} + (\alpha^3 + \alpha)(\alpha^4)^{q^1} \\
&= \alpha^8 + \alpha^7 + \alpha^6 + \alpha^{11} + \alpha^9 \\
&= \alpha^4 + \alpha^2 + \alpha + 1 , \\
f(a_2) &= (\alpha^4 + \alpha^3 + \alpha^2)(\alpha^3)^{q^0} + (\alpha^3 + \alpha)(\alpha^3)^{q^1} \\
&= \alpha^7 + \alpha^6 + \alpha^5 + \alpha^9 + \alpha^7 \\
&= \alpha^2 + \alpha , \\
f(a_3) &= (\alpha^4 + \alpha^3 + \alpha^2)(\alpha^2)^{q^0} + (\alpha^3 + \alpha)(\alpha^2)^{q^1} \\
&= \alpha^6 + \alpha^5 + \alpha^4 + \alpha^7 + \alpha^5 \\
&= \alpha^3 + \alpha^2 + \alpha + 1 .
\end{aligned}$$

Kodeordet V svarende til beskedpolynomiet er da rummet udspændt af $(a_1, f(a_1))$, $(a_2, f(a_2))$ og $(a_3, f(a_3))$;

$$V = \text{span}\{(1000010111), (0100000110), (0010001111)\} . \tag{6.12}$$

De resterende $2^{10} - 1$ kodeord i $\mathcal{C}$ konstrueres på tilsvarende måde ved at vælge alle forskellige u'er indeholdt i $\mathbb{F}_{2^5}^2$ og gentage ovenstående procedure. Koden som er konstrueret er da en kode af typen $[8, 3, 10, 4]$. Minimumsafstanden er $D(\mathcal{C}) = 4$ så sætning 6.6 giver, at koden er i stand til at rette 1 fejl eller 1 sletning, da det kræves at $(t + \rho) < 2$. ▲

I det følgende afsnit præsenteres en struktur der kan anvendes til at dekode et modtaget underrum U til det afsendte kodeord $V \in \mathcal{C}$ under bestemte forudsætninger.

6.3 Dekodning af KK-Koden

I afsnit 6.1 blev operatorkanalen introduceret. Hvis vi sender et kodeord $V \in \mathcal{C}$ over operatorkanalen og modtager et underrum U, så fortæller sætning 6.6 at det er muligt at dekode med en minimumsafstandsdekoder hvis

$$D(\mathcal{C}) > 2(t + \rho) \; . \tag{6.13}$$

Her er t dimensionen af fejlrummet E og ρ er det maksimale antal sletninger forårsaget af operatorkanalen. Denne oplysning benyttes i det følgende til at fastsætte under hvilke betingelser, det er muligt at dekode et modtaget underrum til det afsendte kodeord.

Lad V være et kodeord i koden $\mathcal{C}$, der er konstrueret som i det foregående afsnit, således at $\dim(V) = \ell$. Vi antager i det følgende, at dimensionen af det underrum U, som modtages er $r = \ell - \rho + t$, og en basis for dette underrum betegnes ved mængden $\{(x_1, y_1), \ldots, (x_r, y_r)\}$. Under denne konstruktion er $\dim(U \cap V) = \ell - \rho$. En basis for $U \cap V$ betegnes ved mængden $\{(a_1, b_1), \ldots, (a_{\ell-\rho}, b_{\ell-\rho})\}$. Afstanden mellem U og V er da

$$\begin{aligned} d(U, V) &= \dim(U) + \dim(V) - 2\dim(U \cap V) \\ &= \ell - \rho + t + \ell - 2\ell + 2\rho = t + \rho \; . \end{aligned}$$

Fra sætning 6.11 haves at $D(\mathcal{C}) = 2(\ell - k + 1)$, så hvis $2(\ell - k + 1) > 2(t + \rho) > t + \rho$, således at betingelse (6.13) er opfyldt, er det muligt under denne konstruktion at dekode U til V.

I afsnit 5.2 blev en algoritme præsenteret, som konstruerer et ikke-nul bivariat lineariseret polynomium $Q(x, y)$ på formen (5.6). Lad den lineært uafhængige mængde som $Q(x, y)$ er konstrueret over være basen for det modtaget rum U. Så opfylder

$$Q(x, y) = Q_x(x) + Q_y(y) \;\text{ at }\; Q(x_i, y_i) = 0 \;\text{ for alle }\; (x_i, y_i) \in U \; . \tag{6.14}$$

Hvis der yderligere gælder at $Q(x, y)$ opfylder, at $Q_x(x)$ er et lineariseret polynomium over $\mathbb{F}_{q^m}$ med grad højest $q^{\tau-1}$, og at $Q_y(y)$ er et lineariseret polynomium over $\mathbb{F}_{q^m}$ med grad højest $q^{\tau-k}$, så kan $Q(x, y)$ benyttes til dekodning. Dette forklares yderligere i det følgende, hvor vi også redegører for $Q(x, y)$'s egenskaber, samt bestemmer et udtryk for parameteren τ.

Lad $f \in \mathscr{L}^k_{q^m}[x]$ så fås at

$$Q(x, f(x)) = Q_x(x) + Q_y(f(x)) = Q_x(x) + Q_y \circ f(x) \; . \tag{6.15}$$

Da $f(x)$ har grad højest q^{k-1} følger, at $Q(x, f(x))$ har grad højest $q^{\tau-1}$. Polynomiet i (5.6) kan omskrives således at udtrykket i (6.15) fremkommer;

$$\begin{aligned} Q(x,y) &= Q_x(x) + Q_y(y) + Q_y \circ f(x) - Q_y \circ f(x) \\ &= Q_x(x) + Q_y \circ f(x) + Q_y(y) - Q_y \circ f(x) \\ &= Q(x, f(x)) + Q_y(y - f(x)) \ . \end{aligned} \tag{6.16}$$

Betragtes basen for $U \cap V$ giver konstruktionen af $Q(x,y)$ at $Q(a_i, b_i) = 0$ for $i \in \{1, \ldots, \ell - \rho\}$, mens der fra konstruktionen af V gælder, at for $(a_i, b_i) \in V$ er $b_i = f(a_i)$, hvor f er et lineariseret polynomium. Dette giver at

$$0 = Q(a_i, b_i) = Q(a_i, f(a_i)) \text{ for } i \in \{1, \ldots, \ell - \rho\} \ .$$

Så $Q(x, f(x))$ er et lineariseret polynomium med rødder $a_1, \ldots, a_{\ell-\rho}$. Heraf er $Q(x, f(x))$ et lineariseret polynomium af grad højest $q^{\tau-1}$ som evaluerer til nul på et rum med dimensionen $\ell - \rho$. Hvis tilfældet er at

$$\ell - \rho \geq \tau \ , \tag{6.17}$$

så må $Q(x, f(x))$ have flere nulpunkter end dets grad, hvilket kun er muligt hvis $Q(x, f(x)) = 0$. Under antagelsen (6.17) giver (6.16) så at $Q(x,y) = Q_y(y - f(x))$ og $-Q_x(x) = Q_y(f(x))$, da $Q(x,y)$ og $Q(x, f(x))$ er bivariate lineærerede polynomier.

Som nævnt i det foregående er det muligt at dekode hvis

$$\ell - k + 1 > t + \rho \ . \tag{6.18}$$

Det bemærkes desuden at da $\dim(U) = r$ kan (6.14) betragtes som et homogent ligningssystem bestående af r ligninger med $2\tau - k + 1$ ubekendte. Et sådant system har en ikke-nulløsning hvis der er flere ubekendte end ligninger. Heraf ønskes at

$$r = \ell - \rho + t < 2\tau - k + 1$$

Denne ulighed er opfyldt hvis

$$\begin{aligned} r + k &= \ell - \rho + t + k < 2\tau + 1 \\ &\leq 2\tau \ , \end{aligned}$$

så ved at vælge

$$\tau = \left\lceil \frac{r+k}{2} \right\rceil \tag{6.19}$$

opnås det ønskede. Desuden giver (6.19) sammen med (6.18) at

$$\begin{aligned} \tau &= \left\lceil \frac{\ell - \rho + t + k}{2} \right\rceil \\ &< \left\lceil \frac{\ell - \rho + \ell - \rho + 1}{2} \right\rceil = \left\lceil \ell - \rho + \frac{1}{2} \right\rceil \ , \end{aligned}$$

hvorfor

$$\tau \leq \ell - \rho + \frac{1}{2} \,. \tag{6.20}$$

Da τ er et heltal er (6.17) opfyldt. Heraf fås, at forudsætningerne for at det konstruerede bivariat lineariserede polynomium $Q(x, y)$ kan anvendes til dekodning er, at graden af $Q(x, y)$ er højest $q^{\tau-1}$ hvor τ er bestemt ved (6.19). Desuden skal koden $\mathcal{C}$ konstrueres således at minimumsafstanden er tilstrækkelig stor som angivet i sætning 6.6.

Bemærkning 6.13. Det er muligt at bestemme τ da både k og r er kendt ved dekoderen. Den oprindelige kode $\mathcal{C}$ er kendt, og dennes minimumsafstand er givet ved $2(\ell - k + 1)$ hvorfra k kan udledes. Ellers, hvis konstruktionen af koden også er kendt, så vides hvilken mængde $\mathscr{L}_{q^m}^k[x]$ beskedpolynomierne tilhører, hvorfra k kan aflæses direkte. Desuden fastsættes r fra det modtaget rum U, da r er dimensionen af U.

Samlet giver det foregående følgende dekodningsmetode;

1. Lad en basis for U være givet og konstruer $Q(x, y)$ ud fra algoritme 3. Hvis graden af $Q(x, y)$ er højest $q^{\tau-1}$ kan $Q(x, y)$ benyttes til dekodning.

2. Ved anvendelse af algoritme 2 med input $a(x) = -Q_x(x)$ og $b(x) = Q_y(x)$ kan $q(x) = f(x)$ bestemmes såfremt $r(x) = 0$.

3. Fra kodens konstruktion kendes mængden $A = \{\alpha_1, \ldots, \alpha_\ell\}$ så en basis for $\tilde{V}$ bliver $\{(\alpha_1, f(\alpha_1)), \ldots, (\alpha_\ell, f(\alpha_\ell))\}$. Hvis $d(U, \tilde{V}) < \ell - k + 1$ er opfyldt så er $\tilde{V}$ et kodeord i $\mathcal{C}$.

Årsagen til at algoritme 3 benyttes til at bestemme $Q(x, y)$ i stedet for Gauss elimination er at løsning af ligningssystemer er mere krævende. Ved Gauss elimination haves en matrix af størrelsen $r \times (2\tau - k + 1)$ og der kræves så i det værste tilfælde

$$\begin{aligned} r(2\tau - k + 1 - 1) + (r - 1)(2\tau - k + 1 - 2) + \cdots + 1(2\tau - k + 1 - r) \\ \leq r^2(2\tau - k + 1) \leq (\ell + m)^2(2\tau - k + 1) \end{aligned}$$

multiplikationer og additioner til at bestemme $Q(x, y)$. Heraf er kompleksiteten af Gauss elimination $O((\ell + m)^2(2\tau - k + 1))$. Jævnfør bemærkning 5.16 er algorime 3 mere effektiv.

I det følgende eksempel benyttes algoritme 3 fra side 57 til at dekode et modtaget rum U til et kodeord V.

Eksempel 6.14. Lad $\mathcal{C}$ være koden konstrueret i eksempel 6.12 indeholdt i vektorrummet W, jævnfør ligning (6.11). Denne kode er konstrueret således at der ved dekodning kan fejlkorrigeres op til én fejl. Denne fejl er enten en sletning forårsaget af operatorkanalen hvorved $U = \mathcal{H}_2(V) \oplus \{0\}$ eller en tilførelse af fejlinformation således at $U = V \oplus E$, hvor $\dim(E) = 1$. Følgende illustreres først at dekodning er muligt, når fejlen er forårsaget af en sletning påført af operatorkanalen, og efterfølgende at dekodning også er mulig, når fejlen er forårsaget af uønsket information.

Antag at det modtaget rum U er givet ved

$$U = \text{span}\{(1100010001), (1110011110)\} .$$

Dimensionen af U er her $r = 2$. For at kunne dekode har vi også brug for at kende k. Fra kodens konstruktion ved vi at beskedpolynomierne ligger i $\mathscr{L}_{2^5}^2[x]$, hvorfor $k = 2$. Vi anvender algoritme 3 til at dekode U med input $B = \{(1100010001), (1110011110)\}$. Algoritmen begynder med at definere

$$h_0(x, y) = x; \quad h_1(x, y) = y;$$

Herefter gennemløbes **for**-løkken for $i = 1$ og $i = 2$;

For $i = 1$: $\Delta_0 := (11000) = \alpha^4 + \alpha^3$; $\Delta_1 := (10001) = \alpha^4 + 1$. Da hverken Δ_0 eller Δ_1 er nul undersøges $(1, k-1)$-vægtet grad af $h_0(x, y)$ og $h_1(x, y)$.

$$\begin{aligned} \deg_{1,k-1}(h_0) &= \max\{0, 2 - 1 - \infty\} = 0; \\ \deg_{1,k-1}(h_1) &= \max\{-\infty, 2 - 1 + 0\} = 1; \end{aligned}$$

Da graden af $h_0(x, y)$ er mindre en graden af $h_1(x, y)$ fås at $h_0(x, y) \prec h_1(x, y)$ så

$$\begin{aligned} h_1(x, y) &:= (\alpha^4 + 1)x + (\alpha^4 + \alpha^3)y , \\ h_0(x, y) &:= x^2 + (\alpha^4 + \alpha^3)^{2-1}x = x^2 + (\alpha^4 + \alpha^3)x . \end{aligned}$$

For $i = 2$: $\Delta_0 := (\alpha^4 + \alpha^3 + \alpha^2)^2 + (\alpha^4 + \alpha^3)(\alpha^4 + \alpha^3 + \alpha^2) = \alpha^3 + \alpha + 1$; $\Delta_1 := (\alpha^4 + 1)(\alpha^4 + \alpha^3 + \alpha^2) + (\alpha^4 + \alpha^3)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha) = \alpha^4 + \alpha + 1$; Igen er hverken Δ_0 eller Δ_1 nul så den $(1, k-1)$-vægtet grad bestemmes;

$$\begin{aligned} \deg_{1,k-1}(h_0) &= \max\{1, 2 - 1 - \infty\} = 1; \\ \deg_{1,k-1}(h_1) &= \max\{0, 2 - 1 + 0\} = 1; \end{aligned}$$

Der haves lighed, så

$$\begin{aligned} h_1(x, y) &:= (\alpha^4 + \alpha + 1)(x^2 + (\alpha^4 + \alpha^3)x) + (\alpha^3 + \alpha + 1)((\alpha^4 + 1)x + (\alpha^4 + \alpha^3)y) \\ &= (\alpha^4 + \alpha + 1)x^2 + (\alpha^3 + 1)x + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha)y , \\ h_0(x, y) &:= (x^2 + (\alpha^4 + \alpha^3)x)^2 + (\alpha^3 + \alpha + 1)^{2-1}(x^2 + (\alpha^4 + \alpha^3)x) \\ &= x^{2^2} + (\alpha + 1)x^2 + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha)x . \end{aligned}$$

Den $(1, k-1)$-vægtet grad af $h_0(x,y)$ og $h_1(x,y)$ sammenlignes for at afgøre output af algoritmen.

$$\deg_{1,k-1}(h_0(x,y)) = \max\{2, 2-1+0\} = 2;$$
$$\deg_{1,k-1}(h_1(x,y)) = \max\{1, 2-1+0\} = 1;$$

Da $h_1(x,y) \prec h_0(x,y)$ bliver output

$$Q(x,y) := h_1(x,y) = (\alpha^4+\alpha+1)x^2 + (\alpha^3+1)x + (\alpha^4+\alpha^3+\alpha^2+\alpha)y\,.$$

Hvis $Q(x,y)$ skal kunne benyttes til dekodning er det en forudsætning at graden af $Q_x(x)$ er højest $q^{\tau-1}$, og graden af $Q_y(y)$ er højest $q^{\tau-k}$. Konstanten τ er givet ved $\tau = \left\lceil \frac{2+2}{2} \right\rceil = 2$ da $r=2$ og $k=2$. Da $\deg(Q_x(x)) = q^1$ og $\deg(Q_y(y)) = q^0$ er dette opfyldt og vi har opnået succes ved anvendelse af algoritme 3.

For at færdiggøre dekodningen skal algoritme 2 benyttes til at bestemme beskedpolynomiet $f(x)$. Vi lader $a(x) := -Q_x(x) = (\alpha^4+\alpha+1)x^2+(\alpha^3+1)x$ og $b(x) := Q_y(x) = (\alpha^4+\alpha^3+\alpha^2+\alpha)x$ og gennemløber algoritmen. Dette giver output

$$q(x) = (\alpha^3+\alpha)x^2 + (\alpha^4+\alpha^3+\alpha^2)x; \quad r(x) = 0;$$

hvorfor beskedpolynomiet er

$$f(x) := q(x) = (\alpha^3+\alpha)x^2 + (\alpha^4+\alpha^3+\alpha^2)x\,. \tag{6.21}$$

Ved at benytte mængden A fra konstruktionen af koden $\mathcal{C}$ opnås kodeordet

$$\tilde{V} = \text{span}\{(1000010111), (0100000110), (0010001111)\}\,. \tag{6.22}$$

Da

$$\begin{aligned} d(U,\tilde{V}) &= 2\dim(U+\tilde{V}) - \dim(U) - \dim(\tilde{V}) \\ &= 2\cdot 3 - 2 - 3 = 1 < \ell - k + 1 = 2\,, \end{aligned}$$

er det lykkedes at dekode U til et kodeord i $\mathcal{C}$. Desuden er dette kodeord præcis kodeordet fra (6.12).

Dekodningsalgoritmen bør også være i stand til at fejlkorrigere når det underrum U, som er modtaget, har konstruktionen $U = V \oplus E$, hvor $V \in \mathcal{C}$ og $\dim(E) = 1$. Dette undersøges ved at lade $E = \{(0000000001)\}$ således at det modtaget underrum bliver

$$U = \text{span}\{(1100010001), (1110011111), (0110001001), (0010001111)\}$$

Algoritme 3 benyttes på sammen vis som ovenfor til at bestemme $Q(x, y)$. Dette giver

$$Q(x,y) := h_1(x,y) = x^{2^2} + (\alpha^4+\alpha^3+\alpha^2+\alpha)x^2 + x + \alpha^4 y^2 + (\alpha^3+\alpha^2+1)y$$

I dette tilfælde er $\tau = \left\lceil \frac{4+2}{2} \right\rceil = 3$ så $Q_x(x)$ og $Q_y(y)$ opfylder betingelserne for dekodning. Igen benyttes algoritme 2 med $a(x) := Q_x(x) = x^{2^2} + (\alpha^4 + \alpha^3+\alpha^2+\alpha)x^2+x$ og $b(x) := Q_y(x) = \alpha^4 x^2 + (\alpha^3+\alpha^2+1)x$ til at bestemme beskedpolynomiet. Her fås at $r(x) = 0$ så

$$f(x) := q(x) = (\alpha^3+\alpha)x^2 + (\alpha^4+\alpha^3+\alpha^2)x\ .$$

Dette beskedpolynomium er det sammen som i (6.21) hvorved det dekodet kodeord igen bliver $\tilde{V}$ i (6.22). ▲

Kapitel 7

Singleton Grænsen

I dette kapitel ses der på Singleton Grænsen for koder $\mathcal{C}$ over rummet $\mathcal{P}(W, \ell)$. Vi bestemmer grænsen for konstant-dimensionskoder. Sidst i kapitlet ses der på KK-kodens evne til at nå Singleton Grænsen. Først beskrives imidlertid hvorledes det er muligt at bestemme nye koder ud fra en allerede eksisterende kode.

7.1 Den Punkterede Kode

Først betragtes hvordan koder over rummet $\mathcal{P}(W, \ell)$ kan punkteres. Antag, at $\mathcal{C}$ er en kode af konstant dimension over rummet $\mathcal{P}(W, \ell)$. Her har W dimensionen N, og $\mathcal{C}$ består af underrum fra W af dimension ℓ. Lad W^* være et underrum af W af dimension $N-1$. Den punkterede kode $\mathcal{C}^*$ af $\mathcal{C}$ opnås så ved at erstatte ethvert kodeord $V \in \mathcal{C}$ med $V^* = \mathcal{H}_{\ell-1}(V \cap W^*)$, hvor $\mathcal{H}_{\ell-1}$ er sletningsoperatoren. Der er to mulige situationer for dette. Hvis $V \cap W^*$ har dimension $\ell - 1$ så $V \not\subset W^*$, og der gælder at $V^* = V \cap W^*$ bliver kodeord i $\mathcal{C}^*$. Hvis V er et underrum i W^* erstattes kodeordet $V \in \mathcal{C}$ med et $\ell - 1$ dimensionalt underrum af V, som så bliver et kodeord i den punkterede kode $\mathcal{C}^*$. Heraf ses at punkteringskoden ikke nødvendigvis er entydig. For den punkterede kode haves følgende sætning.

Sætning 7.1. *Lad $\mathcal{C} \subseteq \mathcal{P}(W, \ell)$ være en $[N, \ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$ kode med $D(\mathcal{C}) > 2$, hvor alle kodeord i $\mathcal{C}$ har dimension ℓ, og lad W^* være et $(N-1)$-dimensionalt underrum af W. Så gælder der, at $\mathcal{C}^*$ er en $[N-1, \ell-1, \log_q |\mathcal{C}|, D(\mathcal{C}^*)]$ kode med konstant dimension hvor $D(\mathcal{C}^*) \geq D(\mathcal{C}) - 2$. [KK08, Sætning 8]*

Bevis. Konstruktionen af $\mathcal{C}^*$ giver at det kun er kardinaliteten og minimumsafstanden af koden der skal vises. Minimumsafstanden betragtes først. Lad V_1 og V_2 være to forskellige kodeord i $\mathcal{C}$, så er $V_1^* = \mathcal{H}_{\ell-1}(V_1 \cap W^*)$ og $V_2^* = \mathcal{H}_{\ell-1}(V_2 \cap W^*)$ kodeord i $\mathcal{C}^*$. Her gælder der, at $V_1^* \subset V_1$ og $V_2^* \subset V_2$ og derfor er $V_1^* \cap V_2^* \subseteq V_1 \cap V_2$. Dette giver, at

$$2\dim(V_1^* \cap V_2^*) \leq 2\dim(V_1 \cap V_2) \leq 2\ell - D(\mathcal{C}),$$

da $d(V_1, V_2) = 2\ell - 2\dim(V_1 \cap V_2) \geq D(\mathcal{C})$. For den punkterede kode $\mathcal{C}^*$ haves derfor

$$\begin{aligned} d(V_1^*, V_2^*) &= \dim(V_1^*) + \dim(V_2^*) - 2\dim(V_1^* \cap V_2^*) \\ &= 2(\ell - 1) - 2\dim(V_1^* \cap V_2^*) \\ &\geq 2\ell - 2 - (2\ell - D(\mathcal{C})) \qquad (7.1) \\ &= D(\mathcal{C}) - 2. \end{aligned}$$

Da V_1 og V_2 var valgt arbitrært i $\mathcal{C}$ gælder ulighed (7.1) for alle kodeord V_1^* og V_2^* i $\mathcal{C}^*$, hvor $V_1 \neq V_2$, og der fås at $D(\mathcal{C}^*) \geq D(\mathcal{C}) - 2$.

Per antagelse er $D(\mathcal{C}) > 2$, så minimumsafstanden for $\mathcal{C}^*$ er $d(V_1^*, V_2^*) > 0$ for alle $V_1^*, V_2^* \in \mathcal{C}^*$, hvor $V_1 \neq V_2$ i $\mathcal{C}$. Derfor er V_1^* og V_2^* forskellige i $\mathcal{C}^*$. Dette giver at antallet af kodeord i $\mathcal{C}^*$ er lig antallet af kodeord i $\mathcal{C}$, og kardinaliteten af $\mathcal{C}^*$ er $\log_q |\mathcal{C}|$. □

Bemærkning 7.2. Hvis der foretages en punktering i koden $\mathcal{C}^*$, fås en ny kode $\tilde{\mathcal{C}}^*$ hvis minimumsafstand er begrænset ved $D(\tilde{\mathcal{C}}^*) \geq D(\mathcal{C}^*) - 2 \geq (D(\mathcal{C}) - 2) - 2 = D(\mathcal{C}) - 4$. Af dette fås at foretages der k punkteringer i koden $\mathcal{C}$ så har minimumsafstanden i den nye kode $\mathcal{C}^*$ egenskaben at $D(\mathcal{C}^*) \geq D(\mathcal{C}) - 2k$.

7.2 Komplementærkoden

Udover punkteringskoden $\mathcal{C}^*$ er det også muligt at konstruere komplementærkoden $\mathcal{C}^\perp$ til koden $\mathcal{C} \subseteq \mathcal{P}(W, \ell)$. Først bestemmes komplementærmængden til et kodeord i $\mathcal{C}$. For et kodeord $V \in \mathcal{C}$, som er et underrum i W, er komplementærmængden $V^\perp$ i W givet ved

$$V^\perp = \{\tilde{\mathbf{v}} \in W \mid \tilde{\mathbf{v}} \cdot \mathbf{v} = 0 \text{ for alle } \mathbf{v} \in V\},$$

hvor $\tilde{\mathbf{v}} \cdot \mathbf{v}$ betegner det indre produkt mellem vektorerne $\tilde{\mathbf{v}}$ og $\mathbf{v}$. Når kodeordet V har dimension ℓ så har $V^\perp$ dimension $N - \ell$. Det er heraf muligt definere komplementærkoden.

Definition 7.3 (Komplementærkode)**.** Lad $\mathcal{C}$ være en kode i $\mathcal{P}(W, \ell)$ så er komplementærkoden til $\mathcal{C}$ givet ved

$$\mathcal{C}^\perp = \{V^\perp \subset W \mid V \in \mathcal{C}\}.$$

For komplementærkoden til en konstant-dimensionskode haves følgende.

Sætning 7.4. *Lad $\mathcal{C}$ være en $[N, \ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$ kode med konstant dimension, så er komplementærkoden $\mathcal{C}^\perp$ en $[N, N-\ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$ kode med konstant dimension. [KK08, s.8]*

Bevis. Da begge koder $\mathcal{C}$ og $\mathcal{C}^\perp$ består af underrum fra W, der har dimension N, skal kun dimensionen af kodeordene, kardinaliteten og minimumsafstand bestemmes for $\mathcal{C}^\perp$. Først betragtes dimensionen af kodeordene i $\mathcal{C}^\perp$; Der gælder for et kodeord $V \in \mathcal{C}$ at $\dim(V) + \dim(V^\perp) = \dim(W)$, og af dette fås

$$\dim(V^\perp) = \dim(W) - \dim(V) = N - \ell,$$

da alle $V \in \mathcal{C}$ har dimension ℓ. Det vil sige at alle kodeord i $\mathcal{C}^\perp$ har dimension $N - \ell$.

For kardinaliteten haves, at da $V^\perp$ kun er et kodeord i $\mathcal{C}^\perp$, hvis V er et kodeord i $\mathcal{C}$, må der gælde at $|\mathcal{C}^\perp| = |\mathcal{C}|$.

Lad $V_1^\perp, V_2^\perp \in \mathcal{C}^\perp$ så er afstanden mellem disse kodeord

$$\begin{aligned} d(V_1^\perp, V_2^\perp) &= \dim(V_1^\perp + V_2^\perp) - \dim(V_1^\perp \cap V_2^\perp) \\ &= \dim((V_1 \cap V_2)^\perp) - \dim((V_1 + V_2)^\perp) \\ &= N - \dim(V_1 \cap V_2) - (N - \dim(V_1 + V_2)) \\ &= \dim(V_1 + V_2) - \dim(V_1 \cap V_2) \\ &= d(V_1, V_2). \end{aligned}$$

Heraf er afstanden mellem to kodeord $V_1, V_2 \in \mathcal{C}$ bevaret. Dette gælder specielt for minimumsafstanden hvilket vil sige at $D(\mathcal{C}^\perp) = D(\mathcal{C})$. Koden $\mathcal{C}^\perp$ er derfor en $[N, N-\ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$ kode. □

Fra komplementærkodens egenskaber fås derfor at for koder med konstant dimension kan vi begrænse os selv til at kigge på koder af typen $[N, \ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$ hvor $\ell \leq N - \ell$. Dette skyldes at for en kode $\mathcal{C}$ hvor $\ell > N - \ell$ kan vi erstatte $\mathcal{C}$ med $\mathcal{C}^\perp$ men bevare afstandsforholdene, hvilket betyder at $\mathcal{C}^\perp$ har de samme fejlretningsevner.

7.3 Den Gaussiske Koefficient og Singleton Grænsen

Inden Singleton Grænsen gives defineres den q-ære Gaussiske koefficient, som giver antallet af forskellige underrum af dimension r i et m-dimensionalt vektorrum over $\mathbb{F}_q$.

7.3. DEN GAUSSISKE KOEFFICIENT OG SINGLETON GRÆNSEN

Definition 7.5 (q-ær Gaussisk koefficient)**.** For ikke-negative heltal m og r, hvor $r \leq m$, er den q-ære Gaussiske koefficient givet ved

$$\begin{bmatrix} m \\ r \end{bmatrix}_q = \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)} = \prod_{i=0}^{r-1} \frac{q^{m-i}-1}{q^{r-i}-1}.$$

I tilfælde $r = 0$ haves at $\begin{bmatrix} m \\ r \end{bmatrix}_q = 1$. [KK08]

Den Gaussiske koefficient har følgende egenskaber.

Lemma 7.6. *Den q-ære Gaussiske koefficient er symmetrisk og på intervallerne $\left[0, \lfloor \frac{m}{2} \rfloor\right]$ og $\left[\lceil \frac{m}{2} \rceil, m\right]$ er den hhv. stigende og aftagende.*

Bevis. Det vises først at den q-ære Gaussiske koefficient er symmetrisk. Betragt

$$\begin{aligned}
\begin{bmatrix} m \\ r \end{bmatrix}_q &= \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)} \\
&= \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-r+1}-1)(q^{m-r}-1)\cdots(q-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)(q^{m-r}-1)\cdots(q-1)} \\
&= \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{r+1}-1)}{(q^{m-r}-1)(q^{m-r-1}-1)\cdots(q-1)} \\
&= \begin{bmatrix} m \\ m-r \end{bmatrix}_q,
\end{aligned}$$

heraf er $\begin{bmatrix} m \\ r \end{bmatrix}_q = \begin{bmatrix} m \\ m-r \end{bmatrix}_q$ for alle $r \in [0, m]$. Specielt fås at koefficienten er symmetrisk omkring

$$\begin{bmatrix} m \\ \lfloor \frac{m}{2} \rfloor \end{bmatrix}_q \text{ og } \begin{bmatrix} m \\ \lceil \frac{m}{2} \rceil \end{bmatrix}_q.$$

Den q-ære Gaussiske koefficient betragtes på intervallet $\left[0, \lfloor \frac{m}{2} \rfloor\right]$, hvis koefficienten er stigende på dette interval gælder der af symmetrien, at den er aftagende på intervallet $\left[\lceil \frac{m}{2} \rceil, m\right]$. Antag, at $k \in \left[1, \lfloor \frac{m}{2} \rfloor\right]$, så haves

$$\begin{bmatrix} m \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^{m-i}-1}{q^{k-i}-1} = \frac{q^{m-k+1}-1}{q^k-1} \prod_{i=0}^{k-2} \frac{q^{m-i}-1}{q^{k-1-i}-1} = \frac{q^{m-k+1}-1}{q^k-1} \begin{bmatrix} m \\ k-1 \end{bmatrix}_q.$$

Der gælder, at $\frac{q^{m-k+1}-1}{q^k-1} > 1$ for $k \in \left[1, \lfloor \frac{m}{2} \rfloor\right]$, altså er $\begin{bmatrix} m \\ k \end{bmatrix}_q > \begin{bmatrix} m \\ k-1 \end{bmatrix}_q$, og koefficienten er stigende på intervallet. □

Ovenstående lemma medfører at for $q > 1$ har den Gaussiske koefficient en øvre begrænsning.

Lemma 7.7. *Lad $q > 1$, da opfylder den q-ære Gaussiske koefficient, $\begin{bmatrix} m \\ r \end{bmatrix}_q$, at*

$$q^{-r(m-r)} \begin{bmatrix} m \\ r \end{bmatrix}_q < 4,$$

for $0 < r < m$. [KK08, lemma 4]

Bevis. Der gælder for den Gaussiske koefficient at denne kan skrives som

$$\begin{aligned}
\begin{bmatrix} m \\ r \end{bmatrix}_q &= \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)} \\
&= \frac{q^m q^{m-1}\cdots q^{m-r+1}}{q^r q^{r-1}\cdots q} \cdot \frac{(1-q^{-m})(1-q^{-m+1})\cdots(1-q^{-m+r-1})}{(1-q^{-r})(1-q^{-r+1})\cdots(1-q^{-1})} \\
&= q^{r(m-r)} \frac{(1-q^{-m})(1-q^{-m+1})\cdots(1-q^{-m+r-1})}{(1-q^{-r})(1-q^{-r+1})\cdots(1-q^{-1})} \\
&< q^{r(m-r)} \frac{1}{(1-q^{-r})(1-q^{-r+1})\cdots(1-q^{-1})} \qquad (7.2) \\
&< q^{r(m-r)} \prod_{j=1}^{\infty} \frac{1}{1-q^{-j}} \,. \qquad (7.3)
\end{aligned}$$

Uligheden i (7.2) og (7.3) følger af at $1 - q^{-k} < 1$ for $k \geq 1$. Da $q \geq 2$ fås at

$$\prod_{j=1}^{\infty} \frac{1}{1-q^{-j}} \leq \prod_{j=1}^{\infty} \frac{1}{1-2^{-j}} = \frac{1}{Q_0} < 4 \,,$$

hvor $Q_0 \approx 0,2888$, [Ber80, s.577]. Af dette fås at $q^{-r(m-r)} \begin{bmatrix} m \\ r \end{bmatrix}_q < 4$. □

Følgende gives Singleton Grænsen.

Sætning 7.8 (Singleton Grænsen)**.** *Lad $\mathcal{C} \subseteq \mathcal{P}(W, \ell)$ være en $[N, \ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$ kode, hvor W er et N-dimensionalt vektorrum over $\mathbb{F}_q$. Så gælder der om $\mathcal{C}$, at*

$$|\mathcal{C}| \leq \begin{bmatrix} N - \frac{D(\mathcal{C})-2}{2} \\ \max\{\ell, N-\ell\} \end{bmatrix}_q .$$

[KK08, Sætning 9]

Bevis. Først ønskes det at punktere $\mathcal{C}$ i alt $\frac{D(\mathcal{C})-2}{2}$ gange, hvilket er muligt, da enhver afstand mellem kodeord i $\mathcal{C}$ er lige, så $\frac{D(\mathcal{C})-2}{2}$ er et heltal. Af disse punkteringer opnås koden $\mathcal{C}^*$ af typen $\left[N - \frac{D(\mathcal{C})-2}{2}, \ell - \frac{D(\mathcal{C})-2}{2}, \log_q |\mathcal{C}|, D(\mathcal{C}^*)\right]$, hvor alle kodeord i $\mathcal{C}^*$ har dimension $\ell - \frac{D(\mathcal{C})-2}{2}$. Fra bemærkning 7.2 gælder at minimumsafstanden $D(\mathcal{C}^*) \geq 2$. Det vil sige at $\mathcal{C}^*$ stadig har det samme

antal kodeord som $\mathcal{C}$, men at den optræder i rummet $\mathcal{P}\left(W, \ell - \frac{D(\mathcal{C})-2}{2}\right)$. Koden $\mathcal{C}^*$ kan ikke have flere kodeord end der er underrum af dimension $\ell - \frac{D(\mathcal{C})-2}{2}$ i W, og antallet af disse er givet ved den q-ære Gaussiske koefficient. Der haves derfor at

$$|\mathcal{C}^*| \leq \begin{bmatrix} N - \frac{D(\mathcal{C})-2}{2} \\ \ell - \frac{D(\mathcal{C})-2}{2} \end{bmatrix}_q = \begin{bmatrix} N - \frac{D(\mathcal{C})-2}{2} \\ N - \ell \end{bmatrix}_q = a \; . \tag{7.4}$$

Ved at kigge på den punkterede komplementærkode til $\mathcal{C}$ fås tilsvarende, at

$$\left|(\mathcal{C}^{\perp})^*\right| \leq \begin{bmatrix} N - \frac{D(\mathcal{C})-2}{2} \\ N - \ell - \frac{D(\mathcal{C})-2}{2} \end{bmatrix}_q = \begin{bmatrix} N - \frac{D(\mathcal{C})-2}{2} \\ \ell \end{bmatrix}_q = b \; .$$

Hvis det antages, at $\ell < N - \ell$ gælder der, at

$$\ell - \frac{D(\mathcal{C}) - 2}{2} < \ell < N - \ell \; .$$

Lemma 7.6 og ligning (7.4) giver således at $a < b$ hvis og kun hvis $\ell < N - \ell$.

Da koderne $\mathcal{C}, \mathcal{C}^*$ og $(\mathcal{C}^{\perp})^*$ alle indeholder det samme antal kodeord gælder der, at

$$|\mathcal{C}| \leq \begin{bmatrix} N - \frac{D(\mathcal{C})-2}{2} \\ \max\{\ell, N - \ell\} \end{bmatrix}_q \; .$$

□

Udover at have en øvre grænse for antallet af mulige kodeord er det også interessant at bestemme en øvre grænse for informationshastigheden for koden. Informationshastigheden for en kode er defineret ved følgende.

Definition 7.9. Lad $\mathcal{C}$ være en kode af typen $[N, \ell, \log_q |\mathcal{C}|, D(\mathcal{C})]$. Da er informationshastigheden for $\mathcal{C}$

$$R = \frac{\log_q (|\mathcal{C}|)}{N\ell} \; .$$

Til grænsen for informationshastigheden behøves lille-o notation, den er givet ved følgende.

Definition 7.10. Lad $f, g : \mathbb{Z}^+ \to \mathbb{R}^+$ været givet. Funktionen $f(x)$ siges at være lille-o af $g(x)$, skrives $f(x) = o(g(x))$, hvis der for $c \in \mathbb{Z}^+$ eksisterer $k \in \mathbb{Z}^+$, således at for $k < x$ gælder der, at $f(x) \leq cg(x)$.

Den øvre grænse for informationshastigheden for $\mathcal{C}$ kan bestemmes vha. Singleton Grænsen.

Korollar 7.11. *Lad $\mathcal{C}$ være en $[N, \ell, \log_q|\mathcal{C}|, D(\mathcal{C})]$ kode med konstant dimension, hvor $\ell \leq \frac{N}{2}$, da er informationshastigheden for $\mathcal{C}$ øvre begrænset af*

$$R \leq 1 - \frac{\ell+1}{N} + \frac{1}{\ell} - \frac{D(\mathcal{C})}{2\ell} + \frac{D(\mathcal{C})}{2N} + \frac{o(1)}{N\ell} ,$$

hvor $\frac{o(1)}{N\ell} \to 0$ for $N \to \infty$. [KK08, Korollar 10]

Bevis. For koden $\mathcal{C}$ gælder der af definition 7.9, at $R = \frac{\log_q|\mathcal{C}|}{N\ell}$. Fra Singleton grænsen haves der, at

$$R = \frac{\log_q|\mathcal{C}|}{N\ell} \leq \frac{\log_q\left(\left[\begin{smallmatrix} N-\frac{D(\mathcal{C})-2}{2} \\ \max\{\ell, N-\ell\}\end{smallmatrix}\right]_q\right)}{N\ell} = \frac{\log_q\left(\left[\begin{smallmatrix} N-\frac{D(\mathcal{C})-2}{2} \\ N-\ell\end{smallmatrix}\right]_q\right)}{N\ell} ,$$

da det er antaget, at $\ell \leq \frac{N}{2}$. Fra lemma 7.7 fås derfor at

$$\begin{aligned} R &< \frac{\log_q\left(4q^{(N-\ell)\left(N-\frac{D(\mathcal{C})-2}{2}-N+\ell\right)}\right)}{N\ell} \\ &= \frac{(N-\ell)\left(\ell-\frac{D(\mathcal{C})-2}{2}\right)}{N\ell} + \frac{\log_q(4)}{N\ell} \\ &= \frac{N\ell - \frac{N(D(\mathcal{C})-2)}{2} - \ell^2 + \frac{\ell(D(\mathcal{C})-2)}{2}}{N\ell} + \frac{\log_q(4)}{N\ell} \\ &= 1 - \frac{\ell+1}{N} + \frac{1}{\ell} - \frac{D(\mathcal{C})}{2\ell} + \frac{D(\mathcal{C})}{2N} + \frac{\log_q(4)}{N\ell} . \end{aligned}$$

Da $\log_q(4)$ er konstant gælder der, at $\log_q(4) = o(1)$, og korollaret er vist. □

Det er interessant at finde koder der kan nå Singleton Grænsen, således at det maksimale antal mulige kodeord i en kode $\mathcal{C}$ opnås og hermed højeste informationshastighed. Vi betragter KK-koden konstrueret i afsnit 6.2. Der gælder af sætning 6.11 at KK-koden er en $[\ell+m, \ell, mk, 2(\ell-k+1)]$ kode af konstant dimension, og ud fra dette bliver informationshastigheden for KK-koden

$$R = \frac{\log_q|\mathcal{C}|}{N\ell} = \frac{mk}{(\ell+m)\ell} . \tag{7.5}$$

Af korollar 7.11 er Singleton Grænsen for KK-koden

$$\begin{aligned} R &\leq 1 - \frac{\ell+1}{\ell+m} + \frac{1}{\ell} - \frac{2(\ell-k+1)}{2\ell} + \frac{2(\ell-k+1)}{2(\ell+m)} + \frac{o(1)}{(\ell+m)\ell} \\ &= \frac{k}{\ell} - \frac{k}{\ell+m} + \frac{o(1)}{(\ell+m)\ell} \\ &= \frac{mk}{(\ell+m)\ell} + \frac{o(1)}{(\ell+m)\ell} . \end{aligned} \tag{7.6}$$

7.3. DEN GAUSSISKE KOEFFICIENT OG SINGLETON GRÆNSEN

Da størrelsen $\frac{o(1)}{(\ell+m)\ell}$ går imod nul for $\ell + m \to \infty$, fås at informationshastigheden R for KK-koden, (7.5), har samme asymptotiske opførsel som Singleton Grænsen, (7.6). KK-koden opnår derfor tilnærmelsesvis Singleton Grænsen.

Kapitel 8

Forberedelse til Liste-L-Dekodning

Vi har i de foregående kapitler fokuseret på det fejlkorrigerende netværkskodningsproblem, hvor dekodning var baseret på en minimumsafstandsdekoder. Vi ønsker at forbedre dekodningsradiusen i det efterfølgende, hvorfor vi modificerer KK-koden således at den kan benyttes til liste-L-dekodning. Dette medfører yderligere at det er nødvendigt at udvide de resterende begreber, som er benyttet i konstruktionen og dekodningen af KK-koden. Dette kapitel indeholder derfor en konstruktion af en kommutativ delring, konstruktion af et multivariat lineariseret polynomium og en algoritme, som kan løse ligninger over ringen af lineariserede polynomier.

Det multivariate lineariserede polynomium er givet tilsvarende det bivariate lineariserede polynomium i definition 5.9. Vi antager i det følgende at det multivariate lineariseret polynomium altid er et polynomium i $(L+1)$ variable.

Definition 8.1. Et multivariat lineariseret polynomium er et polynomium på formen

$$Q(x_0, \ldots, x_L) = Q_0(x_0) + Q_1(x_1) + \cdots + Q_L(x_L) \ ,$$

hvor $Q_i(x_i)$ er et lineariseret polynomium med grad $q^{d_i(Q)}$ for $i \in \{0, \ldots, L\}$. I tilfælde hvor $Q_i(x_i) = 0$ defineres $d_i(Q) = -\infty$.

8.1 Kommutativ Delring

I dette afsnit bestemmes en kommutativ delring af $\mathscr{L}_{q^m}[x]$ og antallet af nulløsninger til et $(L+1)$-variat lineariseret polynomium over denne delring fastsættes. Inden delringen betragtes indføres en notation for at tage kompositionen af et lineariseret polynomium $f(x)$ med sig selv i gange.

Definition 8.2. Lad $f(x)$ være et lineariseret polynomium og $i \in \mathbb{N}$, da betegnes kompositionen af $f(x)$ med sig selv i gange ved

$$f^{\circ i}(x) = \underbrace{f(f(\cdots f(x)\cdots))}_{i} \ .$$

I tilfælde $i = 0$ defineres $f^{\circ 0}(x) = x$.

Ringen af lineariserede polynomier $\mathscr{L}_{q^m}[x]$ præsenteret i kapitel 5 er ikke kommutativ og for et polynomium af formen

$$\sum_{i=0}^{L} Q_i \circ f^{\circ i}(x) = 0 \quad \text{hvor} \quad f(x) \in \mathscr{L}_{q^m}[x] \ , \tag{8.1}$$

kan der derfor eksistere mere end L lineariserede polynomier $f(x) \in \mathscr{L}_{q^m}[x]$ som opfylder ligning (8.1). Dette illustreres ved hjælp af følgende eksempel.

Eksempel 8.3. Vi betragter polynomiet

$$x^{q^2} - f^{\circ 2}(x) = 0 \ , \tag{8.2}$$

som er et lineariseret polynomium på formen givet i (8.1). Dette ses ved at lade $L = 2$, $Q_0(x) = x^{q^2}$, $Q_1(x) = 0$, $Q_2(x) = -x$ og lade $f^{\circ i} \in \mathscr{L}_{q^m}[x]$ for $i \in \{0, 1, 2\}$. Ligning (8.2) har herved løsninger $f(x) = ax^q$, hvorom der gælder at $a^{q+1} = 1$ i $\mathbb{F}_{q^m}$.

Der gælder at $x^{q^m} - x = 0$ er definerende polynomium for legemet $\mathbb{F}_{q^m}$, og dette har derfor q^m forskellige rødder i $\mathbb{F}_{q^m}$. Hvis der ses bort fra nulløsningen fås polynomiet

$$x^{q^m-1} - 1 = 0 \ , \tag{8.3}$$

som så har $q^m - 1$ forskellige rødder i $\mathbb{F}_{q^m}$. Hvis m er lige så gælder der, at

$$\frac{q^m - 1}{q + 1} = q^{m-1} - q^{m-2} + q^{m-3} - \cdots + q - 1 \ ,$$

altså $(q + 1)|(q^m - 1)$, og heraf fås at $(x^{q+1} - 1)|(x^{q^m-1} - 1)$. Da (8.3) kan faktoriseres til

$$\prod_{\alpha \in \mathbb{F}_{q^m} \setminus \{0\}} (x - \alpha) \ ,$$

gælder der for m lige, at $x^{q+1} - 1 = (x - \alpha_1) \cdots (x - \alpha_{q+1})$ hvor $\alpha_1, \ldots, \alpha_{q+1} \in \mathbb{F}_{q^m}$. Derfor haves $q + 1$ forskellige løsninger for $x \in \mathbb{F}_{q^m}$ til $x^{q+1} - 1 = 0$.

Erstattes x i ovenstående med a fås således at der er $q + 1$ løsninger til (8.2), når m er lige, og da $q \geq 2$ fås at der er flere løsninger for $f(x) \in \mathscr{L}_{q^m}[x]$ end $L = 2$. ▲

Da der kan findes mere end L løsninger for $f(x) \in \mathscr{L}_{q^m}[x]$, der opfylder (8.1), ønsker vi at bestemme en kommutativ delring af $\mathscr{L}_{q^m}[x]$, hvor der vil eksistere maksimalt L løsninger til (8.1). Dette vises i sætning 8.5. Først gives et lemma, som fortæller hvornår to lineariserede polynomier kommuterer.

Lemma 8.4. *Lad $f(x)$ og $g(x)$ være lineariserede polynomier over legemet $\mathbb{F}_q$, så kommuterer de, dvs.*

$$f(x) \circ g(x) = f(x) \circ g(x) \ .$$

[MV12, Lemma 1]

Bevis. Lad $f(x) = \sum_{i=0}^{d_1} a_i x^i$ og $g(x) = \sum_{j=0}^{d_2} b_j x^j$, hvor $a_i, b_j \in \mathbb{F}_q$. Ved brug af ligning (5.4) fås

$$f(x) \circ g(x) = \sum_{k=0}^{d_1+d_2} c_k x^{q^k} \ , \text{ hvor } c_k = \sum_{i=0}^{k} a_i b_{k-i}^{q^i} \ ,$$

og

$$g(x) \circ f(x) = \sum_{k=0}^{d_1+d_2} \tilde{c}_k x^{q^k} \ , \text{ hvor } \tilde{c}_k = \sum_{i=0}^{k} a_i^{q^{k-i}} b_{k-i} \ .$$

Idet $a_i, b_j \in \mathbb{F}_q$ haves, at $a_i^{q^{k-i}} = a_i$ og $b_{k-i}^{q^i} = b_{k-i}$ for alle i, j og k. For ethvert k følger, at

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}^{q^i} = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k} a_i^{q^{k-i}} b_{k-i} = \tilde{c}_k \ .$$

Der gælder derfor at $f(x)$ og $g(x)$ kommuterer, altså $f(x) \circ g(x) = g(x) \circ f(x)$. □

De lineariserede polynomier over legemet $\mathbb{F}_q$ kan samles i mængden $\mathscr{L}_q[x]$, som sammen med de binære operationer $+$ og $\circ$ giver en kommutativ ring ved brug af sætning 5.3 og lemma 8.4.

Sætning 8.5. *Lad Q_i for $0 \in \{1, \ldots, L\}$ være lineariserede polynomier over $\mathbb{F}_{q^m}$, hvor mindst et Q_i er ikke-nul. Da har*

$$\sum_{i=0}^{L} Q_i \circ f^{\circ i}(x) = 0 \tag{8.4}$$

højest L løsninger for $f(x)$ i $\mathscr{L}_q[x]$. [MV12, Theorem 2]

Bevis. Der laves induktion efter L for $L \geq 0$.

Basisskridt: For $L = 0$ haves ligningen $Q_0 \circ f^{\circ 0}(x) = Q_0 \circ x$, og der må derfor gælde at Q_0 er ikke-nul. Der eksisterer derfor ingen $f(x)$ i $\mathscr{L}_q[x]$ således at (8.4) er opfyldt.

Induktionsantagelse: Antag at sætningen er opfyldt for $L - 1$.

Induktionsskridt: Antag, at $L \geq 1$. Hvis der ikke findes $f(x) \in \mathscr{L}_q[x]$ som opfylder (8.4) haves, at sætningen er opfyldt, da $L > 0$.

Antag der eksisterer en løsning $f_0(x) \in \mathscr{L}_q[x]$ til (8.4), hvilket giver at

$$\sum_{i=0}^{L} Q_i \circ f_0^{\circ i}(x) = 0. \tag{8.5}$$

Det skal så vises at der højest er $L - 1$ løsninger i $\mathscr{L}_q[x]$ til (8.4) hvis der ses bort fra $f_0(x)$. Antag at $f(x) \in \mathscr{L}_q[x]$ og $f(x) \neq f_0(x)$. Ved at trække (8.5) fra (8.4) fås

$$\sum_{i=1}^{L} Q_i \circ (f^{\circ i}(x) - f_0^{\circ i}(x)) = 0\ . \tag{8.6}$$

Summen starter her med $i = 1$ da $f^{\circ 0}(x) = x = f_0^{\circ 0}(x)$. Da løsningerne ønskes fundet i $\mathscr{L}_q[x]$ gælder der af lemma 8.4 at $f(x)$ og $f_0(x)$ kommuterer. Heraf fås for $i \geq 1$ at

$$\begin{aligned} & \left(\sum_{j=0}^{i-1} f_0^{\circ i-j-1}(x) \circ f^{\circ j}(x) \right) \circ (f(x) - f_0(x)) \qquad (8.7) \\ = & \sum_{j=0}^{i-1} f_0^{\circ i-j-1}(x) \circ f^{\circ j+1}(x) - \sum_{j=0}^{i-1} f_0^{\circ i-j}(x) \circ f^{\circ j}(x) \\ = & \ f^{\circ i}(x) - f_0^{\circ i}(x)\ . \end{aligned}$$

Ved at sætte (8.7) ind i (8.6) fås

$$\begin{aligned} & \sum_{i=1}^{L} Q_i \circ \left(\sum_{j=0}^{i-1} \left(f_0^{\circ i-j-1}(x) \circ f^{\circ j}(x) \right) \circ (f(x) - f_0(x)) \right) \\ = & \left(\sum_{i=1}^{L} Q_i \circ \sum_{j=0}^{i-1} f_0^{\circ i-j-1}(x) \circ f^{\circ j}(x) \right) \circ (f(x) - f_0(x)) = 0\ , \qquad (8.8) \end{aligned}$$

da ringen af lineariserede polynomier er associativ. Da der gælder, at $f - f_0 \neq 0$ kan der divideres med dette på begge sider af (8.8), og der fås

$$\begin{aligned} & \sum_{i=1}^{L} Q_i \circ \sum_{j=0}^{i-1} f_0^{\circ i-j-1}(x) \circ f^{\circ j}(x) \\ = & \sum_{j=0}^{L-1} \left(\sum_{i=j+1}^{L} Q_i \circ f_0^{\circ i-j-1}(x) \right) \circ f^{\circ j}(x) = 0\ . \qquad (8.9) \end{aligned}$$

Per induktionsantagelse gælder der, at (8.9) højest har $L-1$ løsninger for $f(x)$ i $\mathscr{L}_q[x]$, og heraf haves sammen med $f_0(x)$ højest L løsninger til (8.4). □

Følgende eksempel er en fortsættelse på eksempel 8.3, som illustrerer at når vi betragter løsninger i $\mathscr{L}_q[x]$ eksisterer der maksimalt L løsninger.

Eksempel 8.6 (Fortsættelse af eksempel 8.3)**.** Betragt ligningen givet i (8.2), vi ønsker at bestemme løsninger i $\mathscr{L}_q[x]$ istedet for i $\mathscr{L}_{q^m}[x]$. Der gælder stadig at løsningerne er på formen $f(x) = ax^{q^2}$, hvor der skal gælde at $a^{q+1} = 1$, men da der arbejdes over legemet $\mathbb{F}_q$ fås, at $a^{q+1} = a^q \cdot a = a \cdot a = a^2$. Altså er det ligningen $a^2 = 1$ der skal bestemmes løsninger til over $\mathbb{F}_q$, og der gælder at denne maksimalt kan have 2 løsninger. Det vil sige at der højest er $L = 2$ løsninger $f(x)$ til (8.2) over $\mathscr{L}_q[x]$. ▲

8.2 Konstruktion af Multivariat Lineariseret Polynomium

Det multivariate lineariserede polynomium $Q(x, y_1, \ldots, y_L)$ skal benyttes ved liste-L-dekodening. I dette afsnit præsenteres to forskellige metoder til at konstruere Q. Først konstrueres Q ved hjælp af en interpolationsalgoritme og efterfølgende ved løsning af ligningssystemer.

8.2.1 Interpolationsalgoritme

I dette afsnit præsenteres en algoritme fra [XYS11], som konstruerer et multivariat lineariseret polynomium $Q(x, y_1, \ldots, y_L) \in \mathscr{L}_{q^m}[x, y_1, \ldots, y_L]$. Algoritme 3 fra afsnit 5.2 er et special tilfælde af denne algoritme. Algoritmen i [XYS11] er beskrevet i et generelt setup, hvor den algebraiske struktur er et vilkårligt frit modul. Beskrivelsen som følger i dette afsnit er en oversættelse til tilfældet, hvor den algebraiske struktur er ringen af lineariserede polynomier.

Bemærkning 8.7. Vi veksler mellem at lade det $(L+1)$-variate lineariserede polynomium Q være indeholdt i $\mathscr{L}_{q^m}[x, y_1, \ldots, y_L]$ eller $\mathscr{L}_{q^m}[x_0, x_1, \ldots, x_L]$. Årsagen er at vi gerne vil konstruere et $(L+1)$-variat lineariseret polynomium, som afhænger af variablene $x, y_1, \ldots, y_L$. Dog har vi til tider brug for at have kendskab til hvilken orden monomierne i Q optræder i, og i dette tilfælde simplificerer det notationen, hvis Q afhænger af variablene $x_0, x_1, \ldots, x_L$.

Lad

$$\mathcal{P} = \Big\{(x_1, y_{1,1}, \ldots, y_{1,L}), (x_2, y_{2,1}, \ldots, y_{2,L}), \ldots, (x_{|\mathcal{P}|}, y_{|\mathcal{P}|,1}, \ldots, y_{|\mathcal{P}|,L})\Big\}$$

være en mængde af punkter indeholdt i $\mathbb{F}_{q^m}^{L+1}$ kaldet interpolationspunkter. Så ønskes det at konstruere $Q(x, y_1, \ldots, y_L)$, således at

$$Q(x_i, y_{i,1}, \ldots, y_{i,L}) = 0 \text{ for alle } i \in \{1, \ldots, |\mathcal{P}|\} \,. \tag{8.10}$$

Når Q er konstrueret over en mængde af interpolationspunkter således at (8.10) er opfyldt, kaldes Q for et interpolationspolynomium. Graden af et $(L+1)$-variat lineariseret polynomium defineres til følgende.

Definition 8.8 ($(k-1)L$-vægtet grad)**.** Lad et $(L+1)$-variat lineariseret polynomium $Q(x_0, x_1, \ldots, x_L) = Q_0(x_0) + Q_1(x_1) + \ldots + Q_L(x_L)$ være givet, hvor $Q_i(x_i)$ har grad $q^{d_i(Q)}$ for $i \in \{0, \ldots, L\}$. Den $(k-1)L$-vægtet grad af Q er defineret ved

$$\deg_{(k-1)L}(Q) = \max\{d_0(Q), k-1+d_1(Q), \ldots, (k-1)L + d_L(Q)\} \,.$$

I den efterfølgende algoritme har vi brug for at bestemme det polynomium som er minimalt under en ordning. Følgende defineres derfor først en ordning på monomierne i et $(L+1)$-variat lineariseret polynomium og efterfølgende en orden på $(L+1)$-variate lineariserede polynomier.

Definition 8.9 (Total orden på monomier)**.** Lad $x_j^{q^a}$ og $x_h^{q^b}$ være givet. Hvis $\deg_{(k-1)L}(x_j^{q^a}) < \deg_{(k-1)L}(x_h^{q^b})$ så siges $x_j^{q^a} < x_h^{q^b}$. I tilfælde hvor

$$\deg_{(k-1)L}(x_j^{q^a}) = \deg_{(k-1)L}(x_h^{q^b}) \tag{8.11}$$

og $j < h$ defineres at $x_j^{q^a} < x_h^{q^b}$. Hvis $j = h$ i (8.11) er der tale om samme monomium og heraf er $x_j^{q^a} = x_h^{q^b}$.

Eksempel 8.10. Lad $Q(x_0, x_1, x_2) = x_0^{q^3} + x_0^{q^0} + x_2^q \in \mathscr{L}_{q^5}^5$ være givet. Vi ønsker at bestemme det ledende monomium i Q for $k = 2$. Fra definition 8.9 fås at

$$\deg_{(k-1)L}(x_0^{q^0}) = 0, \quad \deg_{(k-1)L}(x_0^{q^3}) = 3 \quad \text{og} \quad \deg_{(k-1)L}(x_2^q) = 3 \,.$$

Monomierne $x_0^{q^3}$ og x_2^q har samme $(k-1)L$-vægtet grad, men da $0 < 2$ følger af definitionen at $x_0^{q^3} < x_2^q$. Monomierne i Q kan derfor ordnes $x_0^{q^0} < x_0^{q^3} < x_2^q$ og heraf ses at $\mathrm{LM}(Q) = x_2^q$. ▲

Vi udvider fra monomier til at betragte $(L+1)$-variate lineariserede polynomier. Lad f, g være to $(L+1)$-variate lineariserede polynomier og antag at $\deg_{(k-1)L}(f) = \deg_{(k-1)L}(g)$. Der gælder så at

$$\begin{aligned} & \max\{d_0(f), k-1+d_1(f), (k-1)2+d_2(f), \ldots, (k-1)L+d_L(f)\} \\ = \; & \max\{d_0(g), k-1+d_1(g), (k-1)2+d_2(g), \ldots, (k-1)L+d_L(g)\} \,, \end{aligned}$$

hvorfor der findes $i, j \in \{0, \ldots, L\}$ således at $(k-1)i+d_i(f) = (k-1)j+d_j(g)$. Dette kan omskrives til $d_i(f) = d_j(g) + (k-1)(j-i)$. Antag uden tab af generalitet at $i < j$ så giver definition 8.9 at

$$x_i^{q^{d_i(f)}} = x_i^{q^{d_j(g)+(k-1)(j-i)}} < x_j^{q^{d_j(g)}} \,,$$

så $\mathrm{LM}(f) < \mathrm{LM}(g)$. Her er det muligt at ordne f og g på trods af lighed i den $(k-1)L$-vægtet grad. Hvis $i = j$ så har f og g samme ledende monomium og i dette tilfælde er det ikke muligt at sammenligne de to $(L+1)$-variate lineariserede polynomier.

Ovenstående giver anledning til en orden på $(L+1)$-variate lineariserede polynomier.

Definition 8.11 (Orden på $(L+1)$-variate lineariserede polynomier)**.** Lad $f(x_0, x_1, \ldots, x_L)$ og $g(x_0, x_1, \ldots, x_L)$ være $(L+1)$-variate lineariserede polynomier. Hvis $\deg_{(k-1)L}(f) < \deg_{(k-1)L}(g)$ så gælder at

$$f(x_0, x_1, \ldots, x_L) \prec g(x_0, x_1, \ldots, x_L) \,. \tag{8.12}$$

I tilfælde hvor $\deg_{(k-1)L}(f) = \deg_{(k-1)L}(g)$ men $\mathrm{LM}(f) < \mathrm{LM}(g)$ gælder (8.12). Såfremt $\mathrm{LM}(f) = \mathrm{LM}(g)$ siges f og g at være ikke-sammenlignelige.

Det følgende lemma vedrørende ikke-sammenlignelige $(L+1)$-variate lineariserede polynomier er tilsvarende lemma 5.13 fra afsnit 5.2.

Lemma 8.12. *Antag at $f(\cdot)$ og $g(\cdot)$ er to ikke-sammenlignelige $(L+1)$-variate lineariserede polynomier under orden $\prec$. For et passende valgt $\gamma \in \mathbb{F}_{q^m}$ kan da konstrueres en linear kombination $h(\cdot) = f(\cdot) + \gamma g(\cdot)$, hvorom det gælder at $h(\cdot) \prec f(\cdot)$ og $h(\cdot) \prec g(\cdot)$.*

Tilsvarende algoritme 3 er idéen bag algoritme 4 iterativt at konstruere $L+1$ forskellige $(L+1)$-variate lineariserede polynomier, som alle opfylder (8.10), for til sidst at udvælge det polynomium, som er mindst under den fastsatte orden. For at kunne konstruere et $(L+1)$-variat lineariseret polynomium har vi brug for løbende at evaluere de konstruerede polynomier i interpolationspunkterne. Til dette defineres en mængde af funktionaler D_i for $i \in \{1, \ldots, |\mathcal{P}|\}$, som tager et $(L+1)$-variat lineariseret polynomium som input og givet et output i $\mathbb{F}_{q^m}$.

8.2. KONSTRUKTION AF MULTIVARIAT LINEARISERET POLYNOMIUM

Definition 8.13. Lad $Q(x, y_1, \ldots, y_L)$ være et $(L+1)$-variat lineariseret polynomium og lad $(x_i, y_{i,1}, \ldots, y_{i,L}) \in \mathbb{F}_{q^m}^{L+1}$. Da er funktionalen D_i defineret ved

$$D_i(Q) = Q(x_i, y_{i,1}, \ldots, y_{i,L}) = Q_0(x_i) + Q_1(y_{i,1}) + \ldots + Q_L(y_{i,L}) \, .$$

For hver funktionale D_i antag at K_i er kernen af D_i. Det vil sige at K_i indeholder alle de $(L+1)$-variate lineariserede polynomier, som evaluerer til nul i punktet $(x_i, y_{i,1}, \ldots, y_{i,L}) \in \mathbb{F}_{q^m}^{L+1}$. Definer $\overline{K}_i = K_1 \cap K_2 \cap \cdots \cap K_i$, så ønsker vi med algoritme 4 at bestemme det interpolationspolynomium $Q \in \overline{K}_{|\mathcal{P}|}$, som er minimalt under orden $\prec$.

Lemma 8.14. *En funktion i $\overline{K}_{|\mathcal{P}|}$ som er minimal under orden $\prec$ er entydig op til en skalar. [XYS11, Lemma 1]*

Bevis. Antag at både f og g er minimale i $\overline{K}_{|\mathcal{P}|}$. Så må de have samme ledende monomium, hvorved de er ikke-sammenlignelige. Fra lemma 8.12 følger så, at der findes et $(L+1)$-variat lineariseret polynomium $h = f + \gamma g$, som opfylder, at $h \prec f$ samt $h \prec g$, og som desuden fra konstruktionen er minimalt i $\overline{K}_{|\mathcal{P}|}$. Men dette er i modstrid med antagelsen om, at f og g er minimale i $\overline{K}_{|\mathcal{P}|}$. Heraf må $h = 0$, og derfor er f og g ens op til en skalar. □

Udover at vide om et givent $(L+1)$-variat lineariseret polynomium $Q(x_0, x_1, \ldots, x_L)$ er minimalt under orden $\prec$, er vi også interesseret i at have kendskab til hvilken variabel, der indgår i det ledende monomium i Q, når Q er minimal. Lad $L(x) \in \mathscr{L}_{q^m}[x]$ så defineres funktionen $\mathrm{ind}(\cdot)$ i dette afsnit ved $\mathrm{ind}(L(x) \circ x_j) = j$ og $\mathrm{ind}(Q) = \mathrm{ind}(\mathrm{LM}(Q))$. Funktionen, $\mathrm{ind}(\cdot)$, indikere altså hvilken variabel som indgår i det ledende monomium i Q.

Desuden defineres mængden $S_j = \{Q \in \mathscr{L}_{q^m}[x_0, x_1, \ldots, x_L] \mid \mathrm{ind}(Q) = j\}$. Mængden S_j består altså af alle de $(L+1)$-variate lineariserede polynomier hvis ledende monomium er i variablen x_j.

I algoritme 4 benyttes notationen j^* til at indikere hvilket polynomium blandt en mængde af polynomier, som er minimalt under ordenen på $(L+1)$-variate lineariserede polynomier. Lad $h_{i,0}, h_{i,1}, \ldots, h_{i,n}$ være forskellige $(L+1)$-variate lineariserede polynomier, hvor $n \leq L$. Vi ønsker så at bestemme det $j \in \{0, \ldots, n\}$, som opfylder at $h_{i,j} \prec h_{i,g}$ for alle $g \neq j$, hvor $g \in \{0, \ldots, n\}$. Heraf notationen

$$j^* := \{j \in H \mid h_{i,j} \prec h_{i,g} \text{ for } g \neq j \text{ hvor } g \in H\} \, ,$$

hvor $H \subseteq \{0, 1, \ldots, L\}$.

Algoritme 4 Konstruktion af et $(L+1)$-variat lineariseret polynomium; **Lvar**(B).

Input: Interpolationspunkter $\mathcal{P} = \{ (x_1, y_{1,1}, \ldots, y_{1,L}), \ldots, (x_{|\mathcal{P}|}, y_{|\mathcal{P}|,1}, \ldots, y_{|\mathcal{P}|,L}) \} \in W$.
$h_{0,0} = x$;
for $j = 1, \ldots, L$ **do**
    $h_{0,j} = y_j$;
end for
for $i = 0, \ldots, |\mathcal{P}| - 1$ **do**
    for $j = 0, \ldots, L$ **do**
        $h_{i+1,j} := h_{i,j}$;
        $\Delta_{i+1,j} := D_{i+1}(h_{i,j})$;
    end for
    $H := \{j | \Delta_{i+1,j} \neq 0\}$;
    if $H \neq \emptyset$ **then**
        $j^* := \{j \in H | h_{i,j} \prec h_{i,g}$ for $g \neq j$ hvor $g \in H\}$;
        for $j \in H$ **do**
            if $j \neq j^*$ **then**
                $h_{i+1,j} := \Delta_{i+1,j^*} h_{i,j} - \Delta_{i+1,j} h_{i,j^*}$;
            else if $j = j^*$ **then**
                $h_{i+1,j} := \Delta_{i+1,j}(h_{i,j})^q - D_{i+1}((h_{i,j})^q) h_{i,j}$;
            end if
        end for
    end if
end for
$Q := \{h_{|P|,j} \mid h_{|P|,j} \prec h_{|P|,g}$ for $g \neq j$ hvor $g \in \{0, \ldots, L\}\}$;
Output: Et $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L) = Q_0(x) + Q_1(y_1) + \ldots + Q_L(y_L)$.

Til at bevise at output af algoritme 4 altid er et $Q \in \overline{K}_{|\mathcal{P}|}$, som er minimalt under orden $\prec$, defineres følgende for hvert iterativt skridt $i \in \{1, \ldots, |\mathcal{P}|\}$;

$$\begin{aligned} T_{i,j} &:= \overline{K}_i \cap S_j \quad \text{og} \\ h_{i,j} &:= \min_{h \in T_{i,j}} \{h\} \, , \end{aligned} \tag{8.13}$$

hvor minimum i (8.13) refererer til orden på de $(L+1)$-variate lineariserede polynomier. Desuden defineres $T_{0,j} := \mathscr{L}_{q^m}[\cdot] \cap S_j$. Som nævnt tidligere konstruerer algoritme 4 sideløbende $L+1$ forskellige $(L+1)$-variate lineariserede polynomier. Vi ønsker at vise at disse polynomier specielt opfylder (8.13) for $j \in \{0, \ldots, L\}$, når tilfældet er at polynomiet $h_{i+1,j}$ altid konstrueres fra $h_{i,j}$ forudsat at en begyndelsesværdi for $h_{0,j}$ er givet.

Lemma 8.15. *For $i \in \{0, \ldots, |\mathcal{P}| - 1\}$ gælder at $h_{i+1,j}$ konstrueret i algoritme 4 er minimal under orden $\prec$ i $T_{i+1,j}$. [XYS11, Lemma 2]*

Bevis. Dette vises ved induktion efter i.

Basisskridt: Indledningsvist definerer algoritmen de lineariserede polynomier $h_{0,0} = x$ og $h_{0,j} = y_j$ for $j \in \{1, \ldots, L\}$. Der gælder for disse lineariserede polynomier at $h_{0,j}$ er minimal i S_j for $j \in \{0, \ldots, L\}$, da der ikke findes polynomier hvis ledende monomium er et monomium i variablen x eller y_j som har mindre grad. Heraf er $h_{0,j}$ minimal under $\prec$ i $T_{0,j}$.

Induktionsantagelse: Det antages at for $i \geq 0$ er $h_{i,j}$ minimal i $T_{i,j}$.

Induktionsskridt: Algoritme 4 kan konstruere polynomiet $h_{i+1,j}$ på tre forskellige måder ud fra $h_{i,j}$. Vi viser efterfølgende at i alle tre tilfælde er $h_{i+1,j}$ minimal i $T_{i+1,j}$ under induktionsantagelsen.

i. Hvis $h_{i,j} \in T_{i+1,j}$ så defineres $h_{i+1,j} := h_{i,j}$. Da $h_{i,j}$ er minimal i $T_{i,j}$ og da $T_{i+1,j} \subset T_{i,j}$ så er $h_{i+1,j}$ også minimal i $T_{i+1,j}$.

For alle de $j \in \{0, \ldots, L\}$ hvorom det gælder, at $h_{i,j} \notin T_{i+1,j}$, bestemmer algoritmen det polynomium, som er minimalt under orden $\prec$. Dette polynomium betegnes h_{i,j^*}.

ii. Hvis $h_{i,j} \neq h_{i,j^*}$ så defineres $h_{i+1,j} := D_{i+1}(h_{i,j^*})h_{i,j} - D_{i+1}(h_{i,j})h_{i,j^*}$. Denne konstruktion giver at $D_{i+1}(h_{i+1,j}) = 0$, hvorved $h_{i+1,j} \in K_{i+1}$. Da $h_{i,j^*} \prec h_{i,j}$ så er graden af $h_{i,j}$ bevaret således at $\text{ind}(h_{i+1,j}) = \text{ind}(h_{i,j})$, hvilket betyder at $h_{i+1,j} \in S_j$, hvorved $h_{i+1,j} \in T_{i+1,j}$. Desuden, da $h_{i,j}$ er minimal i $T_{i,j}$ er $h_{i+1,j}$ ligeledes minimal i $T_{i,j}$, og da $T_{i+1,j} \subset T_{i,j}$ så må $h_{i+1,j}$ også være minimal i $T_{i+1,j}$.

iii. Hvis $h_{i,j} = h_{i,j^*}$ så konstrueres h_{i+1,j^*} ved

$$h_{i+1,j^*} := D_{i+1}(h_{i,j^*})(h_{i,j^*})^q - D_{i+1}((h_{i,j^*})^q)h_{i,j^*} \ .$$

Denne konstruktion giver at $D_{i+1}(h_{i+1,j^*}) = 0$, så $h_{i+1,j^*} \in K_{i+1}$. Desuden, da $h_{i,j^*} \in \overline{K}_i$ så gælder at $(h_{i,j^*})^q \in \overline{K}_i$. Dette medfører at for $k < i$ er $D_k(h_{i+1,j^*}) = 0$, hvorfor $h_{i+1,j^*} \in \overline{K}_{i+1}$. Dette betyder yderligere at $h_{i+1,j^*} \in T_{i+1,j^*}$.

Det antages modsætningsvist at der findes et $f_{i+1,j^*} \in T_{i+1,j^*}$, som opfylder at

$$f_{i+1,j^*} \prec h_{i+1,j^*} \ . \tag{8.14}$$

Da $T_{i+1,j^*} \subset T_{i,j^*}$ så gælder at $f_{i+1,j^*} \in T_{i,j^*}$. Polynomiet h_{i,j^*} er minimal i T_{i,j^*}, så $\deg_{(k-1)L}(h_{i,j^*}) \leq \deg_{(k-1)L}(f_{i+1,j^*})$. Bemærk at $\mathrm{LM}(h_{i+1,j^*}) = \mathrm{LM}((h_{i,j^*})^q)$ så (8.14) giver at

$$\deg_{(k-1)L}(h_{i,j^*}) \leq \deg_{(k-1)L}(f_{i+1,j^*}) < \deg_{(k-1)L}((h_{i,j^*})^q) \ . \tag{8.15}$$

Den skarpe ulighed i (8.15) følger af at både f_{i+1,j^*} og $(h_{i,j^*})^q$ ligger i S_{j^*}, så de må have ledende monomium i samme variabel, men hvis $\mathrm{LM}(f_{i+1,j^*}) = \mathrm{LM}((h_{i,j^*})^q)$, så er de ikke-sammenlignelige, hvilket er en modstrid med (8.14). Desuden da $h_{i,j^*}, (h_{i,j^*})^q \in S_{j^*}$, så findes intet $f_{i+1,j^*} \in S_{j^*}$ som opfylder at

$$\deg_{(k-1)L}(h_{i,j^*}) < \deg_{(k-1)L}(f_{i+1,j^*}) < \deg_{(k-1)L}((h_{i,j^*})^q) \ .$$

Heraf er den eneste mulighed at $\mathrm{LM}(f_{i+1,j^*}) = \mathrm{LM}(h_{i,j^*})$. Fra lemma 8.12 følger så at der findes et polynomium $h = f_{i+1,j^*} + \gamma h_{i,j^*} \in T_{i,j^*}$, for $\gamma \in \mathbb{F}_{q^m}$, hvorom der gælder at $h \prec h_{i,j^*}$. Dette er en modstrid med at h_{i,j^*} er minimal i T_{i,j^*}. Heraf findes f_{i+1,j^*} ikke og h_{i+1,j^*} er minimal i T_{i+1,j^*}.

□

Sætning 8.16. *Det $(L+1)$-variate lineariserede polynomium $Q(x, y_1, \ldots, y_L)$ som er output af algoritme 4 med input $\mathcal{P}$ er minimal under orden $\prec$ i $\overline{K}_{|\mathcal{P}|}$.*

Bevis. Output af algoritme 4 er det polynomium som er minimal under $\prec$ i mængden $\{h_{|\mathcal{P}|,0}, h_{|\mathcal{P}|,1}, \ldots, h_{|\mathcal{P}|,L}\}$. Lad Q være dette polynomium. Fra lemma 8.15 gælder, at for hvert $j \in \{0, \ldots, L\}$ er $h_{|\mathcal{P}|,j}$ minimal i $T_{|\mathcal{P}|,j} = \overline{K}_{|\mathcal{P}|} \cap S_j$. Da alle $h_{|\mathcal{P}|,j}$ er indeholdt i $\overline{K}_{|\mathcal{P}|}$, og da Q er minimal blandt alle $h_{|\mathcal{P}|,j}$ må Q være indeholdt i $\overline{K}_{|\mathcal{P}|}$. Desuden, da $S_0 \cup S_1 \cup \cdots \cup S_L = \mathscr{L}_{q^m}[x, y_1, \ldots, y_L]$ så er $T_{|\mathcal{P}|,0} \cup T_{|\mathcal{P}|,1} \cup \cdots \cup T_{|\mathcal{P}|,L} = \overline{K}_{|\mathcal{P}|}$, og heraf må Q være minimal under $\prec$ i $\overline{K}_{|\mathcal{P}|}$. □

I det følgende eksempel illustreres algoritme 4.

Eksempel 8.17. Lad en mængde af interpolationspunkter være givet ved

$$\begin{aligned}\mathcal{P} &= \{(10000, 01010, 11100), (11010, 10110, 11000), (01100, 01110, 01000),\\ &\quad (00010, 00110, 10010), (00100, 10100, 11110)\} \subset \mathbb{F}_{2^5}^3 ,\end{aligned}$$

og antag at $k = 2$. Legemet $\mathbb{F}_{2^5}$ er, som i tidligere eksempler, konstrueret over det irreducible polynomium $x^5 + x^3 + 1 \in \mathbb{F}_2[x]$. Vi benytter interpolationspunkterne til at konstruere $Q(x, y_1, y_2)$.

Algoritme 4 definerer indledningsvist tre lineariserede polynomier, som hvert betragtes som et tre-variat lineariseret polynomium.

$$h_{0,0} := x; \quad h_{0,1} := y_1; \quad h_{0,2} := y_2;$$

For $i = 0$ betragtes det første interpolationspunkt; $\mathcal{P}_0 = (10000, 01010, 11100)$. Algoritmen definerer da

$$\begin{aligned} h_{1,0} &:= h_{0,0} = x; & \Delta_{1,0} &:= D_1(h_{0,0}) = \alpha^4;\\ h_{1,1} &:= h_{0,1} = y_1; & \Delta_{1,1} &:= D_1(h_{0,1}) = \alpha^3 + \alpha;\\ h_{1,2} &:= h_{0,2} = y_2; & \Delta_{1,2} &:= D_1(h_{0,2}) = \alpha^4 + \alpha^3 + \alpha^2; \end{aligned}$$

Da $\Delta_{1,0}, \Delta_{1,1}, \Delta_{1,2} \neq 0$ defineres $H = \{0, 1, 2\}$. Vi skal bestemme hvilket polynomium $h_{0,i}$ for $i \in H$, som er minimalt under ordningen $\prec$.

$$\begin{aligned} \deg_{(k-1)L}(h_{0,0}) &= \max\{0, 2-1-\infty, 4-2-\infty\} = 0;\\ \deg_{(k-1)L}(h_{0,1}) &= \max\{-\infty, 2-1+0, 4-2-\infty\} = 1;\\ \deg_{(k-1)L}(h_{0,2}) &= \max\{-\infty, 2-1-\infty, 4-2+0\} = 2; \end{aligned}$$

Heraf ses at $j^* = 0$. De tre polynomier redefineres følgende;

$$\begin{aligned} h_{1,0} &:= \alpha^4 x^q + D_1(x^q)x = \alpha^4 x^q + (\alpha^4 + \alpha^3 + \alpha)x;\\ h_{1,1} &:= \alpha^4 y_1 + (\alpha^3 + \alpha)x = (\alpha^3 + \alpha)x + \alpha^4 y_1;\\ h_{1,2} &:= \alpha^4 y_2 + (\alpha^4 + \alpha^3 + \alpha^2)x = (\alpha^4 + \alpha^3 + \alpha^2)x + \alpha^4 y_2; \end{aligned}$$

For $i = 1$ betragtes det andet interpolationspunkt; $\mathcal{P}_1 = (11010, 10110, 11000)$. Ovenstående procedure gentages.

$$\begin{aligned} h_{2,0} := h_{1,0} &= \alpha^4 x^q + (\alpha^4 + \alpha^3 + \alpha)x; & \Delta_{2,0} &:= D_2(h_{1,0}) = \alpha^4 + \alpha + 1;\\ h_{2,1} := h_{1,1} &= (\alpha^3 + \alpha)x + \alpha^4 y_1; & \Delta_{2,1} &:= D_2(h_{1,1}) = \alpha^4 + \alpha + 1;\\ h_{2,2} := h_{1,2} &= (\alpha^4 + \alpha^3 + \alpha^2)x + \alpha^4 y_2; & \Delta_{2,2} &:= D_2(h_{1,2}) = \alpha^4 + \alpha^2 + 1; \end{aligned}$$

Igen er $H = \{0, 1, 2\}$.

$$\begin{aligned}
\deg_{(k-1)L}(h_{1,0}) &= \max\{1, 2-1-\infty, 4-2-\infty\} = 1;\\
\deg_{(k-1)L}(h_{1,1}) &= \max\{0, 2-1+0, 4-2-\infty\} = 1;\\
\deg_{(k-1)L}(h_{1,2}) &= \max\{0, 2-1-\infty, 4-2+0\} = 2;
\end{aligned}$$

Det ses at $h_{1,0}$ og $h_{1,1}$ har samme $(k-1)L$-vægtet grad så det er nødvendigt at sammenligne de ledende monomier i $h_{1,0}$ og $h_{1,1}$ for at afgøre ordningen. Det ses at $\mathrm{LM}(h_{1,0}) = x^q$ og $\mathrm{LM}(h_{1,1}) = y_1$. Fra definition 8.9 haves så at $x^q < y_1$, da x er ordnet før y_1. Dette medfører at $h_{1,0} \prec h_{1,1}$ så $j^* = 0$. Redefineringen bliver,

$$\begin{aligned}
h_{2,0} &:= \alpha^{10}\alpha^8 x^{q^2} + \alpha^{10}\alpha^{16}x^q + D_2(\alpha^8 x^{q^2} + \alpha^{16}x^q)(\alpha^4 x^q + \alpha^8 x)\\
&= (\alpha^4 + \alpha^3 + 1)x^{q^2} + (\alpha^4 + \alpha^2 + \alpha + 1)x^q + (\alpha^2 + 1)x;\\
h_{2,1} &:= \alpha^{10}(\alpha^{29}x + \alpha^4 y_1) + \alpha^{10}(\alpha^4 x^q + \alpha^8 x)\\
&= (\alpha + 1)x^q + (\alpha + 1)x + (\alpha + 1)y_1;\\
h_{2,2} &:= \alpha^{10}(\alpha^{24}x + \alpha^4 y_2) + \alpha^{13}(\alpha^4 x^q + \alpha^8 x)\\
&= (\alpha^4 + \alpha^3)x^q + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)x + (\alpha + 1)y_2;
\end{aligned}$$

For $i = 2, 3, 4$ gentages det ovenstående igen. Afsluttede opnås at

$$\begin{aligned}
h_{5,0} &:= (\alpha^3 + \alpha^2 + \alpha)x^{q^5} + (\alpha^3 + \alpha + 1)x^{q^4} + (\alpha^3 + \alpha + 1)x^{q^3}\\
&\quad +(\alpha^3 + \alpha + 1)x^{q^2} + (\alpha^3 + \alpha + 1)x^q + (\alpha^2 + 1)x;\\
h_{5,1} &:= (\alpha + 1)x^q + (\alpha + 1)x + (\alpha + 1)y_1;\\
h_{5,2} &:= (\alpha^4 + \alpha^2 + \alpha + 1)x^{q^2} + (\alpha^4 + \alpha^2 + \alpha + 1)x + (\alpha^4 + \alpha^2 + \alpha + 1)y_2;
\end{aligned}$$

For at afgøre hvilket polynomium som bliver output af algoritmen undersøges den $(k-1)L$-vægtet grad,

$$\begin{aligned}
\deg_{(k-1)L}(h_{5,0}) &= \max\{5, 2-1-\infty, 4-2-\infty\} = 5;\\
\deg_{(k-1)L}(h_{5,1}) &= \max\{1, 2-1+0, 4-2-\infty\} = 1;\\
\deg_{(k-1)L}(h_{5,2}) &= \max\{2, 2-1-\infty, 4-2+0\} = 2;
\end{aligned}$$

Heraf ses at $h_{5,1}$ har mindst $(k-1)L$-vægtet grad, så

$$Q(x, y_1, y_2) = (\alpha + 1)x^q + (\alpha + 1)x + (\alpha + 1)y_1;$$

▲

Bemærkning 8.18. Fra lemma 8.14 følger at polynomiet $Q(x, y_1, y_2)$ konstrueret i ovenstående eksempel er entydigt op til en skalar. Heraf følger at polynomiet

$$Q(x, y_1, y_2) = x^q + x + y_1\ ,$$

også er minimalt under orden $\prec$ i $\overline{K}_{|\mathcal{P}|}$. I nogle tilfælde kunne en simplificering af Q være at foretrække og dette er heraf også muligt.

8.2.2 Løsning af Ligningssystem

Det multivariate lineariserede polynomium

$$Q(x, y_1, \ldots, y_L) = Q_0(x) + Q_1(y_1) + \cdots + Q_L(y_L)$$

kan også bestemmes ved at løse ligningssystemer. Dette skyldes, at koefficienterne i $Q(x, y_1, \ldots, y_L)$ skal bestemmes ud fra en mængde af interpolationspunkter $(x_j, y_{j,1}, \ldots, y_{j,L}) \in \mathcal{P}$ for $j \in \{0, 1, \ldots, |\mathcal{P}| - 1\}$, således at $Q(x_j, y_{j,1}, \ldots, y_{j,L}) = 0$. I det følgende gennemgår vi en metode til at bestemme Q ved hjælp af løsning af ligningssystemer.

Det antages at hvert Q_i for $i \in \{0, \ldots, L\}$ højest har grad $q^{m-i(k-1)-1}$, hvilket vil sige at Q højest har grad q^{m-1}. Således gælder der, at hvert Q_i højest har $m - i(k-1)$ koefficienter, $z_{i,0}, z_{i,1}, \ldots, z_{i,m-i(k-1)-1}$, som skal bestemmes, hvor $z_{i,l}$ hører til monomiet af grad q^l i Q_i. Heraf har Q højest

$$\sum_{i=0}^{L} m - i(k-1) = m(L+1) - (k-1)\frac{L(L+1)}{2} \tag{8.16}$$

koefficienter, $z_{0,0}, \ldots, z_{0,m-1}, z_{1,0}, \ldots, z_{L,m-L(k-1)-1}$. Her gælder der, at koefficienterne $z_{0,l}$ hører til monomier af typen x^{q^l} for $l \in \{0, \ldots, m-1\}$, mens koefficienter af typen $z_{i,l}$ for $i \in \{1, \ldots, L\}$ hører til monomier $y_i^{q^l}$ for $l \in \{0, \ldots, m - i(k-1) - 1\}$. Koefficienterne kan således ud fra deres tilhørende monomier opstilles i en orden ved at bruge ordningen givet i definition 8.9. Det vil sige der fås

$$z_{0,0} < z_{0,1} < \cdots < z_{L,m-L(k-1)-1} \ , \tag{8.17}$$

som en ordning af koefficienterne. Vi samler koefficienterne i en $1 \times (m(L+1) - (k-1)\frac{L(L+1)}{2})$ vektor i rækkefølgen givet i (8.17), således at første komponent i vektoren er $z_{0,0}$. Ved denne ordning af koefficienterne har vi senere lettere ved at bestemme et multivariat lineariseret polynomium af mindst mulig grad.

Interpolationspunkterne i $\mathcal{P}$ har længden $L+1$, og disse skal udvides til punkter af længden $m(L+1) - (k-1)\frac{L(L+1)}{2}$. Dette gøres ved at bestemme værdien af monomierne hørende til koefficienterne i (8.17), for hvert punkt $(x_j, y_{j,1}, \ldots, y_{j,L}) \in \mathcal{P}$, og samle disse i en $\left(m(L+1) - (k-1)\frac{L(L+1)}{2}\right) \times 1$ vektor. Altså for et punkt $(x_j, y_{j,1}, \ldots, y_{j,L}) \in \mathcal{P}$ fås

$$\mathbf{p}_j = \begin{bmatrix} x_j & x_j^q & \cdots & y_{j,L}^{q^{m-L(k-1)-1}} \end{bmatrix}^\top ,$$

hvor komponenterne er placeret, således at de passer med rækkefølgen af de tilhørende koefficienter i (8.17). De nye punkter $\mathbf{p}_j$ for $j \in \{0, \ldots, |\mathcal{P}| - 1\}$ samles i en $\left(m(L+1) - (k-1)\frac{L(L+1)}{2}\right) \times |\mathcal{P}|$ matrix;

$$\mathbf{P} = \begin{bmatrix} \mathbf{p}_0 & \mathbf{p}_1 & \cdots & \mathbf{p}_{|\mathcal{P}|-1} \end{bmatrix} .$$

Af ovenstående fås således et ligningssystem

$$\begin{bmatrix} z_{0,0} & z_{0,1} & \cdots & z_{L,m-L(k-1)-1} \end{bmatrix} \mathbf{P} = [0 \;\; 0 \;\; \cdots \;\; 0] ,$$

som omskrives til

$$\mathbf{P}^\top \begin{bmatrix} z_{0,0} & z_{0,1} & \cdots & z_{L,m-L(k-1)-1} \end{bmatrix}^\top = [0 \;\; 0 \;\; \cdots \;\; 0]^\top . \tag{8.18}$$

Ved at reducere $\mathbf{P}^\top$ kan en løsning for koefficienterne i Q bestemmes. Hvis der gælder, at $m(L+1)-(k-1)\frac{L(L+1)}{2} > |\mathcal{P}|$ fås desuden altid en ikke-triviel løsning og herved er Q ikke-nulpolynomiet. Når Q ikke er nulpolynomiet så kan den rækkereducerede af $\mathbf{P}^\top$ opskrives på parameterform, hvorfor koefficienterne til Q kan fastsættes.

Følgende eksempel illustrerer, hvorledes et multivariat lineariseret polynomium Q bestemmes ud fra en mængde af interpolationspunkter.

Eksempel 8.19. Lad $L = 2$, $q = 2$, $m = 5$, $k = 2$ og lad interpolationspunkterne være givet ved

$$\begin{aligned} \mathcal{P} \;=\; & \{(\alpha^4, \alpha^{29}, \alpha^{24}), (\alpha^8, \alpha^{27}, \alpha^{17}), (\alpha^{16}, \alpha^{23}, \alpha^3), (\alpha, \alpha^{15}, \alpha^6), (\alpha^2, \alpha^{30}, \alpha^{12}), \\ & (\alpha, \alpha^6, \alpha^7), (\alpha^2, \alpha^{12}, \alpha^{14}), (\alpha^4, \alpha^{24}, \alpha^{28}), (\alpha^8, \alpha^{17}, \alpha^{25}), (\alpha^{16}, \alpha^3, \alpha^{19})\} . \end{aligned}$$

Da $L = 2$ skal der bestemmes et 3-variat lineariseret polynomium $Q(x, y_1, y_2)$ og af (8.16) skal $5(2+1) - (2-1)\frac{2(2+1)}{2} = 12$ koefficienter bestemmes. Da $|\mathcal{P}| = 10 < 12$ fås, at der kan bestemmes en ikke-nulløsning til Q. Af (8.17) fås at ordningen på koefficienterne bliver

$$z_{0,0} < z_{0,1} < z_{1,0} < z_{0,2} < z_{1,1} < z_{2,0} < z_{0,3} < z_{1,2} < z_{2,1} < z_{0,4} < z_{1,3} < z_{2,2} . \tag{8.19}$$

Ud fra punkterne i $\mathcal{P}$ bestemmes de udvidede punkter af formen

$$\mathbf{p}_j = \begin{bmatrix} x_j & x_j^q & y_{j,1} & \cdots & y_{j,1}^{q^3} & y_{j,2}^{q^2} \end{bmatrix}^\top ,$$

hvor komponenterne er ordnet på tilsvarende måde som koefficienterne i

(8.19) for $j \in \{0, \ldots, 9\}$. Heraf fås

$$\mathbf{P}^\top = \left[\begin{array}{ccc|ccc|ccc|ccc} \alpha^4 & \alpha^8 & \alpha^{29} & \alpha^{16} & \alpha^{27} & \alpha^{24} & \alpha & \alpha^{23} & \alpha^{17} & \alpha^2 & \alpha^{15} & \alpha^3 \\ \alpha^8 & \alpha^{16} & \alpha^{27} & \alpha & \alpha^{23} & \alpha^{17} & \alpha^2 & \alpha^{15} & \alpha^3 & \alpha^4 & \alpha^{30} & \alpha^6 \\ \alpha^{16} & \alpha & \alpha^{23} & \alpha^2 & \alpha^{15} & \alpha^3 & \alpha^4 & \alpha^{30} & \alpha^6 & \alpha^8 & \alpha^{29} & \alpha^{12} \\ \alpha & \alpha^2 & \alpha^{15} & \alpha^4 & \alpha^{30} & \alpha^6 & \alpha^8 & \alpha^{29} & \alpha^{12} & \alpha^{16} & \alpha^{27} & \alpha^{24} \\ \alpha^2 & \alpha^4 & \alpha^{30} & \alpha^8 & \alpha^{29} & \alpha^{12} & \alpha^{16} & \alpha^{27} & \alpha^{24} & \alpha & \alpha^{23} & \alpha^{17} \\ \alpha & \alpha^2 & \alpha^6 & \alpha^4 & \alpha^{12} & \alpha^7 & \alpha^8 & \alpha^{24} & \alpha^{14} & \alpha^{16} & \alpha^{17} & \alpha^{28} \\ \alpha^2 & \alpha^4 & \alpha^{12} & \alpha^8 & \alpha^{24} & \alpha^{14} & \alpha^{16} & \alpha^{17} & \alpha^{28} & \alpha & \alpha^3 & \alpha^{25} \\ \alpha^4 & \alpha^8 & \alpha^{24} & \alpha^{16} & \alpha^{17} & \alpha^{28} & \alpha & \alpha^3 & \alpha^{25} & \alpha^2 & \alpha^6 & \alpha^{19} \\ \alpha^8 & \alpha^{16} & \alpha^{17} & \alpha & \alpha^3 & \alpha^{25} & \alpha^2 & \alpha^6 & \alpha^{19} & \alpha^4 & \alpha^{12} & \alpha^7 \\ \alpha^{16} & \alpha & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^{19} & \alpha^4 & \alpha^{12} & \alpha^7 & \alpha^8 & \alpha^{24} & \alpha^{14} \end{array}\right] .$$

De lodrette linjer indikere at koefficienterne er delt op efter hvilken $(k-1)L$-vægtet grad deres tilknyttede monomier har. Ved at reducere $\mathbf{P}^\top$ fås

$$\mathbf{P}^\top_{reduceret} = \left[\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] ,$$

og ved at omskrive dette til parameterform fås

$$\begin{bmatrix} z_{0,0} \\ z_{0,1} \\ z_{1,0} \\ z_{0,2} \\ z_{1,1} \\ z_{2,0} \\ z_{0,3} \\ z_{1,2} \\ z_{2,1} \\ z_{0,4} \\ z_{1,3} \\ z_{2,2} \end{bmatrix} = a \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + b \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + c \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} ,$$

hvor $z_{2,1} = a$, $z_{0,4} = b$ og $z_{2,2} = c$. Idet der ønskes et 3-variat lineariseret polynomium af mindst mulig grad sættes $b, c = 0$ og der fås

$$Q(x, y_1, y_2) = a y_1^{q^2} + a y_1 + a y_2^q + a y_2 , \tag{8.20}$$

hvor $a \in \mathbb{F}_{q^m}$. ▲

8.2.3 Kompleksitet af Algoritme versus Ligningssystem

Kompleksiteten af algoritme 4 er domineret af antallet af interpolationspunkter. I [XYS11] fastsætter de at kompleksiteten af algoritme 4 til at være $O(L^2m^2(t+\ell)\ell)$.

Ved Gauss elimination har koefficientmatricen størrelsen

$$|\mathcal{P}| \times \left(m(L+1) - (k-1)\frac{L(L+1)}{2}\right) .$$

Vi vil senere komme ind på at interpolationspunkterne er konstruereret fra et modtaget underrum U, hvis dimension er $r = \ell+t-\rho$, hvor ℓ er dimensionen af det afsendte kodeord, t er dimension det tilførte fejlrum og ρ er bestemt af sletningsoperatoren. Da $|\mathcal{P}| \leq m(\ell+t)$ fås at kompleksiteten af Gauss elimination er

$$O\left(m^2(\ell+t)^2\left(m(L+1) - (k-1)\frac{L(L+1)}{2}\right)\right) . \tag{8.21}$$

Bemærk at

$$L^2m^2(t+\ell)\ell \quad \text{er} \quad O(L^2m^2(t+\ell)^2(k-1)) .$$

Der gælder at $m-L(k-1)-1 \geq 0$, da graden af det lineariserede polynomium $Q_L(\cdot)$ ikke må være negativ. Heraf følger at

$$\begin{aligned} L^2(k-1) &\leq (L+1)(L(k-1)+1) \\ &\leq (L+1)(2L(k-1)+2-L(k-1)) \leq (L+1)(2m-L(k-1)) \\ &\leq 2(m(L+1) - \frac{(k-1)}{2}L(L+1)) , \end{aligned}$$

så $L^2m^2(t+\ell)^2(k-1)$ er $O\left(m^2(\ell+t)^2\left(m(L+1)-(k-1)\frac{L(L+1)}{2}\right)\right)$. Heraf gælder, at

$$L^2m^2(t+\ell)\ell \quad \text{er} \quad O\left(m^2(\ell+t)^2\left(m(L+1) - (k-1)\frac{L(L+1)}{2}\right)\right) .$$

Algoritme 4 er derfor mere effektiv til at bestemme det multivariate lineariserede polynomium end løsning af ligningssystemer. [XYS11]

8.3 Løsning af Ligninger over Ringen af Lineariserede Polynomier

Lad et bivariat lineariseret polynomium $Q(x,y)$ på formen

$$Q(x,y) = Q_0(x) + Q_1(x) \circ y + \cdots + Q_L(x) \circ y^{\circ L} , \tag{8.22}$$

være givet. Her er $Q_i(x)$ et lineariseret polynomium over $\mathbb{F}_{q^m}$ for $i \in \{0, \ldots, L\}$ og y er en variabel i ringen $\mathscr{L}_q[x]$. Vi præsenterer i det følgende en algoritme fra [MV12] som finder alle rødderne $y \in \mathscr{L}_q^k[x]$ i $Q(x, y)$ med grad højest q^{k-1}.

Bemærkning 8.20. Formen af $Q(x, y)$ i (8.22) kan betragtes som formen for et bivariat lineariseret polynomium, da de lineariserede polynomier Q_i for $i \in \{1, \ldots, L\}$ alle afhænger af variablen y. Den lineære egenskaben for lineariserede polynomier medfører at $y^{\circ i}$ er et nyt lineariseret polynomium, og heraf er $Q_i(y^{\circ i})$ igen et lineariseret polynomium, hvorved summen

$$Q_1(x) \circ y + \cdots + Q_L(x) \circ y^{\circ L}$$

også kan betrages som et lineariseret polynomium, der kun afhænger af variablen $y \in \mathscr{L}_q^k[x]$. Heraf kan $Q(x, y)$ i (8.22) omskrives til formen angivet i ligning (5.6).

I dette afsnit betyder formuleringen "et polynomium p er dividerbart med x^{q^s}", at der findes et andet polynomium p' som opfylder at $x^{q^s} \circ p' = (p')^{q^s} = p$. Divisionen er altså med hensyn til kompositionen $\circ$. Heraf siges $Q(x, y)$ at være dividerbart med x^{q^s}, hvis der for alle $i \in \{0, \ldots, L\}$ gælder at $Q_i(x)$ er dividerbart med x^{q^s}, altså $(Q_i'(x))^{q^s} = Q_i(x)$. Vi definerer da

$$Q_{\downarrow s}(x, y) = Q_0'(x) + Q_1'(x) \circ y + \cdots + Q_L'(x) \circ y^{\circ L} \ .$$

Hvis $Q(x, y)$ er givet på formen (8.22) og $Q(x, y)$ ikke er nulpolynomiet så kan algoritme 5 benyttes til at finde rødderne $y \in \mathscr{L}_q^k[x]$ i $Q(x, y)$. Som input kræves $Q(x, y) \neq 0$, det k som definerer hvilken ring rødderne ønskes fundet i, og et λ som indikerer hvor mange gange algoritmen allerede er gennemløbet rekursivt. Indledningsvist vælges derfor altid $\lambda = 0$.

I det følgende bevises at mængden $\mathcal{A}$ produceret af algoritme 5 består af alle rødder $y \in \mathscr{L}_q^k[x]$ i $Q(x, y)$. For hvert rekursivt gennemløb af algoritmen redefineres polynomierne $Q, Q_{\downarrow s}$ og H. Antag at det aktuelle kald af algoritmen er $\mathbf{LRR}(Q(x, y), k, \lambda)$. For $\lambda = i \in \{0, \ldots, k-1\}$ defineres

$$P_i(x, y) = Q(x, y); \quad T_i(x, y) = Q_{\downarrow s}(x, y); \quad H_i(x, \gamma) = H(x, \gamma); \quad (8.23)$$

Bemærk at ved første gennemløb af algoritmen er $P_0(x, y) = Q(x, y)$ per antagelse et ikke-nulpolynomium. Desuden, hvis P_i er ikke-nul så følger, at T_i er ikke-nul som medfører, at P_{i+1} er ikke-nul. Heraf er P_i og T_i ikke-nulpolynomier for $i \in \{0, \ldots, k-1\}$. Desuden giver dette faktum, at s i algoritme 5, som benyttes til konstruktion af $Q_{\downarrow s}$, altid er veldefineret når input med $\lambda = 0$ er $Q(x, y) \neq 0$.

Algoritme 5 Løsning af ligninger over ringen af lineariserede polynomier, $\mathbf{LRR}(Q(x,y),k,\lambda)$

Input: Et bivariat lineariseret polynomium $Q(x,y)$, $k \in \mathbb{N}$ samt $\lambda \in \mathbb{N} \cup \{0\}$.
if $\lambda = 0$ **then**
  $\mathcal{A} := \emptyset$;
end if
Definer s til det største heltal som opfylder at $Q(x,y)$ er dividerbart med x^{q^s}.
$H(x,\gamma) := \frac{1}{x} Q_{\downarrow s}(x, \gamma x)$;
$Z := \{\gamma \in \mathbb{F}_q | H(0,\gamma) = 0\}$;
for all $\gamma \in Z$ **do**
  $u_\lambda := \gamma$;
  if $\lambda < k-1$ **then**
    $\mathcal{A} := \mathcal{A} \cup \mathbf{LRR}(Q_{\downarrow s}(x, y^q + \gamma x), k, \lambda + 1)$;
  else if $Q(x, u_{k-1}x) = 0$ **then**
    $\mathcal{A} := \mathcal{A} \cup \{u_0 x^{q^0} + u_1 x^q + \cdots + u_{k-1} x^{q^{k-1}}\}$;
  end if
end for
Output: En mængde $\mathcal{A} \subseteq \mathscr{L}_q^k[x]$ bestående af lineariserede polynomier på formen $L(x) = \sum_{i=0}^{k-1} u_i x^{q^i}$.

Lemma 8.21. *Lad $\mathcal{A}$ være output af algoritme 5 med input $(Q(x,y), k, \lambda = 0)$. Da er ethvert element i $\mathcal{A}$ en rod i Q. [MV12, Lemma 17]*

Bevis. Lad

$$L(x) = u_0 x + u_1 x^q + \cdots + u_{k-1} x^{q^{k-1}} ,$$

være et element i $\mathcal{A}$. Definer $\phi_i(x)$ for $i \in \{0, \ldots, k-1\}$ ved

$$\phi_i(x) = u_i x + u_{i+1} x^q + \cdots + u_{k-1} x^{q^{k-i-1}} .$$

Da u_i'erne er elementer i $\mathbb{F}_q$ så gælder at $\phi_i = \phi_{i+1}^q + u_i x$. Vi ønsker at vise at ϕ_i er en rod i P_i ved hjælp af bagudgående induktion efter $i = k-1, k-2, \ldots, 0$. Hvis dette er tilfældet, så er $\phi_0 = L(x)$ rod i $P_0 = Q(x,y)$ og det ønskede er opnået.

Basisskridt: Lad $i = k-1$ så gælder at $\phi_{k-1} = u_{k-1}x$. Da $L(x)$ per antagelse er indeholdt i $\mathcal{A}$ og da $\lambda = k-1$ følger af **else if**-leddet sidst i algoritme 5 at $0 = Q(x, u_{k-1}x) = P_{k-1}(x, u_{k-1}x)$. Heraf er ϕ_{k-1} en rod i P_{k-1}.

Induktionsantagelse: Antag at ϕ_{i+1} er en rod i P_{i+1} for $i < k-1$.

Induktionsskridt: Vi ønsker at vise at ϕ_i er rod i P_i. Betragt

$$\begin{aligned} P_i(x,\phi_i) &= (T_i(x,\phi_i))^{q^s} \\ &= (T_i(x,\phi_{i+1}^q + u_i x))^{q^s} \ . \end{aligned}$$

Der gælder at $T_i(x,\phi_{i+1}^q + u_i x) = P_{i+1}(x,\phi_{i+1})$ så

$$P_i(x,\phi_i) = (P_{i+1}(x,\phi_{i+1}))^{q^s} = 0 \ ,$$

da $P_{i+1}(x,\phi_{i+1}) = 0$ per induktionsantagelse. Heraf er ϕ_i en rod i P_i. Samlet giver det ovenstående at ethvert element i $\mathcal{A}$ er en rod i $Q(x,y)$. □

Lemma 8.22. *Lad $Q(x,y)$ være givet på formen* (8.22)*, lad*

$$L(x) = f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} \ ,$$

og lad

$$H(x,\gamma) = \frac{1}{x} Q(x,\gamma x) \ .$$

Da er koefficienten hørende til x i $Q(x,L(x))$ lig med $H(0,f_0)$. [MV12, Lemma 16]

Bevis. Betragt $L^{\circ i}(x) = f_0(L^{\circ i-1}) + f_1(L^{\circ i-1})^q + \cdots + f_{k-1}(L^{\circ i-1})^{q^{k-1}}$. Der gælder at koefficienten hørende til x i $L^{\circ i}$ er lig f_0^i. Betragt desuden $Q(x,L(x)) = Q_0(x) + Q_1(x) \circ L(x) + \cdots + Q_L(x) \circ L^{\circ L}(x)$, så gælder at koefficienten hørende til x i $Q(x,L(x))$ er koefficienten hørende til x i

$$Q_0(x) + Q_1(f_0 x) + \cdots + Q_L(f_0^L x) \ .$$

Observer yderligere at

$$xH(x,f_0) = Q(x,f_0 x) = Q_0(x) + Q_1(f_0 x) + \cdots + Q_L(f_0^L x) \ .$$

Koefficienten hørende til x i $H(x,f_0)x$ er konstant leddet i $H(x,f_0)$, som præcist bestemmes ved $H(0,f_0)$. Heraf er koefficienten hørende til x i $Q(x,L(x))$ givet ved $H(0,f_0)$. □

Lemma 8.23. *Lad*

$$L(x) = f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} \in \mathscr{L}_q^k[x] \ ,$$

være en rod i $Q(x,y)$. Lad P_i, T_i og H_i være defineret som i (8.23)*. Der gælder for $i \in \{0,\ldots,k-1\}$ at*

i. Polynomiet ϕ_i defineret ved

$$\phi_i = f_i x + f_{i+1} x^q + \cdots + f_{k-1} x^{q^{k-i-1}} \ ,$$

er en rod i $P_i(x,y)$.

ii. $H_i(0, f_i) = 0$.

[MV12, Lemma 18]

Bevis. Fra definitionen af P_i og T_i gælder at $P_0 = Q(x, y)$,

$$P_i(x, y) = (T_i(x, y))^{q^{s_i}} \quad \text{og} \quad P_{i+1}(x, y) = T_i(x, y^q + f_i x) \ ,$$

hvor s_i er det største heltal som opfylder at $P_i(x, y)$ er dividerbart med $x^{q^{s_i}}$. Desuden er $H_i(x, \gamma) = \frac{1}{x} T_i(x, \gamma x)$. Vi viser følgende del *i.* ved induktion efter i.

Basisskridt: For $i = 0$ er $\phi_0 = L(x)$. Per antagelse er $L(x)$ en rod i $Q(x, y) = P_0$.

Induktionsantagelse: Antag at ϕ_i er en rod i $P_i(x, y)$ for $0 \leq i < k-1$.

Induktionsskridt: Bemærk at $\phi_i = \phi_{i+1}^q + f_i x$, så $y = \phi_{i+1}$ er en rod i $P_i(x, y^q + f_i x)$ per induktionsantagelse. Da T_i er defineret ud fra P_i følger at $y = \phi_{i+1}$ også er en rod i $T_i(x, y^q + f_i x) = P_{i+1}(x, y)$.

For at bevise del *ii.* observer at

$$P_i(x, \phi_i(x)) = T_i(x, \phi_i(x))^{q^{s_i}} = 0 \ ,$$

medfører at $T_i(x, \phi_i(x)) = 0$. Fra lemma 8.22 følger at koefficienten hørende til x i $T_i(x, \phi_i(x))$ er lig med $H(0, f_i)$. Da $T_i(x, \phi_i(x))$ er nulpolynomiet må $H(0, f_i) = 0$. □

Lemma 8.24. *Lad $\mathcal{A}$ være output af algoritme 5 med input $(Q(x, y), k, \lambda = 0)$. Da er enhver rod i Q indeholdt i $\mathcal{A}$. [MV12, Lemma 19]*

Bevis. Lad

$$L(x) = f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} \in \mathscr{L}_q^k[x] \ ,$$

være en rod i $Q(x, y)$. Vi ønsker at vise ved induktion efter i for $i \in \{0, \ldots, k-1\}$, at der findes en rekursiv følge i algoritme 5, hvor gennemløb i kalder **LRR** med parameterne (P_i, k, i).

Basisskridt: For $i = 0$ haves det indledende gennemløb af algoritme 5. Her er $P_0(x, y) = Q(x, y)$ så algoritmen kaldes med parameterne $(P_0(x, y), k, 0)$.

Induktionsantagelse: Antag at for $0 \leq i < k - 1$ haves gennemløbet **LRR**(P_i, k, i).

Induktionsskridt: Fra lemma 8.23 er $H_i(0, f_i) = 0$ så $\gamma = f_i$ er en af rødderne i $P_i(x, y)$. Da $i < k - 1$ per induktionsantagelse så fås ved det næste rekursive kald med $\gamma = f_i$ og $\lambda = i$ at

$$(T_i(x, y^q + f_i x), k, \lambda + 1) = (P_{i+1}(x, y), k, i + 1)$$

Heraf er det ønskede vist.

Når den rekursive følge når til det gennemløb hvor $i = k - 1$ så følger af lemma 8.23, at $P_{k-1}(x, f_i x) = 0$ og så tilføjes $L(x)$ til mængden $\mathcal{A}$. □

Sætning 8.25. *Lad $Q(x, y)$ være et bivariat lineariseret polynomium på formen (8.22). Hvis $(Q(x, y), k, \lambda = 0)$ er input i Algoritme 5, så producerer algoritmen en mængde $\mathcal{A}$ bestående af alle rødder i Q indeholdt i $\mathscr{L}_q^k[x]$. [MV12, Theorem 20]*

Bevis. Fra lemma 8.21 fås at ethvert elementer i $\mathcal{A}$ er en rod i Q. Lemma 8.24 giver at enhver rod i Q er indeholdt i $\mathcal{A}$. Heraf består $\mathcal{A}$ af alle rødder i Q. □

Eksempel 8.26. I afsnit 8.2.1, eksempel 8.17 blev det tre-variate lineariserede polynomium $Q(x, y_1, y_2) = (\alpha+1)x^q+(\alpha+1)x+(\alpha+1)y_1$ konstrueret ud fra en mængde af interpolationspunkter $\mathcal{P}$. Ved at omforme dette polynomium til et bivariat lineariseret polynomium kan vi benytte algoritme 5 til at finde nulpunkter i $\mathscr{L}_q^k[x]$.

Lad $y_1 = y^{\circ 1}$ og $y_2 = y^{\circ 2}$. Så fås at

$$Q(x, y_1, y_2) = Q(x, y) = (\alpha + 1)x^q + (\alpha + 1)x + (\alpha + 1)x \circ y \ .$$

Input i algoritme 5 bliver så $Q(x, y) = (\alpha+1)x^q+(\alpha+1)x+(\alpha+1)x\circ y$, $k = 2$ og $\lambda = 0$. Da λ altid bør defineres til nul ved første gennemløb af algoritmen konstrueres først en tom mængde $\mathcal{A}$ hvori de fundne beskedpolynomier løbende placeres. Da graden af $Q_1(x)$ er q^0 defineres $s = 0$ indledningsvist, således at $Q_{\downarrow 0}(x, y) = (\alpha+1)x^q+(\alpha+1)x+(\alpha+1)x\circ y$. Polynomiet $H(x, \gamma)$ bliver så

$$H(x, \gamma) := (\alpha + 1)x^{q-1} + (\alpha + 1) + (\alpha + 1)\gamma \ ,$$

hvorved $H(0, \gamma) = (\alpha + 1) + (\alpha + 1)\gamma$. Her er $\gamma = 1$ en rod i $\mathbb{F}_2$ så $Z = \{1\}$ og $u_0 = 1$. Da $\lambda = 0 < k - 1 = 1$ så gennemløbes algoritmen igen, denne gang med

$$\begin{aligned} Q(x, y^q + \gamma x) &= (\alpha + 1)x^q + (\alpha + 1)x + ((\alpha + 1)x) \circ (y^q + \gamma x) \\ &= (\alpha + 1)x^q + (\alpha + 1)x^q \circ y \quad =: \tilde{Q}(x, y) \ , \end{aligned}$$

$k = 2$ og $\lambda = 1$. Da både $\tilde{Q}_0$ og $\tilde{Q}_1$ har grad q vælge $s = 1$, hvorved

$$\tilde{Q}_{\downarrow 1}(x, y) = (\alpha + 1)x + (\alpha + 1)x \circ y \ .$$

Så bliver

$$H(x,\gamma) := (\alpha+1) + (\alpha+1)\gamma \ ,$$

hvor $\gamma = 1$ er rod i $H(0,\gamma)$. Endnu en gang defineres $Z = \{1\}$ og $u_1 = 1$. Da $\lambda = 1 = k-1$ så undersøges hvorvidt $\tilde{Q}(x, u_1 x) = 0$. Dette er tilfældet da $\tilde{Q}(x, u_1 x) = (\alpha+1)x^q + (\alpha+1)x^q = 0$. Output af algoritmen bliver heraf

$$\mathcal{A} = u_0 x^{q^0} + u_1 x^{q^1} = x^{q^0} + x^q \ .$$

Da $\mathcal{A}$ kun består af et enkelt polynomium, gælder der, at Q kun har en rod i $\mathscr{L}_q^k[x]$. ▲

Kapitel 9

Koder der er Anvendelige til Liste-L-Dekodning

I kapitel 6 præsenterede vi en kodekonstruktion, hvor vi ved minimumsafstandsdekodning kunne dekode til det korrekte kodeord, så længe antallet af fejl og sletninger var mindre end den halve minimumsafstand. Det vil sige at det ud fra et modtaget underrum U kun var muligt at dekode til et kodeord. I dette kapitel betragtes liste-L-dekodning, som dekoder til en liste af størrelse maks L indeholdende underrum, som output U kan gå hen i. Heraf kan minimumsafstandsdekodningen i kapitel 6 betragtes som liste-1-dekodning.

9.1 Konstruktion af MV-Koden

I dette afsnit laves en modifikation af KK-koden, som blev præsenteret i afsnit 6.2, denne modification er konstrueret af Mahdavifar og Vardy i [MV12], og koden kaldes derfor MV-koden. Modifikationen består bl.a. af at udvide rummet W, hvori kodeordene er indeholdt, således at kodeordene bliver længere. Dette medfører en øget fejlretningsevne for koden.

Tilsvarende KK-koden konstrueres først et rum W hørende til operatorkanalen. Vi betragter derfor mængden $A = \{\alpha_1, \ldots, \alpha_\ell\} \subset \mathbb{F}_{q^m}$ som består af ℓ lineært uafhængige vektorer over $\mathbb{F}_q$ og fastsætter $L \in \mathbb{N}$. Rummet W bliver således

$$W = \operatorname{span}\{A\} \oplus \underbrace{\mathbb{F}_{q^m} \oplus \cdots \oplus \mathbb{F}_{q^m}}_{L} ,$$

så W er et vektorrum over $\mathbb{F}_q$ med dimension $\ell+Lm$. En MV-kode består som i kapitel 6 af en mængde underrum af W, kaldet kodeord. Konstruktionen af kodeordene sker efter samme model som KK-koden, dog med enkelte ændringer. Et kodeord konstrueres på følgende måde;

1. Bestem en vektor af beskedsymboler af længden k, givet ved $\mathbf{u} = (u_0, \ldots, u_{k-1}) \in \mathbb{F}_q^k$.
2. For vektoren af beskedsymboler defineres et lineariseret beskedpolynomium $f \in \mathscr{L}_q^k[x]$, således
$$f(x) = \sum_{i=0}^{k-1} u_i x^{q^i} \ ,$$
hvis koefficienter svarer til beskedsymbolerne i $\mathbf{u}$.
3. Ud fra beskedpolynomiet $f(x)$ bestemmes kompositionerne
$$f^{\circ 2}(x), \quad f^{\circ 3}(x), \quad \cdots, \quad f^{\circ L}(x) \ .$$
Her gælder der, at $f^{\circ i}(x) \in \mathscr{L}_q^{i(k-1)+1}[x]$, for $i \in \{2, 3, \ldots, L\}$.
4. For ethvert $\alpha_i \in A$, for $i \in \{1, \ldots, \ell\}$, defineres en $L+1$ tupel $\Big(\alpha_i, f(\alpha_i), f^{\circ 2}(\alpha_i), \ldots, f^{\circ L}(\alpha_i)\Big)$. Alle ℓ tupler er således et element i W, og disse er lineært uafhængige, da $\{\alpha_1, \ldots, \alpha_\ell\}$ er en lineært uafhængig mængde. Det vil sige at
$$V = \left\{ \Big(\alpha_1, f(\alpha_1), \ldots, f^{\circ L}(\alpha_1)\Big), \ldots, \Big(\alpha_\ell, f(\alpha_\ell), \ldots, f^{\circ L}(\alpha_\ell)\Big) \right\}$$
er et underrum i W af dimension ℓ. Dette underrum er et kodeord i $\mathcal{C}$.

Af 1. ses at legemet hvori beskedsymbolerne bestemmes er mindre end ved KK-koderne, hvilket skyldes at vi ønsker lineariserede polynomier $f(x)$ i ringen $\mathscr{L}_q^k[x]$, således at sætning 8.5 er opfyldt.

Informationshastigheden for MV-koden konstrueret ved ovenstående fremgangsmåde er betydelig lavere end informationshastigheden KK-koden. Dette skyldes at valget af beskedsymboler er indeholdt i $\mathbb{F}_q$ i stedet for $\mathbb{F}_{q^m}$, så antallet af mulige kodeord i MV-koden er reduceret med en faktor m, samtidig med at dimensionen af MV-koden er øget i forhold til KK-koden. Informationshastigheden for MV-koden er fra definition 7.9

$$R = \frac{\log_q(q^k)}{\ell(\ell + Lm)} = \frac{k}{\ell(\ell + Lm)} \ . \tag{9.1}$$

Vi definerer følgende en kodes pakkehastighed.

Definition 9.1. Pakkehastigheden for en kode $\mathcal{C}$ over $\mathbb{F}_{q^m}$, hvis kodeord har dimension ℓ er givet ved

$$R^* = \frac{\log_{q^m} |\mathcal{C}|}{\ell} = \frac{\log_q |\mathcal{C}|}{\ell m} \ .$$

I det følgende defineres en normal basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, så vi kan udnytte det faktum at beskedsymbolerne er over $\mathbb{F}_q$ til at opveje reduceringen af kodens hastighed. Først betragtes en basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Proposition 9.2. *Lad $\mathbb{F}_{q^m}$ være et udvidelseslegeme over $\mathbb{F}_q$. Da findes et primitivt element $\alpha \in \mathbb{F}_{q^m}$ således at $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right\}$ er en basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. [MS77, Theorem 27]*

Dette propositon giver mulighed for at definere en normal basis for $\mathbb{F}_{q^m}$.

Definition 9.3 (Normal basis for $\mathbb{F}_{q^m}$)**.** Lad α være et primitivt element i $\mathbb{F}_{q^m}$. En basis for $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ på formen $\left\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\right\}$ kaldes en normal basis for $\mathbb{F}_{q^m}$.

Heraf fås at en mængde $A = \{\alpha\}$, hvor α er et primitivt element der frembringer normal basen for $\mathbb{F}_{q^m}$, kan udvides til mængden $A' = \{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$. Da A' er en basis over $\mathbb{F}_q$ gælder der at elementerne i A' er lineært uafhængige over $\mathbb{F}_q$. For et lineariseret polynomium $f(x) \in \mathscr{L}_q[x]$ haves at

$$f\left(\alpha^{q^j}\right) = \sum_{i=0}^{k-1} u_i \left(\alpha^{q^j}\right)^{q^i} = \sum_{i=0}^{k-1} u_i \left(\alpha^{q^i}\right)^{q^j} = \left(\sum_{i=0}^{k-1} u_i \alpha^{q^i}\right)^{q^j} = f(\alpha)^{q^j} \ ,$$

for $j \in \{0, 1, \ldots, m-1\}$, da $u_i \in \mathbb{F}_q$ så $u_i^{q^j} = u_i$. Det vil sige at ved at sende $V = (\alpha, f(\alpha), \ldots, f^{\circ L}(\alpha))$ gennem operatorkanalen under antagelsen, at der ingen sletninger finder sted, kan vi bestemme $V' = (\alpha^{q^j}, f(\alpha^{q^j}), \ldots, f^{\circ L}(\alpha^{q^j}))$ for $j \in \{0, \ldots, m-1\}$, og herfra udlede de resterende elementer i normal basen. Dette gør at der ved dekodningen (se afsnit 9.2) kan rettes flere fejl end hvis det kun var muligt at bestemme V. Da den forbedrede fejlretningsevne opnås ved kun at sende V gennem operatorkanalen forbedres pakkehastigheden for MV-koden.

Af ovenstående idé betragtes i den restende del af dette afsnit kun koder, hvis kodeord har dimension lig med en.

Vektorer af beskedsymboler, $\mathbf{u} \in \mathbb{F}_q^k$ tages over i underrum V ved afbildningen $\mathrm{ew}_A : \mathbb{F}_q^k \to \mathcal{P}(W, 1)$. Når ew_A er injektiv fås at underrummene V er forskellige, og underrummene kan derfor betragtes som kodeord. MV-koden vil i disse tilfælde være værdimængden af ew_A.

Sætning 9.4. *Lad α være et element i $\mathbb{F}_{q^m}$ og $A = \{\alpha\}$. Hvis $k \leq m$ så er afbildningen* $\mathrm{ew}_A : \mathbb{F}_q^k \to \mathcal{P}(W, 1)$ *injektiv.*

Bevis. Antag at $k \leq m$. Vi ønsker så at vise at hvis to beskedpolynomier afbilleder hen i det samme, så er disse ens. Antag, at $\mathrm{ew}_A(f) = \mathrm{ew}_A(g)$ og definer $h(x) = f(x) - g(x)$. Der gælder pr. antagelse, at $h(\alpha) = f(\alpha) - g(\alpha) = 0$. Af den normale basis for $\mathbb{F}_{q^m}$ fås derfor at

$$h\left(\alpha^{q^j}\right) = f(\alpha)^{q^j} - g(\alpha)^{q^j} = (f(\alpha) - g(\alpha))^{q^j} = 0 \ ,$$

for $j \in \{0, 1, \ldots, m-1\}$. Af dette har $h(x)$ i alt q^m nulpunkter, da ethvert $x \in \mathrm{span}\{\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}\}$ er nulpunkt for $h(x)$. Da $k \leq m$ gælder der heraf at polynomiet $h(x)$ har flere nulpunkter end dets grad og $h(x) = 0$. Af dette fås at $f(x) = g(x)$, og ew_A er injektiv. □

Af ovenstående sætning fås at hvis $k \leq m$ så vil en kode $\mathcal{C}$ i $\mathcal{P}(W, 1)$ være værdimængden for afbildningen ew_A.

Det følgende eksempel illustrerer en konstruktion af en kode der kan benyttes til liste-2-dekodning.

Eksempel 9.5. Vi ønsker at konstruere en kode bestående af 1-dimensionale kodeord over $\mathbb{F}_2$, som kan benyttes til liste-2-dekodning. Vi kalder denne kode for $\mathcal{C}_2$. Definer $A = \{(10000)\} \subset \mathbb{F}_{2^5}$ og lad $L = 2$. Vektorrummet W er da givet ved

$$W \ = \ \mathrm{span}\{(10000)\} \oplus \mathbb{F}_{2^5} \oplus \mathbb{F}_{2^5} \ .$$

Dimensionen af W er 11 over $\mathbb{F}_2$. Som besked vælges $\mathbf{u} = (1, 1) \in \mathbb{F}_2^2$, således at det tilsvarende beskedpolynomium $f \in \mathscr{L}_2^2[x]$ bliver

$$f(x) = x^{2^0} + x^{2^1} \ .$$

I bilag D.1 er legemet $\mathbb{F}_{2^5}$ konstrueret over det irreducible polynomium $x^5 + x^3 + 1 \in \mathbb{F}_2[x]$ med $x = \alpha$ som det primitivt element. Da $A = \{(10000)\} = \alpha^4$ bliver $f(\alpha^4) = \alpha^3 + \alpha = \alpha^{29}$ og $f(\alpha^{29}) = \alpha^4 + \alpha^3 + \alpha^2$. Et kodeord svarende til f bliver da underrummet givet ved

$$V = \mathrm{span}\{(10000, 01010, 11100)\} \ .$$

Der findes tre andre kodeord i $\mathcal{C}_2$, som konstrueres på tilsvarende måde ved at vælge de tre tilbageværende beskeder $\mathbf{u} \in \mathbb{F}_2^2$ til at danne beskedpolynomier ud fra. Heraf er koden $\mathcal{C}_2$ givet ved

$$\begin{aligned} \mathcal{C}_2 \ = \ & \{(10000, 01010, 11100), (10000, 10000, 10000), \\ & (10000, 11010, 01100), (10000, 00000, 00000)\} \ . \end{aligned}$$

▲

9.2 Dekodning af MV-Koden

I dette afsnit betragtes liste-L-dekodningen af MV-koden konstrueret i afsnit 9.1. Til dekodningen benyttes algoritme 4 og 5 præsenteret i hhv. afsnit 8.2.1 og 8.3.

Lad MV-koden bestå af kodeord V, hvor der som tidligere nævnt, gælder at $\dim(V) = 1$. Da dimensionen af de afsendte kodeord V er 1 må der ikke ske sletninger, når kodeordene sendes gennem operatorkanalen. Hvis der sker en sletning så vil alt afsendt information forsvinde. I det følgende betragtes derfor kun tilfælde, hvor det afsendte kodeord eventuelt tilføres fejlinformation på sin vej gennem operatorkanalen. Altså optræder sletningsoperatoren $\mathcal{H}_k(V)$ ikke, kun fejlrummet E kan tilføjes kodeord.

Lad V være et afsendt kodeord konstrueret fra beskedpolynomium $f(x)$. Der modtages et rum U, som har dimension $r = 1 + t$, hvor t som tidligere er dimensionen af fejlrummet E, og der gælder at $V \subseteq U$. Først bestemmes en basis for rummet U over $\mathbb{F}_q$, denne består af elementer $(x_i, y_{i,1}, \ldots, y_{i,L})$, hvor $i \in \{1, \ldots, r\}$. Ud fra denne basis bestemmes mængden

$$\mathcal{P} = \left\{ \left(x_i^{q^j}, y_{i,1}^{q^j}, \ldots, y_{i,L}^{q^j} \right) \;\middle|\; 1 \leq i \leq r,\ 0 \leq j \leq m-1 \right\} , \qquad (9.2)$$

hvor punkterne i $\mathcal{P}$ kaldes interpolationspunkter. I det følgende eksempel konstrueres interpolationspunkterne for et modtaget rum U.

Eksempel 9.6. Lad U være et modtaget underrum med basis

$$B = \{(10000, 01010, 11100)\} ,$$

over $\mathbb{F}_2$ indeholdt i $\mathbb{F}_{2^5}^3$. Basen betragtes som det første interpolationspunkt da $q^0 = 1$. Det næste interpolationspunkt med $q = 2$ bliver

$$\begin{aligned} \mathcal{P}_1 &= ((\alpha^4)^2, (\alpha^3 + \alpha)^2, (\alpha^4 + \alpha^3 + \alpha^2)^2) = (\alpha^8, \alpha^{27}, \alpha^{17}) \\ &= (11010, 10110, 11000) . \end{aligned}$$

Det tredje interpolationspunkt bestemmes til

$$\begin{aligned} \mathcal{P}_2 &= ((\alpha^4)^{2^2}, (\alpha^3 + \alpha)^{2^2}, (\alpha^4 + \alpha^3 + \alpha^2)^{2^2}) = ((\alpha^8)^2, (\alpha^{27})^2, (\alpha^{17})^2) \\ &= (01100, 01110, 01000) . \end{aligned}$$

De resterende to interpolationspunkter bliver bestemt på tilsvarende måde. Samlet bliver interpolationspunkterne konstrueret over B

$$\begin{aligned} \mathcal{P} = \{&(10000, 01010, 11100), (11010, 10110, 11000), (01100, 01110, 01000), \\ &(00010, 00110, 10010), (00100, 10100, 11110)\} \subset \mathbb{F}_{2^5}^3 . \end{aligned}$$

▲

Interpolationspunkterne kan i algoritme 4 benyttes til at konstruere et $(L+1)$-variat lineariseret polynomium

$$Q(x, y_1, \ldots, y_L) = Q_0(x) + Q_1(y_1) + \cdots + Q_L(y_L) \,, \tag{9.3}$$

hvor der gælder, at

$$Q(x_i, y_{i,1}, \ldots, y_{i,L}) = 0 \quad \text{for alle} \quad (x_i, y_{i,1}, \ldots, y_{i,L}) \in \mathcal{P} \,. \tag{9.4}$$

Det antages at polynomiet $Q(x, y_1, \ldots, y_L)$ højest har grad $q^{\mu-1}$, hvor $\mu \in \mathbb{N}$.

Hvis det eneste $(L+1)$-variate lineariseret polynomium der opfylder (9.4) er nulpolynomiet, er det ikke muligt at dekode U til V. Vi antager derfor, at $Q(x, y_1, \ldots, y_L)$ ikke er nulpolynomiet. Polynomiet $Q(x, \ldots, y_L)$ omskrives til et bivariat polynomium ved at lade $y_i = y^{\circ i}$, så der haves $Q(x, y^{\circ 1}, \ldots, y^{\circ L}) = Q(x, y)$. Ved anvendelse af algoritme 5 er det heraf muligt at bestemme alle rødder $f(x) \in \mathscr{L}_q^k[x]$, således at

$$Q\left(x, f(x), \ldots, f^{\circ L}(x)\right) = 0 \,. \tag{9.5}$$

Det lineariserede polynomium $f^{\circ i}(x)$ har højest grad $q^{i(k-1)}$, så for hvert $Q_i(\cdot)$ i ligningen (9.3) følger, at disse højest har grad $q^{\mu - i(k-1)-1}$ for $i \in \{0, 1, \ldots, L\}$.

Interpolationspolynomiet $Q(x, y_1, \ldots, y_L) \neq 0$ og beskedpolynomiet $f(x)$ som har konstrueret V definerer et polynomium

$$E(x) = Q\left(x, f(x), \ldots, f^{\circ L}(x)\right) = \sum_{i=0}^{L} Q_i \circ f^{\circ i}(x) \,. \tag{9.6}$$

Lemma 9.7. *Lad $\alpha \in \mathbb{F}_{q^m}$. Polynomiet $E(x)$ har rødder α^{q^j} for $j \in \{0, 1, \ldots, m-1\}$. [MV12, Lemma 6]*

Bevis. Da det antages, at der ikke sker sletninger i netværket, er det afsendte kodeord en delmængde af det modtaget underrum, altså $V \subseteq U$. Heraf haves at $\left(\alpha, f(\alpha), \ldots, f^{\circ L}(\alpha)\right) \in U$, og af (9.2) fås at $\left(\alpha^{q^j}, f(\alpha)^{q^j}, \ldots, f^{\circ L}(\alpha)^{q^j}\right) \in \operatorname{span}\{\mathcal{P}\}$ for $j \in \{0, 1, \ldots, m-1\}$, da f er et lineariseret polynomium. Ud fra (9.4) ses herved, at

$$Q\left(\alpha^{q^j}, f(\alpha)^{q^j}, \ldots, f^{\circ L}(\alpha)^{q^j}\right) = 0 \,,$$

og da $f(x) \in \mathscr{L}_q^k[x]$ haves desuden, at $f^{\circ i}(\alpha)^{q^j} = f^{\circ i}\left(\alpha^{q^j}\right)$ for $i \in \{0, \ldots, L\}$ og $j \in \{0, \ldots, m-1\}$. Dette giver, at

$$E(\alpha^{q^j}) = Q\left(\alpha^{q^j}, f(\alpha^{q^j}), \ldots, f^{\circ L}(\alpha^{q^j})\right) = 0 \,,$$

og heraf, at α^{q^j} er rod i $E(x)$ for alle $j \in \{0, 1, \ldots, m-1\}$. □

Bemærkning 9.8. Rødderne $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ i $E(x)$ kan betragtes som m lineært uafhængige rødder over $\mathbb{F}_q$.

Lemma 9.9. *Lad $q^{\mu-1}$ være højeste grad af det lineariserede polynomium $Q(x, y_1, \ldots, y_L)$. Hvis $\mu \leq m$, så er $E(x)$ nulpolynomiet. [MV12, Korollar 7]*

Bevis. Antag $\mu = m$, altså at q^{m-1} er højeste grad af $Q(x, y_1, \ldots, y_L)$. Da $f(x) \in \mathscr{L}_q^k[x]$ har $f(x)$ højest grad q^{k-1} og graden af $Q_i \circ f^{\circ i}(x)$ for $i \in \{0, \ldots, L\}$ er derfor højest

$$q^{m-i(k-1)-1+i(k-1)} = q^{m-1} \ .$$

Heraf fås at $E(x)$ højest har grad q^{m-1}, men af lemma 9.7 har $E(x)$ i alt q^m rødder, og $E(x)$ må derfor være nulpolynomiet. □

I tilfælde hvor $E(x)$ er nulpolynomiet fås, at beskedpolynomiet $f(x)$ er en løsning til (9.5). Det vil sige at hvis der kan bestemmes et ikke-nul interpolationspolynomium $Q(x, y_1, \ldots, y_L)$, som højest har grad q^{m-1} kan det oprindelige beskedpolynomium bestemmes.

Det ønskes derfor at afgøre under hvilke forhold der altid findes en ikke-nulløsning for $Q(x, y_1, \ldots, y_L)$, som opfylder (9.4). Dette gøres ved at sætte en begrænsning på dimensionen af rummet U, der kan tolkes som en begrænsning på antallet af fejl, der kan korrigeres for.

Lemma 9.10. *Lad U være et underrum i W med dimension $t+1$, og lad $\mathcal{P}$ være mængden af interpolationspunkter for U. Så findes en ikke-nulløsning for et $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L)$ af højest grad q^{m-1} som opfylder, at*

$$Q(x_i, y_{i,1}, \ldots, y_{i,L}) = 0 \quad \textit{for alle} \quad (x_i, y_{i,1}, \ldots, y_{i,L}) \in \mathcal{P} \ , \tag{9.7}$$

hvis

$$t < L - \frac{L(L+1)}{2}\frac{(k-1)}{m} \ .$$

[MV12, Lemma 4]

Bevis. Fra (9.2) haves at mængden af interpolationspunkter $\mathcal{P}$ indeholder $mr = m(1+t)$ punkter, og heraf kan (9.7) betragtes som et ligningssystem bestående af $m(1+t)$ homogene ligninger. Idet hvert lineariseret polynomium $Q_i(\cdot)$ for $i \in \{0, \ldots, L\}$ højest har grad $q^{m-i(k-1)-1}$ fås at antallet af ubekendte er

$$\sum_{i=0}^{L}(m - i(k-1)) = (L+1)m - (k-1)\frac{L(L+1)}{2} \ .$$

For homogene ligningssystemer haves, at hvis der er flere ubekendte end ligninger, da eksisterer en ikke-triviel løsning til systemet. For at garantere en ikke-triviel løsning til (9.7) skal der derfor gælde, at

$$m(1+t) < (L+1)m - (k-1)\frac{L(L+1)}{2} .$$

Af dette fås for dimensionen t af fejlrummet E, at

$$t < \frac{(L+1)m}{m} - 1 - \frac{L(L+1)}{m}\frac{(k-1)}{2} = L - \frac{L(L+1)}{m}\frac{(k-1)}{2} .$$

□

Ud fra ovenstående er metoden til liste-L-dekodning af underrummet U med dimension $1+t$ følgende;

1. Bestem om $t < L - \frac{L(L+1)}{m}\frac{(k-1)}{2}$. Hvis dette ikke tilfældet er dekodningen mislykkes.
2. Bestem en basis $\{(x_1, y_{1,1}, \ldots, y_{1,L}), \ldots, (x_r, y_{r,1}, \ldots, y_{r,L})\}$ for U, hvor $r = 1+t$, og konstruer ud fra denne mængden af interpolationspunkter
$$\mathcal{P} = \left\{ \left(x_i^{q^j}, y_{i,1}^{q^j}, \ldots, y_{i,L}^{q^j} \right) \;\middle|\; 1 \leq i \leq r,\ 0 \leq j \leq m-1 \right\} .$$
3. Konstruer et $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L) \neq 0$ af højest grad q^{m-1} ved anvendelse af algoritme 4 med $\mathcal{P}$ som input.
4. Transformer det $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L)$ til et bivariate lineariseret polynomium $Q(x, y)$.
5. Find alle rødder $f(x) \in \mathscr{L}_q^k[x]$ til (9.5) ved anvendelse af algoritme 5.

Sætning 9.11. *Liste-L-dekodningen angivet ovenfor i punkt* 1. *til* 5. *giver en liste af længde højest L, som indeholder den afsendte meddelelse* **u**, *når*

$$t < L - \frac{L(L+1)}{m}\frac{(k-1)}{2} .$$

[MV12, Sætning 8]

Bevis. Da det er antaget at $t < L - \frac{L(L+1)}{m}\frac{(k-1)}{2}$ så gælder der af lemma 9.10, at $Q(x, y_1, \ldots, y_L) \neq 0$. Fra lemma 9.9 fås at $E(x) = 0$ og $f(x)$ er en løsning til (9.5). Da $Q(x, y_1, \ldots, y_L) \neq 0$ fås af sætning 8.5 at (9.5) højest har L løsninger i $\mathscr{L}_q^k[x]$, og heraf har listen højest længde L og **u** optræder som et af de lineariserede polynomier. □

9.3 Eksempel på Liste-2-Dekodning

I det følgende eksempel dekodes et modtaget underrum, som er output af operatorkanalen, til et kodeord fra koden $\mathcal{C}_2$ konstrueret i eksempel 9.5.

Eksempel 9.12. Lad det modtaget underrum være

$$U = \text{span}\{(\alpha^4, \alpha^{29}, \alpha^{24}), (\alpha, \alpha^6, \alpha^7)\} .$$

Vi benytter metoden fra det foregående afsnit til at dekode U til det afsendte kodeord. Dette er muligt hvis der ingen sletninger er fundet sted i operatorkanalen, og et eventuelt fejlrum højest har dimension $t < 2 - \frac{2(2+1)}{5}\frac{(2-1)}{2} = \frac{7}{5}$. Bemærk at hvis der ingen sletninger er sket i operatorkanalen, så er det afsendte kodeord V indeholdt i spændet af U.

Interpolationspunkterne bestemmes ud fra basen til U;

$$\begin{aligned}\mathcal{P} \;=\; &\Big\{(\alpha^4, \alpha^{29}, \alpha^{24}), (\alpha^8, \alpha^{27}, \alpha^{17}), (\alpha^{16}, \alpha^{23}, \alpha^3), (\alpha, \alpha^{15}, \alpha^6),\\ &(\alpha^2, \alpha^{30}, \alpha^{12}), (\alpha, \alpha^6, \alpha^7)(\alpha^2\alpha^{12}, \alpha^{14}), (\alpha^4, \alpha^{24}, \alpha^{28}),\\ &(\alpha^8, \alpha^{17}, \alpha^{25}), (\alpha^{16}, \alpha^3, \alpha^{19})\Big\} .\end{aligned}$$

Mængden af interpolationspunkter benyttes i algoritme 4 til at konstruere interpolationspolynomiet $Q(x, y_1, y_2)$. Dette giver output

$$Q(x, y_1, y_2) = \alpha^{13} y_1^{q^2} + \alpha^{13} y_1 + \alpha^{13} y_2^q + \alpha^{13} y_2 . \tag{9.8}$$

Bemærk at graden af $Q_1(x)$ er q^2, mens graden af $Q_2(x)$ er q. Da $m = 5$, er det krævet at graden af $Q_1(x)$ højest er q^3 mens graden af $Q_2(x)$ højest er q^2. Dette er tilfældet så graden af $Q(x, y_1, y_2)$ er højest q^{m-1} som krævet. Bemærk desuden at ved at sætte $a = \alpha^{13}$ i (8.20) fås (9.8), hvilket viser at samme interpolationspolynomium kan opnås uanset om Q er bestemt ved at benytte algoritme 4 eller ved at løse ligningssystemer. Interpolationspolynomiet omkrives til et bivariate lineariseret polynomium ved at vælge $y_1 = y^{\circ 1} = y$ og $y_2 = y^{\circ 2}$.

$$Q(x, y) = \alpha^{13} y^{q^2} + \alpha^{13} y + (\alpha^{13} x^q + \alpha^{13} x) \circ y^{\circ 2} .$$

Vi kan herefter benytte algoritme 5 til at bestemme de $y \in \mathscr{L}_q^k[x]$ som opfylder at $Q(x, y) = 0$. Output af algoritme 5 bliver så

$$\mathcal{A} = \{0 \cdot x^{q^0} + 0 \cdot x^q, x^{q^0} + x^q\} .$$

Det er altså lykkedes at dekode U til en liste med to beskedpolynomier. Vi bør være i stand til at afgøre hvilket beskedpolynomium som er benyttet

til konstruktion af det afsendt kodeord fra $\mathcal{C}_2$. Ved at evaluere elementet $\alpha^4 \in \mathbb{F}_{2^5}$ fra konstruktionen af koden i begge beskedpolynomier, skulle vi gerne opnå, at det ene kodeord er indeholdt i spændet af U, mens det andet ikke er. De to beskedpolynomier giver kodeordene;

$$\begin{aligned} V_1' &= \text{span}\{(\alpha^4, \alpha^{29}, \alpha^{24})\} \\ V_2' &= \text{span}\{(\alpha^4, 0, 0)\} \ . \end{aligned}$$

Da $V_1' \subset U$ må det afsendte kodeord være V_1', forudsat at der ingen sletninger har fundet sted i operatorkanalen. ▲

9.4 Generelle MV-Koder

I afsnit 9.1 præsenterede vi en kodekonstruktion af MV-koder, hvor vi fokuserede på koder hvis kodeord havde dimension $\ell = 1$. Dette medførte imidlertid at der ikke måtte ske sletninger i operatorkanalen, så i dette afsnit ændrer vi på MV-kodens konstruktion, således at MV-koder med dimension $\ell > 1$ også kan yde fordel af normal basen fra definition 9.3. Dette gøres blandt andet ved at udvide rummet W endnu en gang.

Lad $\mathbb{F}_q$ være et endeligt legeme og lad $\ell \mid (q-1)$. Så gælder at ligningen $x^\ell - 1 = 0$ har ℓ forskellige rødder i $\mathbb{F}_q$. Vi definerer $e_1 = 1, e_2, \ldots, e_\ell$ til at være disse rødder i $\mathbb{F}_q$. Lad $\mathbb{F}_{q^{\ell m}}$ være et udvidelseslegeme af $\mathbb{F}_q$ og lad γ være en frembringer for en normal basis for $\mathbb{F}_{q^{\ell m}}$. For $i = 1, \ldots, \ell$ defineres

$$\alpha_i = \gamma + e_i\gamma^{q^m} + e_i^2\gamma^{q^{2m}} + \cdots + e_i^{\ell-1}\gamma^{q^{(\ell-1)m}} \ . \tag{9.9}$$

Følgende lemma fastsætter at α_1 og α_i^ℓ er elementer i $\mathbb{F}_{q^m}$.

Lemma 9.13. *For α_i givet ved (9.9) gælder at $\alpha_1 \in \mathbb{F}_{q^m}$ og at for $i \in \{2, \ldots, \ell\}$ ligger α_i^ℓ i legemet $\mathbb{F}_{q^m}$. [MV12, Lemma 9]*

Bevis. Vi betragter $\alpha_i^{q^m}$;

$$\begin{aligned} \alpha_i^{q^m} &= \left(\sum_{j=0}^{\ell-1} e_i^j\gamma^{q^{jm}}\right)^{q^m} = \sum_{j=0}^{\ell-1}\left(e_i^{q^m}\right)^j\gamma^{q^{(j+1)m}} = \sum_{j=0}^{\ell-1} e_i^j\gamma^{q^{(j+1)m}} \\ &= e_i^0\gamma^{q^m} + e_i\gamma^{q^{2m}} + \cdots + e_i^{(\ell-2)}\gamma^{q^{(\ell-1)m}} + e_i^{(\ell-1)}\gamma^{q^{\ell m}} \\ &= \sum_{j=1}^{\ell-1} e_i^{j-1}\gamma^{q^{jm}} + e_i^{(\ell-1)}\gamma^{q^{\ell m}} = \sum_{j=1}^{\ell-1} e_i^{j-1}\gamma^{q^{jm}} + e_i^{-1}\gamma \\ &= \sum_{j=0}^{\ell-1} e_i^{j-1}\gamma^{q^{jm}} = e_i^{-1}\sum_{j=0}^{\ell-1} e_i^j\gamma^{q^{jm}} = e_i^{-1}\alpha_i \ . \end{aligned} \tag{9.10}$$

Ovenstående følger af at $e_i \in \mathbb{F}_q$, hvorfor $e_i^{q^m} = e_i$, og da e_i er rod i $x^\ell - 1 = 0$ følger at $e_i^{(\ell-1)} = e_i^{-1}$. Desuden er γ frembringer for $\mathbb{F}_{q^{\ell m}}$ så $\gamma^{q^{\ell m}} = \gamma$. For $i = 1$ giver (9.10) at $\alpha_1^{q^m} = e_1^{-1}\alpha_1 = \alpha_1$, så $\alpha_1 \in \mathbb{F}_{q^m}$. For $i \in \{2, \ldots, \ell\}$ følger at $\left(\alpha_i^\ell\right)^{q^m} = \left(e_i^{-1}\alpha_i\right)^\ell = e_i^{-\ell}\alpha_i^\ell = \alpha_i^\ell$ så $\alpha_i^\ell \in \mathbb{F}_{q^m}$. □

Vi ønsker i det følgende at konstruere vektorrummet W over legemet $\mathbb{F}_{q^{\ell m}}$. Til dette har vi brug for en basis for $\mathbb{F}_{q^{\ell m}}$ over legemet $\mathbb{F}_q$.

Lemma 9.14. *Mængden*

$$Z = \{\alpha_i^{q^j} | 1 \leq i \leq \ell, 0 \leq j \leq m-1\}$$

er en basis for $\mathbb{F}_{q^{\ell m}}$. *[MV12, Lemma 10]*

Bevis. Definer A og Γ til $1 \times \ell$ vektorer givet ved

$$\begin{aligned} A &= (\alpha_1, \alpha_2, \ldots, \alpha_\ell) \\ \Gamma &= \left(\gamma, \gamma^{q^m}, \ldots, \gamma^{q^{(\ell-1)m}}\right) . \end{aligned}$$

Lad desuden E være en $\ell \times \ell$ matrix givet ved

$$E = \begin{bmatrix} e_1^0 & e_1 & \cdots & e_1^j & \cdots & e_1^{\ell-1} \\ e_2^0 & e_2 & \cdots & e_2^j & \cdots & e_2^{\ell-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ e_i^0 & e_i & \cdots & e_i^j & \cdots & e_i^{\ell-1} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ e_\ell^0 & e_\ell & \cdots & e_\ell^j & \cdots & e_\ell^{\ell-1} \end{bmatrix} .$$

Så gælder at $A = \Gamma E^\top$. Da E er en Vandermonde matrix og da alle e_i'erne er forskellige for $i \in \{1, \ldots, \ell\}$ så gælder at determinanten af E er ikke-nul. Heraf eksisterer den inverse matrix til E og

$$\Gamma = A\left(E^{-1}\right)^\top .$$

Dette udtryk viser at for $j \in \{0, \ldots, \ell-1\}$ er $\gamma^{q^{jm}}$ en linear kombination af $\alpha_1, \ldots, \alpha_\ell$. For $r \in \{0, \ldots, m-1\}$ følger så at $\gamma^{q^{jm+r}}$ er en linear kombination af $\alpha_1^{q^r}, \ldots, \alpha_\ell^{q^r}$. Det vil sige at for $0 \leq h \leq \ell m - 1$ er γ^{q^h} en linear kombination af elementer fra Z. Da γ frembringer $\mathbb{F}_{q^{\ell m}}$ så følger at elementerne i Z udspænder hele $\mathbb{F}_{q^{\ell m}}$. Dog gælder at $|Z| = \ell m$, så Z må være en basis for $\mathbb{F}_{q^{\ell m}}$. □

Lad $A = \{\alpha_1, \ldots, \alpha_\ell\} \subset \mathbb{F}_{q^m}$, hvor α_i for $i \in \{1, \ldots, \ell\}$ er konstrueret som i (9.9). Bemærk at fra konstruktionen af α_i'erne kræves at $\ell \leq q-1$ hvorved elementerne i A er lineært uafhængige over $\mathbb{F}_q$. Fastsæt $L \in \mathbb{N}$. Vektorrummet W defineres til

$$W = \text{span}\{\alpha_1, \ldots, \alpha_\ell\} \oplus \underbrace{\mathbb{F}_{q^{\ell m}} \oplus \cdots \oplus \mathbb{F}_{q^{\ell m}}}_{L \text{ gange}} .$$

Dimensionen af W er da $\ell + \ell m L$ over $\mathbb{F}_q$.

Indkodningen af et kodeord sker på tilsvarende måde som i afsnit 9.1. En beskedvektor $\mathbf{u} \in \mathbb{F}_q^k$ vælges og benyttes til konstruktion af et beskedpolynomium $f(x) \in \mathscr{L}_q^k[x]$. For hvert element $\alpha_i \in A$ konstrueres herefter en $(L+1)$-tupel $v_i \in W$ ved

$$v_i = \left(\alpha_i, f(\alpha_i), f^{\circ 2}(\alpha_i), \ldots, f^{\circ L}(\alpha_i)\right) ,$$

som udspænder kodeordet

$$\begin{aligned} V \;=\; & \text{span}\left\{\left(\alpha_1, f(\alpha_1), f^{\circ 2}(\alpha_1), \ldots, f^{\circ L}(\alpha_1)\right), \left(\alpha_2, f(\alpha_2), f^{\circ 2}(\alpha_2), \ldots, f^{\circ L}(\alpha_2)\right), \right. \\ & \left. \ldots, \left(\alpha_\ell, f(\alpha_\ell), f^{\circ 2}(\alpha_\ell), \ldots, f^{\circ L}(\alpha_\ell)\right)\right\} \subset W . \end{aligned}$$

Som i afsnit 9.1 kan indkodningen af beskedvektorer til kodeord betragtes som en afbildning $\text{ew}_A : \mathbb{F}_q^k \to \mathcal{P}(W, \ell)$. Når A indeholder ℓ elementer fra $\mathbb{F}_{q^m}$, så er ew_A injektiv hvis $k \leq \ell m$.

Korollar 9.15. *Lad $A = \{\alpha_1, \ldots, \alpha_\ell\} \subset \mathbb{F}_{q^m}$. Hvis $k \leq \ell m$ så er afbildningen $\text{ew}_A : \mathbb{F}_q^k \to \mathcal{P}(W, \ell)$ injektiv.*

Bevis. Følger af sætning 9.4. Antag at $k \leq \ell m$, at $\text{ew}_A(f) = \text{ew}_A(g)$ og vis at for $h(x) = f(x) - g(x) \in \mathscr{L}_q^k[x]$, er $\alpha_i^{q^j}$ for $i \in \{1, \ldots, \ell\}, j \in \{0, \ldots, m-1\}$ et nulpunkt i $h(x)$. Fra lemma 9.14 følger så at $h(x)$ har $q^{\ell m}$ nulpunkter. Heraf er $h(x)$ nulpolynomiet og $f(x) = g(x)$, hvorved ew_A er injektiv. □

En MV-kode hvis kodeord har dimension ℓ, kan derfor betragtes som værdimængden af afbildningen ew_A, hvor A indeholder ℓ lineært uafhængige elementer over $\mathbb{F}_q$ konstrueret som i (9.9).

9.5 Dekodning af Generelle MV-Koder

Lad V være et kodeord i en MV-kode præsenteret i afsnit 9.4 med dimension ℓ. Idet V sendes gennem operatorkanalen kan der ske både sletninger og fejl. Hvis $\ell = 1$ haves tilfældet fra afsnit 9.2 og hermed må der ikke ske sletninger. Antallet af sletninger der finder sted udtrykkes ved sletningsoperatoren $\mathcal{H}_k(V)$ og betegnes ρ, mens antallet af fejl der tilføres V fra fejlrummet E er givet ved $t = \dim(E)$. Ud fra det afsendte rum V modtages ved dekoderen et rum U, som er et underrum i W med dimension $r = \ell - \rho + t$. Vi har brug for at sikre os, at hele det afsendte kodeord V ikke bliver slettet i operatorkanalen, så det antages, at $\rho < \ell$, hvilket vil sige at $V \cap U \neq \emptyset$. Fællesmængden $V \cap U$ har dimension $\ell - \rho$.

Der bestemmes en basis for rummet U, og denne er

$$\{(x_i, y_{i,1}, \ldots, y_{i,L}) \mid i \in \{1, 2, \ldots, r\}\} .$$

Ud fra denne basis defineres mængderne

$$\mathcal{P}_h = \left\{ \left(x_i^{q^h}, y_{i,1}^{q^h}, \ldots, y_{i,L}^{q^h} \right) \;\middle|\; 1 \leq i \leq r \right\} , \tag{9.11}$$

for $h \in \{0, 1, \ldots, m-1\}$, og disse samles i en mængde af interpolationspunkter, som er givet ved

$$\mathcal{P} = \bigcup_{h=0}^{m-1} \mathcal{P}_h .$$

For mængderne $\mathcal{P}_h$ haves følgende egenskab.

Lemma 9.16. *Givet mængderne $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_{m-1}$ gælder at*

$$\operatorname{span}\{\mathcal{P}_i\} \cap \operatorname{span}\{\mathcal{P}_j\} = \{\mathbf{0}\} ,$$

for alle i og j, hvor $i \neq j$. [MV12, Lemma 12]

Bevis. Da $x_i \in A$ for ethvert $i \in \{1, \ldots, r\}$ gælder der, at

$$x_i = \nu_1 \alpha_1 + \nu_2 \alpha_2 + \cdots + \nu_\ell \alpha_\ell \;\text{ hvor }\; \nu_1, \ldots, \nu_\ell \in \mathbb{F}_{q^m} .$$

Heraf fås, at

$$x_i^{q^h} = \nu_1^{q^h} \alpha_1^{q^h} + \nu_2^{q^h} \alpha_2^{q^h} + \cdots + \nu_\ell^{q^h} \alpha_\ell^{q^h} ,$$

hvilket vil sige at $x_i^{q^h} \in \operatorname{span}\{\alpha_1^{q^h}, \ldots, \alpha_\ell^{q^h}\}$. Fra lemma 9.14 haves at vektorrummene $\operatorname{span}\{\alpha_1^{q^h}, \ldots, \alpha_\ell^{q^h}\}$ er disjunkte for $h \in \{0, \ldots, m-1\}$. Dette giver at $\operatorname{span}\{\mathcal{P}_h\}$ også er disjunkte for $0 \leq h \leq m-1$. □

Som i afsnit 9.2 kan interpolationspunkterne fra $\mathcal{P}$ anvendes til at bestemme et $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L)$, som opfylder at

$$Q(x_i, y_{i,1}, \ldots, y_{i,L}) = 0 \quad \text{for alle} \quad (x_i, y_{i,1}, \ldots, y_{i,L}) \in \mathcal{P} \, . \tag{9.12}$$

Det antages at Q højest har grad $q^{\omega-1}$, hvilket vil sige at hvert Q_i højest har grad $q^{\omega-i(k-1)-1}$. Hvis Q er nulpolynomiet er det ikke muligt at dekode og det ønskes derfor at bestemme under hvilke forhold for ω det er muligt at garantere en ikke-nulløsning til Q.

Lemma 9.17. *Lad U være et underrum af W med dimension r og $\mathcal{P}$ være mængden af interpolationspunkter for U. Da findes et ikke-nul multivariat lineariseret polynomium $Q(x, y_1, \ldots, y_L)$ af grad højest $q^{\omega-1}$, som opfylder* (9.12)*, hvis*

$$\omega = \left\lceil \frac{mr+1}{L+1} + \frac{L(k-1)}{2} \right\rceil \, . \tag{9.13}$$

[MV12, Lemma 11]

Bevis. Af (9.12) fås et ligningssystem bestående af mr homogene ligninger da $|\mathcal{P}| = mr$. Da ethver Q_i højest har grad $\omega - i(k-1) - 1$ haves der

$$\sum_{i=0}^{L} (\omega - i(k-1)) = (L+1)\omega - (k-1)\frac{L(L+1)}{2}$$

ubekendte som ønskes bestemt. Hvorfor der skal gælde at

$$mr < (L+1)\omega - (k-1)\frac{L(L+1)}{2} \, ,$$

som giver at

$$\omega \geq \frac{mr+1}{L+1} + \frac{L(k-1)}{2},$$

hvilket er opfyldt ved valget i (9.13). □

I det følgende antages det at (9.13) er opfyldt, så $Q(x, y_1, \ldots, y_L)$ er forskelligt fra nulpolynomiet. Vi ønsker at bestemme hvilke lineariserede polynomier $f \in \mathscr{L}_q^k[x]$ der opfylder, at

$$Q\left(x, f(x), \ldots, f^{\circ L}(x)\right) = 0 \, , \tag{9.14}$$

hvilket er muligt ved anvendelse af algoritme 5, hvis $Q(x, y_1, \ldots, y_L)$ er bivariat i stedet for $(L+1)$-variat. For at opnå et bivariat polynomium redefineres de variable som $Q(x, y_1, \ldots, y_L)$ afhænger af, således at $x := x$ og

$y_i := y^{\circ i}$ for $i \in \{1, \ldots, L\}$. Det vil sige at der haves et bivariat polynomium $Q(x, y) = Q(x, y^{\circ 1}, \ldots, y^{\circ L})$.

Det bivariate lineariserede polynomium $Q(x, y^{\circ 1}, \ldots, y^{\circ L})$ som opfylder (9.12), og beskedpolynomiet som har frembragt V definerer et lineariseret polynomium tilsvarende (9.6), altså

$$E(x) = Q(x, f(x), \ldots, f^{\circ L}(x)) = \sum_{i=0}^{L} Q_i \circ f^{\circ i}(x) \ .$$

Det ønskes at bestemme hvor mange lineært uafhængige rødder $E(x)$ har i $\mathbb{F}_q$.

Lemma 9.18. *Det lineariserede polynomium $E(x)$ har mindst $(\ell - \rho)m$ lineært uafhængige rødder over $\mathbb{F}_q$. [MV12, Lemma 13]*

Bevis. Lad $U' = V \cap U$, så har U' dimension $\ell - \rho$. Der gælder for ethvert element $(x, y_1, \ldots, y_L) \in U'$ at $\left(x^{q^h}, y_1^{q^h}, \ldots, y_L^{q^h}\right) \in \text{span}\{\mathcal{P}_h\}$ for $h \in \{0, 1, \ldots, m-1\}$, da $U' \subseteq U$. Da Q er et $(L+1)$-variat lineariseret polynomium bestemt ud fra $\mathcal{P}$ gælder der, at

$$Q\left(x^{q^h}, y_1^{q^h}, \ldots, y_L^{q^h}\right) = 0 \text{ for } (x, y_1, \ldots, y_L) \in U' \text{ og } 0 \leq h \leq m-1 \ . \quad (9.15)$$

Da $U' \subseteq V$ gælder der desuden at $(x, y_1, \ldots, y_L) \in V$, det vil sige at

$$(x, y_1, \ldots, y_L) = \left(\beta, f(\beta), \ldots, f^{\circ L}(\beta)\right) \text{ for } \beta \in \text{span}\{\alpha_1, \ldots, \alpha_\ell\} \ .$$

Beskedpolynomiet $f(x)$ er et element i $\mathscr{L}_q^k[x]$, hvilket betyder, at

$$\left(x^{q^h}, y_1^{q^h}, \ldots, y_L^{q^h}\right) = \left(\beta^{q^h}, f\left(\beta^{q^h}\right), \ldots, f^{\circ L}\left(\beta^{q^h}\right)\right) \ , \quad (9.16)$$

samt at $\left(\beta^{q^h}, f\left(\beta^{q^h}\right), \ldots, f^{\circ L}\left(\beta^{q^h}\right)\right) \in \text{span}\{\mathcal{P}_h\}$ for $0 \leq h \leq m-1$.

Det vil sige at ved at sætte (9.16) ind i (9.15) fås

$$Q\left(\beta^{q^h}, f\left(\beta^{q^h}\right), \ldots, f^{\circ L}\left(\beta^{q^h}\right)\right) = 0 \text{ for } 0 \leq h \leq m-1 \ .$$

Fra lemma 9.16 haves at $\text{span}\{\mathcal{P}_h\}$ er disjunkte for $0 \leq h \leq m-1$, og da $\dim(U') = \ell - \rho$ er antallet af lineært uafhængige rødder i $\mathbb{F}_q$ for $E(x)$ lig med $(\ell - \rho)m$. □

Korollar 9.19. *Lad Q være et $(L+1)$-variat lineariseret polynomium af grad højest $q^{\omega-1}$. Hvis $\omega \leq (\ell - \rho)m$ så er $E(x)$ nulpolynomiet. [MV12, Korollar 14]*

Bevis. Beskedpolynomiet $f(x)$ har højest grad q^{k-1}, da $f(x) \in \mathscr{L}_q^k[x]$. Heraf gælder der, at graden af $Q_i \circ f^{\circ i}(x)$ højest er

$$q^{\omega - i(k-1) - 1 + i(k-1)} = q^{\omega - 1} \quad \text{for} \quad i \in \{0, 1, \ldots, L\} \; .$$

Dette giver at graden af $E(x)$ højest er $q^{\omega-1}$. Af lemma 9.18 fås imidlertid at $E(x)$ har $q^{(\ell-\rho)m}$ nulpunkter, og $E(x)$ har derfor lavere grad end antallet af nulpunkter, hvilket medfører at $E(x)$ er nulpolynomiet. □

Når $E(x)$ er nulpolynomiet gælder der, at $f(x)$ er løsning til (9.14), og herved vil beskedpolynomiet som konstruerede V optræde som output ved dekoderen.

Liste-L-dekodningen af rummet U med dimension $r = \ell - \rho + t$ foregår af ovenstående ved følgende skridt;

1. Bestem parameteren
$$\omega = \left\lceil \frac{mr+1}{L+1} + \frac{L(k-1)}{2} \right\rceil \; .$$

2. Bestem en basis $\{(x_i, y_{i,1}, \ldots, y_{i,L}) \mid 1 \leq i \leq r\}$ for U. Konstruer mængderne $\mathcal{P}_h$ som i (9.11), og bestem mængden af interpolationspunkter
$$\mathcal{P} = \bigcup_{h=0}^{m-1} \mathcal{P}_h \; .$$

3. Konstruer et $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L) \neq 0$ af grad højest $q^{\omega-1}$ ved anvendelse af algoritme 4 med $\mathcal{P}$ som input.

4. Transformer det $(L+1)$-variat lineariseret polynomium $Q(x, y_1, \ldots, y_L)$ til et bivariate lineariseret polynomium $Q(x, y)$.

5. Find alle rødder $f(x)$ af højest grad q^{k-1} til (9.14) ved anvendelse af algoritme 5.

Sætning 9.20. *Liste-L-dekodningen angivet i* 1.- 5. *giver en liste af længde højest L, som indeholder beskedpolynomiet $f(x)$ til det afsendte kodeord V, hvis*

$$L\rho + t \leq \ell L - \frac{L(L+1)(k-1)}{2m} - \frac{1}{m} \; .$$

[MV12, Sætning 15]

Bevis. Af lemma 9.17 gælder der at der findes et ikke-nul $(L+1)$-variat lineariseret polynomium Q, som opfylder (9.12) når

$$\omega = \left\lceil \frac{mr+1}{L+1} + \frac{L(k-1)}{2} \right\rceil .$$

Af korollar 9.19 fås at $E(x)$ er nulpolynomiet og hermed at $f(x)$ er løsning til (9.14), hvis der gælder, at

$$\begin{aligned} \frac{mr+1}{L+1} + \frac{L(k-1)}{2} &\leq \omega \leq (\ell-\rho)m \;\Rightarrow \\ \frac{mr+1}{L+1} + \frac{L(k-1)}{2} &\leq (\ell-\rho)m \; . \end{aligned}$$

Da $r = \ell - \rho + t$ fås at

$$\begin{aligned} \ell - \rho + t + \frac{1}{m} + \frac{L(L+1)(k-1)}{2m} &\leq \ell L - L\rho + \ell - \rho \Leftrightarrow \\ L\rho + t &\leq \ell L - \frac{L(L+1)(k-1)}{2m} - \frac{1}{m} \; . \end{aligned}$$

Ovenstående begrænsning på antallet af sletninger og fejl giver at $E(x)$ er nulpolynomiet, og hermed optræder beskedpolynomiet på listen der konstrueres ved dekodning. Da Q ikke er nulpolynomiet gælder der af sætning 8.5, at (9.14) højest har L løsninger, og heraf får listen højest længde L. □

9.6 Eksempel på Generelle MV-koder

Følgende eksempel illustrerer de generelle MV-koders konstruktion og dekodning når der benyttes liste-2-dekodning. Koden i eksemplet er over det endelige legeme $\mathbb{F}_{3^{10}}$, som er konstrueret ved $\mathbb{F}_{3^{10}} = \mathbb{F}_3[x]/\langle x^{10} + 2x^3 + 2x + 2 \rangle$.

Eksempel 9.21. Lad $q = 3$, $m = 5$, $\ell = 2$, $L = 2$, $k = 2$ og lad γ være en frembringer for $\mathbb{F}_{3^{2\cdot 5}}$. Det ønskes således at konstruere en kode $\mathcal{C}_3$ med kodeord af dimension to, som kan benyttes til liste-2-dekodning ud fra en mængde $A \subset \mathbb{F}_{3^{10}}$ og beskedpolynomier $f(x) \in \mathscr{L}_2^2[x]$. For at bestemme mængden A konstrueres α_1 og α_2 som angivet i (9.9). Først ses at ligningen $x^2 - 1 = 0$ har de to løsninger $x = 1$ og $x = 2$ i $\mathbb{F}_3$ og heraf fås

$$A = \left\{ \left(\gamma + \gamma^{243}\right), \left(\gamma + 2\gamma^{243}\right) \right\} \subset \mathbb{F}_{3^{10}} \; .$$

Rummet W er således givet ved

$$W = \mathrm{span}\{A\} \oplus \mathbb{F}_{3^{10}} \oplus \mathbb{F}_{3^{10}} \; ,$$

og har dimension 22 over $\mathbb{F}_3$. Som beskedvektor vælges $\mathbf{u} = (2,1) \in \mathbb{F}_3^2$ og ud fra denne bestemmes beskedpolynomiet $f(x) \in \mathscr{L}_3^2[x]$ til

$$f(x) = x^3 + 2x \ .$$

Heraf fås et kodeord i koden $\mathcal{C}_3$ til at være

$$\begin{aligned} V &= \operatorname{span}\Big\{\Big(\gamma+\gamma^{243}, \gamma^9+2\gamma^6+\gamma^3+\gamma, \gamma^8+\gamma^7+2\gamma^6+2\gamma^4+\gamma^2+2\gamma+2\Big), \\ &\quad \Big(\gamma+2\gamma^{243}, 2\gamma^9+\gamma^6+\gamma^3, 2\gamma^9+2\gamma^8+2\gamma^7+\gamma^6+\gamma^4+2\gamma^3+2\gamma^2+1\Big)\Big\}. \end{aligned} \tag{9.17}$$

De resterende kodeord i $\mathcal{C}_3$ bestemmes på tilsvarende måde ved at vælge andre beskedvektorer $\mathbf{u} \in \mathbb{F}_3^2$, hvorfra beskedpolynomium og kodeord konstrueres.

Vi antager at kodeordet V fra (9.17) sendes gennem operatorkanalen og at der modtages et rum

$$\begin{aligned} U &= \operatorname{span}\Big\{\Big(\gamma+\gamma^{243}, \gamma^9+2\gamma^6+\gamma^3+\gamma, \gamma^8+\gamma^7+2\gamma^6+2\gamma^4+\gamma^2+2\gamma+2\Big), \\ &\quad \Big(\gamma^{27}+\gamma^{729}, \gamma^{12}, \gamma^{46}\Big)\Big\} \ , \end{aligned}$$

som dekodes ved metoden beskrevet i afsnit 9.5. Dimensionen af U bestemmes til $r = 2$ og heraf bliver $\omega = 5$, hvilket vil sige at polynomiet $Q(x, y_1, y_2)$ højest må have grad 3^4.

Ud fra basen for U konstrueres interpolationspunkterne ved metoden i (9.11). Mængden af interpolationspunkter $\mathcal{P}$ anvendes som input i algoritme 4 til at konstruere interpolationspolynomiet $Q(x, y_1, y_2)$ og der fås output

$$\begin{aligned} Q(x,y_1,y_2) &= \Big(\gamma^8+2\gamma^7+2\gamma^6+\gamma^5+2\gamma+1\Big)x^{3^4} \\ &\quad + \Big(2\gamma^9+\gamma^8+2\gamma^6+2\gamma^5+\gamma^4+2\gamma^2+\gamma\Big)x^{3^3} \\ &\quad + \Big(2\gamma^9+\gamma^8+2\gamma^7+\gamma^5+\gamma^3+2\gamma^2+2\Big)x^{3^2} \\ &\quad + \Big(2\gamma^8+2\gamma^5+\gamma^4+\gamma\Big)x^3 \\ &\quad + \Big(2\gamma^9+\gamma^8+2\gamma^7+2\gamma^6+\gamma^4+2\gamma^3+2\gamma^2+\gamma\Big)x \\ &\quad + \Big(2\gamma^8+\gamma^7+\gamma^6+2\gamma^5+\gamma+2\Big)y_1^{3^3} \\ &\quad + \Big(2\gamma^9+2\gamma^8+2\gamma^7+2\gamma^6+\gamma^5+\gamma^3+2\gamma+2\Big)y_1^{3^2} \\ &\quad + \Big(2\gamma^9+\gamma^8+2\gamma^6+2\gamma^5+\gamma^4+\gamma^3+\gamma^2+\gamma+2\Big)y_1^3 \\ &\quad + \Big(\gamma^9+2\gamma^8+2\gamma^6+2\gamma^5+\gamma^4+2\gamma^3+\gamma^2+2\gamma+1\Big)y_1 \\ &\quad + \Big(2\gamma^9+2\gamma^8+2\gamma^7+2\gamma^5+2\gamma^4+2\gamma^3+\gamma^2\Big)y_2^3 \\ &\quad + \Big(2\gamma^9+\gamma^8+\gamma^7+2\gamma^5+2\gamma^2+\gamma+1\Big)y_2 \ . \end{aligned}$$

Der gælder for $Q(x, y_1, y_2)$ at hvert Q_i for $i \in \{0, 1, 2\}$ højest har grad $q^{\omega - i(k-1)-1}$ så Q kan anvendes til dekodningen. Interpolationspolynomiet Q omskrives derfor til et bivariat lineariseret polynomium $Q(x, y)$ ved at lade $y_1 = y^{\circ 1}$ og $y_2 = y^{\circ 2}$. Hermed kan algoritme 5 benyttes til bestemme de lineariserede polynomier $y \in \mathscr{L}_3^2[x]$ som er rod i $Q(x, y)$. Output af algoritmen er

$$\mathcal{A} = \{1 \cdot x^{3^1} + 2 \cdot x^{3^0}\} .$$

Altså er det lykkedes at dekode det modtaget rum U til en liste indeholdende et polynomium. Ved at evaluere elementerne α_1 og α_2 i dette polynomium fås et kodeord svarende til det afsendte kodeord V fra (9.17). Heraf giver dekodningen et korrekt resultat. ▲

9.7 Minimumsafstand for MV-Koden

I dette afsnit betragtes minimumsafstanden af MV-koder. Dette er relevant, da vi er interesseret i at dekodningen af MV-koderne, beskrevet i afsnit 9.5, er liste-L-dekodning. Det vil sige at fejlretningsevnen ved liste-L-dekodning bør være mindst lige så god som minimumsafstandsdekoderen ved nogle pakkehastigheder.

Afstanden mellem kodeord i MV-koder måles ved samme afstandsfunktion som ved KK-koder givet i definition 6.1. Det vil sige for to kodeord V_1 og V_2 i en MV-kode fås afstanden til at være

$$\dim(V_1) + \dim(V_2) - 2\dim(V_1 \cap V_2) = 2\ell - 2\dim(V_1 \cap V_2) ,$$

da MV-koder har konstant dimension ℓ. For at bestemme minimumsafstanden skal

$$\max_{V_1, V_2 \in \mathcal{C}} (\dim(V_1 \cap V_2))$$

for to kodeord i MV-koden findes. Metoden til dette er tilsvarende metoden anvendt i bevis til sætning 6.11, hvor minimumsafstanden af KK-koden fastsættes.

Sætning 9.22. *For en MV-kode over $\mathbb{F}_{q^{\ell m}}$ konstrueret med parametrene k og L er minimumsafstanden*

$$2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right) .$$

[Mah12]

Bevis. Lad $f, g \in \mathscr{L}_q^k[x]$, hvor der gælder, at $f \neq g$, og definer $V_1 = \mathrm{ew}_A(f)$ og $V_2 = \mathrm{ew}_A(g)$. Antag, at $\dim(V_1 \cap V_2) = r$, da findes r lineært uafhængige elementer $((\alpha_1')^{q^h}, (\beta_1')^{q^h}), \ldots, ((\alpha_r')^{q^h}, (\beta_r')^{q^h})$ for hvert $h \in \{0, \ldots, m-1\}$, hvor $f\left((\alpha_i')^{q^h}\right) = (\beta_i')^{q^h} = g\left((\alpha_i')^{q^h}\right)$ for $i \in \{1, \ldots, r\}$. Heraf følger, at $(\alpha_1')^{q^h}, \ldots, (\alpha_r')^{q^h}$ er lineært uafhængige. Ud fra dette fås, at for alle $b \in \mathrm{span}\{(\alpha_1')^{q^h}, \ldots, (\alpha_r')^{q^h}\}$ haves at $f(b) - g(b) = 0$, hvilket vil sige at f og g har q^{mr} fælles punkter. Antag, at $r \geq \left\lceil \frac{k}{m} \right\rceil$ og lad $\kappa = f - g$. Graden af f og g er højest q^{k-1}. Det vil sige at κ højest kan have grad q^{k-1}, men har $q^{mr} \geq q^{m\left\lceil \frac{k}{m} \right\rceil} \geq q^{m\frac{k}{m}} = q^k$ nulpunkter, hvorved $\kappa = 0$. Heraf gælder at $f = g$, hvilket strider imod antagelsen at $f \neq g$, og derfor gælder, at $r \leq \left\lceil \frac{k}{m} \right\rceil - 1$. Hermed fås at afstanden mellem V_1 og V_2 er nedre begrænset af

$$\dim(V_1) + \dim(V_2) - 2\dim(V_1 \cap V_2) = 2\ell - 2r \geq 2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right) . \quad (9.18)$$

Den højeste fælles dimension to kodeord kan have er $\ell - 1$, da de er ens hvis de har fælles dimension ℓ. Det vil sige at for $r = \ell - 1$ haves

$$2\ell - 2(\ell - 1) \geq 2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right) , \quad (9.19)$$

af (9.18). Fra korollar 9.15 haves at $k \leq \ell m$, hvilket giver at $\frac{k}{m} \leq \left\lceil \frac{k}{m} \right\rceil \leq \ell$, så der gælder, at

$$2\ell - 2(\ell - 1) \leq 2\ell - 2\left(\left\lceil \frac{k}{m} \right\rceil - 1\right) . \quad (9.20)$$

Af (9.19) og (9.20) fås, at

$$2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right) \leq 2\ell - 2(\ell - 1) \leq 2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right) ,$$

og minimumsafstanden for koden er $2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right)$. □

Vi ønsker at betragte MV-kodens fejlretningsevne i forhold til pakkehastigheden for koden, angivet i definition 9.1. For den generelle MV-kode bliver pakkehastigheden således

$$R_{MV}^* = \frac{k}{\ell m} ,$$

og da $k \leq \ell m$ gælder der, at $R^* \in [0, 1]$. Ved dekodning af MV-koden konstrueres det $(L+1)$-variate lineariserede polynomium $Q(\cdot) = Q_0(\cdot) + Q_1(\cdot) + \cdots + Q_L(\cdot)$, hvis lineariserede polynomier $Q_i(\cdot)$ har grad højest $q^{\ell m - (k-1)i - 1}$.

Det vil sige at $\ell m - (k-1)L - 1 \geq 0$, da $Q_L(\cdot)$ ikke må have negativ grad. Heraf fås, at

$$L \leq \frac{\ell m - 1}{k-1} \approx \frac{1}{R^*_{MV}} \,, \tag{9.21}$$

hvilket giver at pakkehastigheden opfylder, at

$$R^*_{MV} \leq \frac{1}{L} \,. \tag{9.22}$$

Dette betyder at for en kode konstrueret med et givet L er fejlretningsevnen mest optimal, når (9.22) er opfyldt, eller sagt med andre ord, for $R^*_{MV} > \frac{1}{L}$, så findes en MV-kode konstrueret med $L' < L$, som har en bedre fejlretningsevne. Desuden, hvis uligheden i (9.21) ikke er opfyldt, så kan vi ikke garantere dekodning og dermed heller ikke fejlkorrigering, jævnfør afsnit 9.5.

Da fejlretningsevnen for MV-koderne ønskes bestemt generelt og ikke kun for en kode med bestemte parametre betragtes den normaliserede minimumsafstand

$$\delta_{MV} = \frac{2\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right)}{2\ell} = \frac{\left(\ell - \left\lceil \frac{k}{m} \right\rceil + 1\right)}{\ell} \to 1 - R^* \,,$$

for $\ell \to \infty$. Her divideres med 2, da vi ønsker at bestemme hvor mange fejl der kan rettes ved minimumsafstandsdekodning, hvilket er begrænset af den halve minimumsafstand. Idet minimumsafstanden for MV-koder ikke afhænger af parameteren L gælder der, at fejlretningsevnen med en minimumsafstandsdekoder er ens for alle MV-koder.

Når dekodning fra afsnit 9.5 betragtes haves fra sætning 9.20, at hvis

$$L\rho + t \leq \ell L - \frac{L(L+1)(k-1)}{2m} - \frac{1}{m} \,,$$

så kan der dekodes, hvilket er en begrænsning på antallet af fejl og sletninger. Af dette fås dekodningsradius for MV-koden til at være

$$\ell L - \frac{L(L+1)(k-1)}{2m} - \frac{1}{m} \,,$$

som beskriver fejlretningsevnen for MV-koden når liste-L-dekodningen anvendes. Som ved minimumsafstanden ønskes den normaliserede dekodningsradius, hvilken er givet ved

$$\tau = L - \frac{L(L+1)(k-1)}{2\ell m} - \frac{1}{\ell m} \approx L - \frac{L(L+1)}{2} R^* \,.$$

Det er ikke muligt at gøre dekodningsradiusen for MV-koder uafhængig af parameteren L. Dette er vi dog heller ikke interesseret i, da vi gerne vil

undersøge hvilken indflydelse liste-størrelsen har på fejlretningsevnen. Dette betyder yderligere, at selvom τ beskriver dekodningsradiusen for MV-koder generelt, skal den bestemmes for ethvert L vi ønsker at betragte.

Da vi ved at KK-koden tilnærmelsesvis når Singleton Grænsen ønskes det at sammenligne fejlretningsevne for KK-koden ved minimumsafstands-dekodning med fejlretningsevnerne for MV-koden ved miminumsafstands- og liste-L-dekodning. For KK-koden bestemmes derfor pakkehastigheden

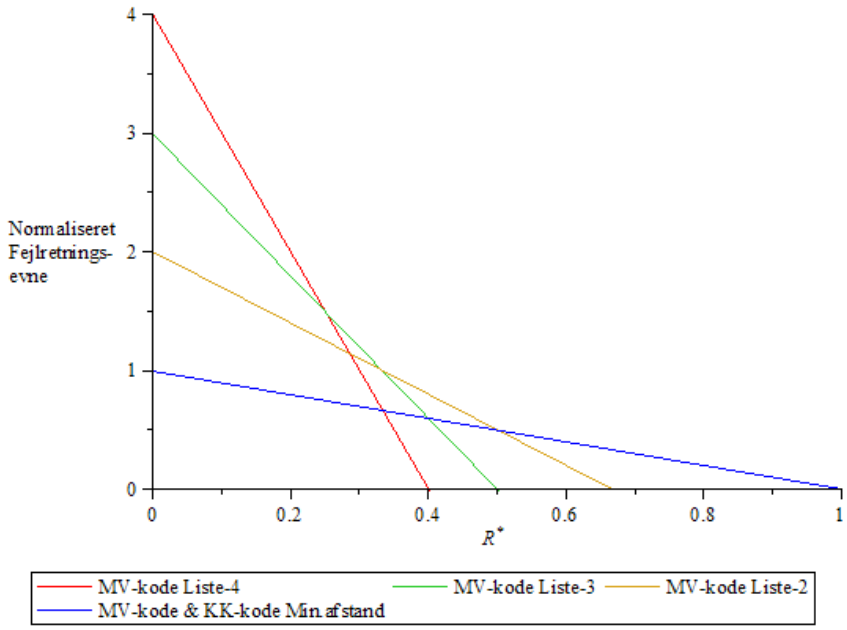
$$R^*_{KK} = \frac{k}{\ell} \, ,$$

og den normaliserede minimumsafstand

$$\delta_{KK} = \frac{2(\ell - k + 1)}{2\ell} = \frac{\ell - k + 1}{\ell} \to 1 - R^* \, ,$$

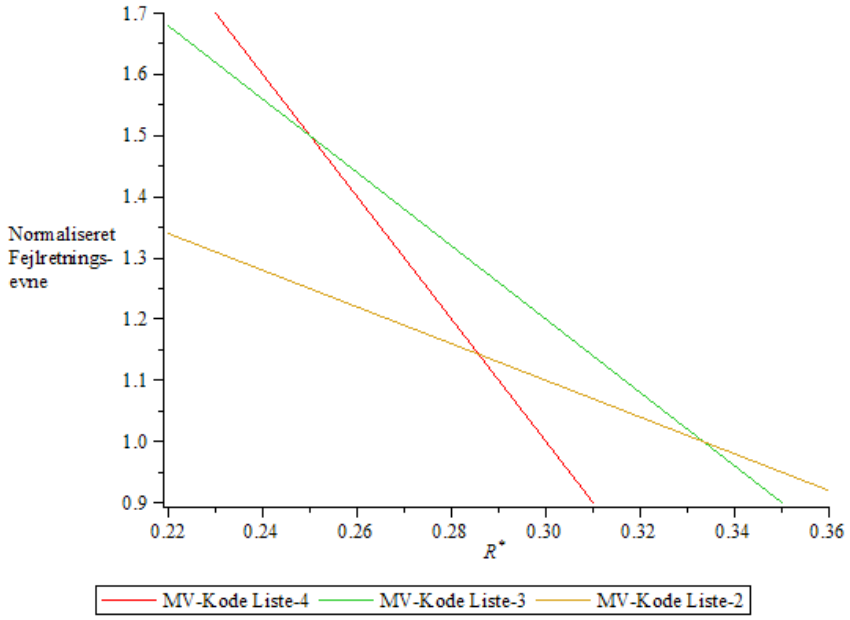
for $\ell \to \infty$.

Forholdene mellem de forskellige fejlretningsevner for KK-koden og MV-koden er illustreret på figur 9.1. Her er valgt kun at betragte liste-2-, liste-3- og liste-4-dekodning for MV-koden. Det ses, at fejlretningsevnen for MV-



Figur 9.1: Fejlretningsevnen ved minimumsafstandsdekodning for KK-kode og MV-kode, samt fejlretningsevnen for MV-kode ved liste-2-, liste-3- og liste-4-dekodning.

koden ved benyttelse af minimumsafstandsdekodning når fejlretningsevnen



Figur 9.2: Udsnit af figur 9.1 med MV-koderne af liste-2, liste-3 og liste-4.

for KK-koden. Ved pakkehastigheder $R^*_{MV} \leq \frac{1}{3}$ ses at der ved liste-L-dekodningen kan opnås en højere fejlretningsevne end hvis minimumsafstandsdekodning benyttes.

Figur 9.2 er et udsnit af figur 9.1 hvor kun fejlretningsevnen for liste-2-, liste-3- og liste-4-dekodning er illustreret. Det ses her at MV-koden liste-4 har den bedste fejlretningsevne for $R^*_{MV} < \frac{1}{4}$, hvorefter MV-koden liste-3 har bedst fejlretningsevne for $\frac{1}{4} < R^*_{MV} < \frac{1}{3}$. MV-koden liste-2 har den bedste fejlretningsevne for $R^*_{MV} > \frac{1}{3}$ blandt de 3 illusterede koder. Dette er som forventet jævnfør (9.22).

Kapitel 10

Opsamling

Vi har i denne specialeafhandling fokuseret på algebraisk netværkskodning med to indgangsvinkler; ønsket om at kunne optimere mængden af afsendt data i et netværk og ønsket om at kunne korrigere for fejl opstået i data under transmission.

I første del af rapporten, "Gröbner Baser og Deres Anvendelse i Netværkskodning", havde vi opstillet et netværkskodningsproblem. Dette bestod her i at bestemme om de nødvendige kommunikationsveje var tilgængelige i netværket, når vi ønskede at sende flere meddelelser til flere modtagere på en gang. Vi viste at multicast netværkskodningsproblemet havde en løsning hvis og kun hvis det tilhørende overgangspolynomium, som var konstrueret ud fra netværkets topologi, var forskelligt fra nul. Desuden havde det generelle netværkskodningsproblem en løsning hvis og kun hvis varieteten af idealet for det generelle netværkskodningsproblem var ikke-tom. Vi undersøgte yderligere successandsynligheden for at finde en løsning til netværkskodningsproblemet, både i tilfælde hvor netværkets topologi er kendt og ukendt. Det viste sig at successandsynlighed er højest når netværkets topologi er kendt.

I del II, "Fejlkorrigerende Netværkskodning", introducerede vi operatorkanalen. Denne var et udtryk for, at vi per antagelse intet kendskab havde til netværks topologien. Vi havde derfor heller ingen kendskab til, hvad der konkret var årsagen til eventuelle fejl i operatorkanalen. Netværkskodningsproblemet bestod derfor i at finde eller konstruere en kode, som var velegnet til fejlkorrigering ved modtagerenheden. Vi præsenterede KK-koden og MV-koden som er velegnet til fejlkorrigering ved henholdsvis minimumsafstandsdekodning og liste-L-dekodning. Det viste sig at med MV-koden kunne vi

opnå en bedre fejlretningsevne ved lave pakkehastigheder end KK-koden. Pakkehastigheden ved minimumsafstandsdekoderen var ens for KK-koden og MV-koden, så ved højere pakkehastigheder kan det være en fordel at benytte minimumsafstandsdekodning ved MV-koden i stedet for liste-L-dekodning.

Forbedring af Fejlretningsevnen for MV-Koden

H. Mahdavifar og A. Vardy har udgivet en anden artikel, [MV11], som optimere MV-kodens fejlretningsevne, således at liste-L-dekodning også giver en god fejlretningsevne ved højere pakkehastigheder. De introducerer multiplicitet i ringen af lineariserede polynomier, således at det er muligt med multiple rødder i de lineariserede polynomier. Dette gøres ved at definere en isomorfi mellem ringen af lineariserede polynomier over $\mathbb{F}_q$ og ringen af polynomier over $\mathbb{F}_q$. Idéen er så at afbillede det konstruerede interpolationspolynomium over i ringen af polynomier over $\mathbb{F}_q$. Her "gennemtvinges" multiple rødder, hvorefter det "nye" polynomium afbildes tilbage i ringen af lineariserede polynomier over $\mathbb{F}_q$. Vi har ikke beskæftiget os med dette, men for yderligere optimering af den fejlkorrigerende MV-koden (sammenlignet med denne rapport) er dette område en undersøgelse værd.

Litteratur

[Ber80] E.R. Berlekamp. *The Technology of Error-Correcting Codes.* Proceedings of the IEEE, Maj 1980.

[CLO92] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Springer, 3. Udgave, 1992.

[GT10] Olav Geil and Casper Thomsen. *Aspects of Random Network Coding.* 2010.

[HMK+06] Tracey Ho, Muriel Médard, Ralf Koetter, Davic R. Karger, Michelle Effros, Jun Shi, and Ben Leong. *A Random Linear Network Coding Approach to Multicast.* IEEE Transactions on Information Theory, Oktober 2006.

[KK08] Ralf Kötter and Frank R. Kschischang. *Coding for Errors and Erasures in Random Network Coding.* IEEE Transactions on Information Theory, `http://arxiv.org/abs/cs/0703061`, 2008.

[KM03] Ralf Koetter and Muriel Médard. *An Algebraic Approach to Network Coding.* IEEE/ACM Transactions, Oktober 2003.

[Lan02] Serge Lang. *Algebra.* Springer-Verlag, 3. Udgave, 2002.

[Mah12] Hessam Mahdavifar. *Privat korrespondance.* 3. maj 2012.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *Theory of Error-Correcting Codes.* North Holland, 8th impression, 1977.

[MV11] Hessam Mahdavifar and Alexander Vardy. *Algrbraic List-decoding of Subspace Codes with Multiplicities.* Forty-Ninth Annual Allerton Conference, September 2011.

[MV12] Hessam Mahdavifar and Alexander Vardy. *Algebraic List-Decoding of Subspace Codes.* `http://arxiv.org/abs/1202.0338`, 2. februar 2012.

[Sch09] Alexander Schrijver. *A Course in Combinatorial Optimization, Electronic Version.* Alexander Schrijver, 2009.

[XYS11] Hongmei Xie, Zhiyuan Yan, and Bruce W. Suter. *Generel Linearized Polynomial Interpolation and Its Applications.* Arxiv, April 2011.

Bilag A

Generelle Begreber fra Algebra

Dette bilag indeholder grundlæggende definitioner og lemmaer som danner baggrund for en del af den teori som er blevet præsenteret igennem projektrapporten. Disse er primært anvendt uden yderligere forklaring. Først defineres et ideal.

Definition A.1 (Ideal)**.** En delmængde $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ er et ideal hvis følgende betingelser er opfyldt;

(*i*) $0 \in \mathbf{I}$.

(*ii*) Hvis $f, g \in \mathbf{I}$ så gælder at $f + g \in \mathbf{I}$.

(*iii*) Hvis $f \in \mathbf{I}$ og $h \in \mathbb{F}[\mathbf{x}]$ så gælder at $hf \in \mathbf{I}$.

[CLO92, s.30]

I afsnit 2.4 benyttes de følgende tre definitioner inddirekte i beviset for proposition 2.21.

Definition A.2. Lad $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ være et ideal og $f, g \in \mathbb{F}[\mathbf{x}]$. Da siges f og g at være kongruente modulo $\mathbf{I}$, hvis $f - g \in \mathbf{I}$, dette skrive

$$f \equiv g \mod \mathbf{I}.$$

[CLO92, s.222]

Definition A.3 (Ækvivalensklasse)**.** Lad $\mathbf{I} \subset \mathbb{F}[\mathbf{x}]$ være et ideal og $f \in \mathbb{F}[\mathbf{x}]$. Da er ækvivalensklassen for f mængden

$$[f] = \{g \in \mathbb{F}[\mathbf{x}] \mid g \equiv f \mod \mathbf{I}\}.$$

[CLO92, s.222]

Definition A.4 (Kvotientring)**.** Kvotienten af $\mathbb{F}[\mathbf{x}]$ modulo $\mathbf{I}$ er mængden af ækvivalensklasser for kongruens modulo $\mathbf{I}$;

$$\mathbb{F}[\mathbf{x}]/\mathbf{I} = \{[f] \mid f \in \mathbb{F}[\mathbf{x}]\}.$$

[CLO92, s.223]

En helt grundlæggende egenskab i dette projekt er at være i stand til at ordne leddene i et polynomium. Derfor handler det følgende afsnit om dette.

A.1 Ordning af Led

Et polynomium $f \in \mathbb{F}[\mathbf{x}]$ består af en række led, hvor hvert led er et produkt af variablene i $\mathbf{x} = (x_1, \ldots, x_n)$. I mange situationer er det fordelagtigt at kunne ordne de indgående led i f på en entydig måde. Dette kunne f.eks. være i tilfælde hvor division mellem polynomier er impliceret eller ved sammenligning af polynomier. Til dette formål defineres følgende et monomium.

Definition A.5 (Monomium)**.** Et monomium $\mathbf{x}^\alpha \in \mathbb{F}[\mathbf{x}]$ et produkt af $x_1, \ldots, x_n$ givet ved

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n} \ ,$$

hvor $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

Fra ovenstående definition følger, at hvis et polynomium kun består af et enkelt led kaldes dette polynomium et monomium.

For at være i stand til at ordne leddene på en passende måde må vi kræve at ordningen er en total ordning. Det vil sige at for ethvert par af monomier $\mathbf{x}^\alpha, \mathbf{x}^\beta \in \mathbb{F}[\mathbf{x}]$ gælder kun et af følgende tilfælde;

$$\mathbf{x}^\alpha < \mathbf{x}^\beta \quad \text{eller} \quad \mathbf{x}^\alpha = \mathbf{x}^\beta \quad \text{eller} \quad \mathbf{x}^\alpha > \mathbf{x}^\beta \ .$$

Ligeledes kræves at ordningen er velordet. En ordning er velordnet hvis det er muligt at liste leddene i en aftagende følge, således at ordningen har et mindste element.

Lemma A.6. *En ordensrelation $>$ på $\mathbb{Z}_{\geq 0}^n$ er velordnet hvis og kun hvis enhver strengt aftagende følge på $\mathbb{Z}_{\geq 0}^n$ er endelig. [CLO92, s.55]*

Bevis. Vi antager kontra-positivt at $>$ ikke er velordnet hvis og kun hvis der findes en uendelig strengt aftagende følge i $\mathbb{Z}_{\geq 0}^n$. Hvis $>$ ikke er velordnet så må der findes en delmængde $S \subset \mathbb{Z}_{\geq 0}^n$ som ikke har noget mindste element. Vi vælger et element fra S kaldet $\alpha(1)$. Da $\alpha(1)$ ikke er det mindste element findes et andet element $\alpha(2) < \alpha(1)$ i S. Dette element er heller ikke det mindste element, så endnu et element fra S kan vælges $\alpha(3) < \alpha(2)$. Ved at fortsætte argumentationen på denne måde fås en uendelig stengt aftagende følge;

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots .$$

Omvendt gælder at hvis en uendelig strengt aftagende følge findes så er mængden $\{\alpha(1), \alpha(2), \alpha(3), \ldots\}$ en ikke-tom delmængde af $\mathbb{Z}_{\geq 0}^n$ som ikke indeholder noget mindste element. Heraf er $>$ ikke velordnet. □

Definition A.7 (Monomiel Ordning)**.** En monomiel ordning er en relation $>$ på $\mathbb{Z}_{\geq 0}^n$ som opfylder følgende betingelser;

(*i*) Relationen $>$ er en total ordning på $\mathbb{Z}_{\geq 0}^n$.

(*ii*) Lad $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$. Hvis $\alpha > \beta$ så gælder at $\alpha + \gamma > \beta + \gamma$.

(*iii*) Relationen $>$ er velordnet på $\mathbb{Z}_{\geq 0}^n$

[CLO92, s.55]

Bemærk at der er en en-til-en korrespondance mellem et monomium $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathbb{F}[\mathbf{x}]$ og n-tuplen $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Det vil sige at en monomiel ordning $>$ på $\mathbb{Z}_{\geq 0}^n$ tilsvarende giver en ordning af monomier i $\mathbb{F}[\mathbf{x}]$. Givet en monomiel ordning $>$ på $\mathbb{Z}_{\geq 0}^n$ og $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ hvor $\alpha > \beta$, haves derfor at for $\mathbf{x}^\alpha, \mathbf{x}^\beta \in \mathbb{F}[\mathbf{x}]$ er $\mathbf{x}^\alpha > \mathbf{x}^\beta$. Følgende defineres den Leksikografiske orden, som er en monomiel ordning.

Definition A.8 (Leksikografisk Orden)**.** Lad tuplerne $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$ være givet. Lad $\gamma = \alpha - \beta$. Hvis komponenten forskellig fra nul længst mod venstre i γ er positiv så siges $\alpha >_{\text{leks}} \beta$. [CLO92, s.56]

Proposition A.9. *Den Leksikografiske orden på $\mathbb{Z}_{\geq 0}^n$ er en monomiel ordning. [CLO92, s.57]*

Bevis. At den Leksikografiske ordning opfylder punkt (*i*)-(*iii*) fra definition A.7 ses følgende;

(*i*) Lad $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ og betragt $\gamma = \alpha - \beta$. Hvis den første ikke-nul komponent i γ er positiv følger af definition A.8 at $\alpha >_{\text{leks}} \beta$. Hvis den første ikke-nul komponent i γ er negativ følger ved ombytning af α og β at $\beta >_{\text{leks}} \alpha$, og hvis alle komponenterne i γ er nul, følger at $\alpha = \beta$. Heraf er den Leksikografiske ordning en total ordning.

(*ii*) Antag at $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ og at $\alpha >_{\text{leks}} \beta$. Så haves at ikke-nul komponenten længest mod venstre i $\gamma = \alpha - \beta$ er positiv. Lad denne komponent være γ_k. Lad $\zeta \in \mathbb{Z}^n_{\geq 0}$. Vi ønsker at vise at $\alpha + \zeta >_{\text{leks}} \beta + \zeta$. Dette ses ved $(\alpha + \zeta) - (\beta + \zeta) = \alpha - \beta = \gamma >_{\text{leks}} 0$. Per antagelse er ikke-nul komponenten længest mod venstre i γ givet ved $\gamma_k > 0$, hvorfor det ønskede er tilfældet.

(*iii*) Antag at $>_{\text{leks}}$ ikke er velordnet. Fra lemma A.6 findes så en uendelig strengt aftagende følge af elementer i $\mathbb{Z}^n_{\geq 0}$.

$$\alpha(1) >_{\text{leks}} \alpha(2) >_{\text{leks}} \alpha(3) >_{\text{leks}} \cdots$$

For alle $\alpha(i) \in \mathbb{Z}^n_{\geq 0}$ betragtes den første komponent. Fra definition A.8 haves at komponenterne former en ikke-voksende følge af ikke-negative heltal. Da $\mathbb{Z}_{\geq 0}$ er velordnet følger fra lemma A.6 at denne følge vil stabilisere på et tidspunkt ved et endeligt element. Der findes altså et k hvorom der gælder, at alle første komponenterne i $\alpha(i)$ for $i \geq k$ er ens. Betragt anden komponent i følgen fra $\alpha(k)$. Ved samme argument som ovenfor vil anden komponenterne stabiliseres på et tidspunkt, og der findes derfor et $k + j$ således at anden komponenterne (og første komponenterne) i $\alpha(i)$ for $i \geq k+j$ alle er ens. Ved at forsætte på denne måde indtil alle n komponenter er gennemløbet opnås elementer for $\ell \geq k+j$ i følgen $\alpha(\ell), \alpha(\ell+1), \ldots$ som alle er ens. Dette er en modstrid med antagelsen om at $\alpha(\ell) >_{\text{leks}} \alpha(\ell+1)$ og den Leksikografiske orden er derfor velordnet.

□

Eksempel A.10. Lad $f(x_1, x_2, x_3) \in \mathbb{F}[x_1, x_2, x_3]$ være givet ved

$$f(x_1, x_2, x_3) = x_1^3 x_2 x_3^2 + x_1 x_2^2 + 4 x_1 x_2 x_3^4 \, .$$

Polynomiet f indeholder tre led. Anvendes den Leksikografiske orden på $\mathbb{F}[x_1, x_2, x_3]$ fås at $x_1^3 x_2 x_3^2 >_{\text{leks}} x_1 x_2^2 >_{\text{leks}} 4 x_1 x_2 x_3^4$, da $(3,2,2) - (1,2,0) = (2,0,2)$ og $(1,2,0) - (1,1,4) = (0,1,-4)$ giver at $(3,2,2) >_{\text{leks}} (1,2,0) >_{\text{leks}} (1,1,4)$. ▲

Den monomielle ordning giver anledning til at definere det ledende monomium og den ledende koefficient, hvorfra det ledende led kan bestemmes.

Definition A.11. Lad en monomiel ordning $>$ være givet og lad $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha \in \mathbb{F}[\mathbf{x}]$ hvor $\alpha \in \mathbb{Z}^n_{\geq 0}$. Om funktionen f gælder at;

(*i*) Multigraden af f er givet ved

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

(*ii*) Den ledende koefficient af f er givet ved

$$\text{LC}(f) = a_{\text{multigrad}(f)} \in \mathbb{F} .$$

(*iii*) Det ledende monomium af f er givet ved

$$\text{LM}(f) = \mathbf{x}^{\text{multigrad}(f)} .$$

(*iv*) Det ledende led af f er givet ved

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f) .$$

[CLO92, s.59]

Multigraden af et produkt eller en sum af polynomier er givet i følgende lemma;

Lemma A.12. *Lad $f, g \in \mathbb{F}[\mathbf{x}]$ være ikke-nulpolynomier. Der gælder at*

(*i*) $\text{multigrad}(fg) = \text{multigrad}(f) + \text{multigrad}(g)$.

(*ii*) *Hvis $f+g \neq 0$ så gælder at* $\text{multigrad}(f+g) \leq \max\{\text{multigrad}(f), \text{multigrad}(g)\}$. *Hvis der specielt gælder at* $\text{multigrad}(f) \neq \text{multigrad}(g)$ *så opnås lighed.*

[CLO92, s.60]

Bevis. Lad $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha$ og lad $g = \sum_\beta b_\beta \mathbf{x}^\beta$. Definer mængden A til at indeholde alle $\alpha \in \mathbb{Z}^n_{\geq 0}$ hvor $a_\alpha \neq 0$ og definer mængden B til at indeholde alle $\beta \in \mathbb{Z}^n_{\geq 0}$ hvor $b_\beta \neq 0$. Vi beviser først del (*i*) og herefter (*ii*).

(*i*) Multigraden af fg kan bestemmes til

$$\begin{aligned} \text{multigrad}(fg) &= \max\left\{\alpha + \beta \in \mathbb{Z}^n_{\geq 0} | \alpha \in A, \beta \in B\right\} \\ &= \max\left\{\alpha \in \mathbb{Z}^n_{\geq 0} | \alpha \in A\right\} + \max\left\{\beta \in \mathbb{Z}^n_{\geq 0} | \beta \in B\right\} \\ &= \text{multigrad}(f) + \text{multigrad}(g) . \end{aligned}$$

(*ii*) Antag at $f+g \neq 0$. Der gælder så at

$$\begin{aligned}
\text{multigrad}(f+g) &= \max\Big\{\max\Big\{\alpha \in \mathbb{Z}^n_{\geq 0} | \alpha \in A \backslash B\Big\}, \\
&\qquad \max\Big\{\alpha \in \mathbb{Z}^n_{\geq 0} | \alpha \in (A \cap B)\Big\}, \\
&\qquad \max\Big\{\beta \in \mathbb{Z}^n_{\geq 0} | \beta \in B \backslash A\Big\}\Big\} \\
&\leq \max\Big\{\max\Big\{\alpha \in \mathbb{Z}^n_{\geq 0} | \alpha \in A \backslash B\Big\}, \qquad \text{(A.1)} \\
&\qquad \max\Big\{\beta \in \mathbb{Z}^n_{\geq 0} | \beta \in B \backslash A\Big\}\Big\} \\
&= \max\{\text{multigrad}(f), \text{multigrad}(g)\} \ .
\end{aligned}$$

Hvis f og g har samme multigrad, $\alpha_i = \beta_i$, risikere monomiet med denne multigrad i summen $f+g$ at forsvinde. Dette er tilfældet hvis $a_{\alpha_i} + b_{\beta_i} = 0$. Derfor er uligheden i (A.1) veldefineret.

□

Det følgende lemma benyttes i beviset hørende til sætning 2.14. Vi beviser det ikke, men henviser den interesserede læser til [CLO92].

Lemma A.13. *Lad en sum være givet ved*

$$\sum_{i=1}^{s} c_i f_i \text{ hvor } c_i \in \mathbb{F} \text{ og } \text{multigrad}(f_i) = \delta \text{ for alle } i \ .$$

Hvis $\text{multigrad}(\sum_{i=1}^{s} c_i f_i) < \delta$ *så er* $\sum_{i=1}^{s} c_i f_i$ *en linear kombination med koefficienter i* $\mathbb{F}$ *af S-polynomier* $S(f_j, f_k)$ *for* $1 \leq j, k \leq s$. *Desuden gælder at hvert S-polynomium har multigrad mindre end* δ. *[CLO92, s.84]*

Bilag B

Resultater fra Algebra

Dette bilag indeholder en divisionsalgoritme for en mængde af polynomier, Hilberts Basis Sætning og Hilberts Nullstellensatz. Alle tre emner er en del abstrakt algebra.

B.1 Divisionsalgoritme

Givet et polynomium $f \in \mathbb{F}[\mathbf{x}]$ og en mængde af polynomier $\{f_1, \ldots, f_t\} \in \mathbb{F}[\mathbf{x}]$ kan det være interessant at undersøge, hvorvidt polynomiet f kan udtrykkes ved en kombination af polynomierne $f_1, \ldots, f_t$. Divisionsalgoritmen, algoritme 6, kan anvendes til denne undersøgelse. Følgende sætning fastsætter egenskaberne ved Divisionsalgoritmen.

Sætning B.1. *Lad $F = (f_1, \ldots, f_t)$ og $f \in \mathbb{F}[\mathbf{x}]$ være givet. Algoritme 6 konstruerer polynomier $a_1, \ldots, a_t, r \in \mathbb{F}[\mathbf{x}]$ således at*

$$f = a_1 f_1 + \cdots + a_t f_t + r,$$

hvor r kaldes resten. Desuden gælder der, at ingen monomier i r er dividerbare med $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t)$.

Bevis. Det skal vises at der for ethvert skridt i algoritmen gælder, at

$$f = a_1 f_1 + \cdots + a_t f_t + p + r. \tag{B.1}$$

Dette er sandt for de angivne begyndelsesværdier af $a_1, \ldots, a_t, r$ og p i algoritme 6, idet der haves, at

$$f = a_1 f_1 + \cdots + a_t f_t + p + r = 0 f_1 + \cdots + 0 f_t + f + 0 = f.$$

Algoritme 6 Divisionsalgoritme i $\mathbb{F}[\mathbf{x}]$

Input: En ordnet t-tupel $F = (f_1, \ldots, f_t)$, et polynomium $f \in \mathbb{F}[\mathbf{x}]$, og en monomiel ordning $>$ på $\mathbb{Z}^n_{\geq 0}$.
Lad $a_1 := 0; \ldots; a_t = 0; r = 0; p := f$;
while $p \neq 0$ **do**
  $i := 1$; divisionstilfælde:=falsk;
  while $i \leq t$ **and** divisionstilfælde=falsk **do**
    if $\mathrm{LT}(f_i)$ dividerer $\mathrm{LT}(p)$ **then**
      $a_i := a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$;
      $p := p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$;
      divisionstilfælde:=sand;
    else
      $i := i + 1$;
    end if
  end while
  if divisionstilfælde=falsk **then**
    $r := r + \mathrm{LT}(p)$;
    $p := p - \mathrm{LT}(p)$;
  end if
end while
Output: Polynomier $a_1, \ldots, a_t, r$ hvor der gælder, at $f = a_1 f_1 + \cdots + a_t f_t + r$.

Det kan derfor antages at (B.1) holder for det første skridt i algoritme 6. Der er to muligheder for algoritmens næste skridt; divisionsskridt eller restskridt. Der ses først på tilfældet ved et divisionsskridt. Her gælder der, at $\mathrm{LT}(p)$ er dividerbar med et $\mathrm{LT}(f_i)$ og algoritmen forøger a_i med $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$ og formindsker p med $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$. Af dette ses, at

$$\left(a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}\right) f_i + \left(p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) = a_i f_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i + p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i = a_i f_i + p,$$

og hermed er summen $a_i f_i + p$ fra skridtet før uændret, og (B.1) gælder stadig efter et divisionsskridt. I tilfældet hvor næste skridt er et restskridt forøges resten r med $\mathrm{LT}(p)$ og polynomiet p formindskes med $\mathrm{LT}(p)$. Det vil sige at summen $p + r$ er uændret i (B.1), da

$$(p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p)) = p + r + \mathrm{LT}(p) - \mathrm{LT}(p) = p + r.$$

Ud fra dette er (B.1) uændret både efter et divisionsskridt og et restskridt, desuden gælder der at algoritme 6 stopper når $p = 0$ og herved fås, at

$$f = a_1 f_1 + \cdots + a_t f_t + r.$$

Der gælder at resten r kun forøges, når $\mathrm{LT}(p)$ ikke er dividerbar med nogle af $\mathrm{LT}(f_i)$'erne for $i \in \{1, \ldots, t\}$, og polynomierne $a_1, \ldots, a_t$ og r har derfor de ønskede egenskaber.

Det er nødvendigt at vise at algoritme 6 afsluttes på et tidspunkt. Dette gøres ud fra observationen at når p redefineres så formindskes multigraden af polynomiet p eller $p = 0$. For divisionsskridtet redefineres p til

$$p' = p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i. \tag{B.2}$$

For at se at multigraden af p falder ses der på det ledende led af $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$, og der fås følgende:

$$\begin{aligned}
\mathrm{LT}\left(\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i\right) &= \mathrm{LC}\left(\frac{\mathrm{LC}(p)\,\mathrm{LM}(p)}{\mathrm{LC}(f_i)\,\mathrm{LM}(f_i)} f_i\right) \mathrm{LM}\left(\frac{\mathrm{LC}(p)\,\mathrm{LM}(p)}{\mathrm{LC}(f_i)\,\mathrm{LM}(f_i)} f_i\right) \\
&= \frac{\mathrm{LC}(p)}{\mathrm{LC}(f_i)} \mathrm{LC}\left(\frac{\mathrm{LM}(p)}{\mathrm{LM}(f_i)} f_i\right) \mathrm{LM}\left(\frac{\mathrm{LC}(p)\,\mathrm{LM}(p)}{\mathrm{LC}(f_i)\,\mathrm{LM}(f_i)}\right) \mathrm{LM}(f_i) \\
&= \frac{\mathrm{LC}(p)}{\mathrm{LC}(f_i)} \mathrm{LC}\,(f_i)\, \frac{\mathrm{LM}(p)}{\mathrm{LM}(f_i)} \mathrm{LM}(f_i) \\
&= \frac{\mathrm{LC}(p)\,\mathrm{LM}(p)}{\mathrm{LC}(f_i)\,\mathrm{LM}(f_i)} \mathrm{LC}(f_i)\,\mathrm{LM}(f_i) \\
&= \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} \mathrm{LT}(f_i) = \mathrm{LT}(p).
\end{aligned} \tag{B.3}$$

Ud fra dette ses det at p og $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i$ har samme ledende led, så dette forsvinder i (B.2), hvorfor $\mathrm{multigrad}(p') < \mathrm{multigrad}(p)$ for $p' \neq 0$. Ved restskridtet redefineres p ved følgende

$$p' = p - \mathrm{LT}(p),$$

og det ses direkte, at $\mathrm{multigrad}(p') < \mathrm{multigrad}(p)$ for $p' \neq 0$. Heraf falder multigraden af p i begge tilfælde. Hvis ikke algoritmen afslutter fås en uendelig følge af aftagende multigrader for p, men da den monomielle ordning $>$ er velordnet, er dette ikke muligt i følge lemma A.6. Altså der er kun en endelig aftagende følge af multigrader, hvilket giver at $p = 0$ vil optræde på et tidspunkt og algoritmen afsluttes. □

Følgende korollar er en direkte konsekvens af Divisionsalgoritmen og sætning B.1

Korollar B.2. *Fastsæt en monomiel ordning $>$ på $\mathbb{Z}^n_{\geq 0}$ og lad $F = (f_1, \ldots, f_t)$ være en ordnet t-tupel af polynomier i $\mathbb{F}[\mathbf{x}]$. Så gælder der, at ethvert $f \in \mathbb{F}[\mathbf{x}]$ kan skrives som*

$$f = a_1 f_1 + \cdots + a_t f_t + r, \tag{B.4}$$

hvor $a_i, r \in \mathbb{F}[\mathbf{x}]$. Der gælder enten, at $r = 0$, eller at r er en linear kombination af monomier med koefficienter i $\mathbb{F}$. Der gælder for monomierne i r, at ingen af disse er dividerbare med $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t)$. Polynomiet r kaldes en rest af f ved division med F. Der gælder desuden at hvis $a_i f_i \neq 0$ så haves at

$$\text{multigrad}(f) \geq \text{multigrad}(a_i f_i). \tag{B.5}$$

[CLO92, s.64]

Bevis. At der findes $a_1, \ldots, a_t$ og r der opfylder (B.4) følger af sætning B.1, og ud fra dette har r også de ønskede egenskaber. Det er derfor kun nødvendigt at undersøge forholdet mellem multigrad(f) og multigrad$(a_i f_i)$. Ethvert led i a_i er af formen $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$ for en eller anden værdi af p. Der gælder fra algoritme 6, at $p = f$ som startværdi og ifølge sætning B.1 gælder der at multigraden af p falder. Det vil sige, at $\mathrm{LT}(p) \leq \mathrm{LT}(f)$. Fra (B.3) fås at $\mathrm{LT}(a_i f_i) = \mathrm{LT}(p)$ for et eller andet p, og heraf at $\mathrm{LT}(a_i f_i) \leq \mathrm{LT}(f)$. Ud fra dette og definition A.11 fås, at multigrad$(a_i f_i) \leq$ multigrad(f). □

Bemærkning B.3. Ulighed (B.5) følger også direkte ved anvendelse af lemma A.12.

B.2 Hilberts Basis Sætning

Hilberts Basis Sætning giver et fundamentalt resultat vedrørende idealer.

Sætning B.4 (Hilberts Basis Sætning)**.** *Ethvert ideal $\mathbf{I} \in \mathbb{F}[\mathbf{x}]$ har en endelig frembringende mængde. Det vil sige $\mathbf{I} = \langle f_1, \ldots, f_t \rangle$ for nogle $f_1, \ldots, f_t \in \mathbf{I}$. [CLO92, s.76]*

Bevis. Hvis $\mathbf{I} = \langle 0 \rangle$ vælges $\{0\}$ som den endelige frembringende mængde og sætningen er sand. Det antages derfor at $\mathbf{I}$ indeholder mindst et ikke-nulpolynomium. Fra proposition 3 [CLO92, s.76] gælder der, at der findes polynomier $f_1, \ldots, f_t \in \mathbf{I}$ således at $\langle \mathrm{LT}(f_1), \ldots \mathrm{LT}(f_t) \rangle = \langle \mathrm{LT}(\mathbf{I}) \rangle$. Heraf ønskes at udlede at $\langle f_1, \ldots, f_t \rangle = \mathbf{I}$. Der gælder direkte at $\langle f_1, \ldots, f_t \rangle \subset \mathbf{I}$, da $f_i \in \mathbf{I}$ for $i \in \{1, \ldots, t\}$.

Lad $f \in \mathbf{I}$. Ved brug af divisionsalgoritmen, algoritme 6, fås at f kan udtrykkes ved

$$f = a_1 f_1 + \cdots + a_t f_t + r.$$

Her gælder der, at r ikke er dividerbar med nogle af $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t)$ fra korollar B.2. Desuden gælder, at

$$r = f - a_1 f_1 - \cdots - a_t f_t \in \mathbf{I}.$$

Hvis $r \neq 0$ så gælder der, at $\mathrm{LT}(r) \in \langle \mathrm{LT}(\mathbf{I}) \rangle = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle$, hvilket betyder at $\mathrm{LT}(r)$ er dividerbar med et $\mathrm{LT}(f_i)$, men så kan r ikke være resten jævnfør det ovennævnte. Der gælder altså at $r = 0$ og heraf at

$$f = a_1 f_1 + \cdots + a_t f_t + 0 \in \langle f_1, \ldots, f_t \rangle$$

for alle $f \in \mathbf{I}$, hvorfor $\mathbf{I} \subset \langle f_1, \ldots, f_t \rangle$. Derfor må ethvert ideal $\mathbf{I}$ have en endelig frembringende mængde. □

Et andet interessant resultat om idealer omhandler en stigende kæde af idealer.

Sætning B.5 (Stigende Kæde)**.** *Lad*

$$\mathbf{I}_1 \subset \mathbf{I}_2 \subset \mathbf{I}_3 \subset \cdots , \tag{B.6}$$

være en stigende kæde af idealer i $\mathbb{F}[\mathbf{x}]$*. Så findes et* $N \geq 1$ *således at*

$$\mathbf{I}_N = \mathbf{I}_{N+1} = \mathbf{I}_{N+2} = \cdots .$$

[CLO92, s.78]

Bevis. Lad den stigende kæde i (B.6) være givet og lad $\mathbf{I} = \bigcup_{i=1}^{\infty} \mathbf{I}_i$. Da er $\mathbf{I}$ også et ideal i $\mathbb{F}[\mathbf{x}]$ hvilket ses ved anvendelse af definition A.1;

(*i*) Der gælder at $0 \in \mathbf{I}$, da $0 \in \mathbf{I}_i$ for alle i.

(*ii*) Antag at $f, g \in \mathbf{I}$, så gælder per definition af $\mathbf{I}$ at $f \in \mathbf{I}_i$ og $g \in \mathbf{I}_j$ for nogle i og j. Da (B.6) er en stigende kæde må gælde at $i \geq j$ eller $j \geq i$, så ved en evt. ombytning af indeks fås at $\mathbf{I}_i \subset \mathbf{I}_j$, så både f og g er indeholdt i $\mathbf{I}_j$. Da $\mathbf{I}_j$ er et ideal gælder at $f + g \in \mathbf{I}_j$ hvorfor $f + g \in \mathbf{I}$.

(*iii*) Antag at $f \in \mathbf{I}$ og at $r \in \mathbb{F}[\mathbf{x}]$, så gælder som ovenstående at $f \in \mathbf{I}_i$ for nogle i, hvorved $r \cdot f \in \mathbf{I}_i \subset \mathbf{I}$.

Da $\mathbf{I}$ er et ideal følger af Hilberts Basis Sætning B.4 at $\mathbf{I}$ har en endelig frembringende mængde; $\mathbf{I} = \langle f_1, \ldots, f_s \rangle$. Fra konstruktionen af $\mathbf{I}$ vides at hvert af disse frembringere f_i er indeholdet i et af idealerne i den stigende kæde (B.6). Antag at for $i \in \{1, \ldots, s\}$ haves at $f_i \in \mathbf{I}_{j_i}$. Lad $N = \max\{j_1, \ldots, j_s\}$ så følger at $f_i \in \mathbf{I}_N$ for alle $i \in \{1, \ldots, s\}$. Vi har så at

$$\mathbf{I} = \langle f_1, \ldots, f_s \rangle \subset \mathbf{I}_N \subset \mathbf{I}_{N+1} \subset \cdots \subset \mathbf{I}$$

Heraf følger at den stigende kæde stabiliseres således at for et $N \geq 1$ gælder at $\mathbf{I}_N = \mathbf{I}_{N+1} = \cdots$. □

B.3 Hilberts Nullstellensatz

I afsnit 2.4 er definitionen for varieteten af et ideal givet. De følgende sætninger knytter en sammenhæng mellem varieteten af et ideal og de polynomier som frembringer idealet.

Proposition B.6 (Den svage Nullstellensatz)**.** *Lad* $\overline{\mathbb{F}}$ *være et algebraisk aflukket legeme og* $\mathbf{I} \subseteq \overline{\mathbb{F}}[\mathbf{x}]$ *være et ideal der opfylder, at* $\mathbf{V}(\mathbf{I}) = \emptyset$*. Så gælder der, at* $\mathbf{I} = \overline{\mathbb{F}}[\mathbf{x}]$*. [CLO92, s.170]*

For beviset af den svage Nullstellensatz henvises den interesserede læser til [CLO92].

Sætning B.7. *Lad* $\mathbf{I} \subseteq \mathbb{F}[\mathbf{x}]$ *være et ideal. Så gælder der, at* $1 \in \mathbf{I}$ *hvis og kun hvis* $\mathbf{V}(\mathbf{I}) = \emptyset$*.*

Bevis. Antag, at $1 \in \mathbf{I}$ så gælder der direkte at $\mathbf{V}(\mathbf{I}) = \emptyset$, da et konstant polynomium ingen nulpunkter har.

Antag omvendt, at $\mathbf{V}(\mathbf{I}) = \emptyset$ så fås af den svage Nullstellensatz at $\mathbf{I} = \mathbb{F}[\mathbf{x}]$, hvilket vil sige at $1 \in \mathbf{I}$. □

Bilag C

Grafteori

Opstillingen af et netværkskodningsproblem givet i definition 3.1 bygger på en grafrepræsentation af det givne netværk. I det følgende gives derfor et udpluk af den bagvedliggende grafteori som benyttes i kapitel 3 og kapitel 4.

C.1 Minimum Snit Maximum Flow

Vi præsenterer Minimum Snit Maximum Flow sætningen. Denne benyttes i afsnit 3.1.1 til at konkludere, at der skal bruges h disjunkte veje for at sende h meddelelser. Før minimum snit maximum flow sætningen gives defineres først grundlæggende begreber fra grafteorien vedrørende netværker. Her defineres først et snit og et $s-r$ snit.

Definition C.1 (Snit)**.** Lad $G = (V, E)$ være en graf og $\{V_1, V_2\}$ være en opdeling af V. Da kaldes $E(V_1, V_2)$, som er mængden af kanter mellem V_1 og V_2, et snit.

For $s, r \in V$, er et $s-r$ snit er en mængde $E' \subset E$, hvor $E' = \text{ud}(U)$ for en mængde $U \subset V$, hvor $s \in U$ men $r \notin U$.

Følgende proposition giver forholdet mellem disjunkte veje og snit i et netværk.

Proposition C.2 (Mengers Sætning)**.** *Lad $G = (V, E)$ været en orienteret graf og lad $s, r \in V$. Så er det maksimale antal $s-r$ disjunkte veje lig med den mindste $s-r$ snit. [Sch09, Korollar 4.1b]*

C.1. MINIMUM SNIT MAXIMUM FLOW

For at beskrive hvor meget information der kan sendes over hver kant i netværket tales der om kapacitet. Kapacitetsfunktionen for et netværk er givet ved $c : E \to \mathbb{R}_+$. Denne afbilledes her over i de positive reelle tal, da en kant med kapacitet nul kan betragtes som en kanal hvor intet kan sendes over. Denne kant kan da ignoreres i det givne netværk. Kapaciteten af et $s - r$ snit er givet ved

$$c(\mathrm{ud}(U)) = \sum_{e \in \mathrm{ud}(U)} c(e) \ .$$

For at beskrive den information der skal sendes mellem s og r haves et $s-r$ flow, som er en funtion $f : E \to \mathbb{R}$ med egenskaberne

1. $f(e) \geq 0$ for alle $e \in E$,
2. $\sum_{e \in \mathrm{ind}(v)} f(e) = \sum_{e \in \mathrm{ud}(v)} f(e)$ for alle $v \in V \backslash \{s, r\}$.

Den samlede mængde af flow i et netværk beskrives ved værdien af et flow, som er givet ved

$$\mathrm{value}(f) = \sum_{e \in \mathrm{ud}(s)} f(e) - \sum_{e \in \mathrm{ind}(s)} f(e) \ .$$

Et $s - r$ flow f siges at være under kapacitetsfunktionen c, hvis der gælder, at $f(e) \leq c(e)$ for alle $e \in E$.

Sætning C.3 (Minimum Snit Maximum Flow)**.** *For en orienteret graf $G = (V, E)$, med punkter $s, r \in V$ og kapacitetsfunktion $c : E \to \mathbb{R}_+$ er den maksimale værdi af et $s - r$ flow under c lig med den mindste kapacitet af et $s - r$ snit. [Sch09, Sætning 4.2]*

Der gælder at den mindste kapacitet af et snit kan betragtes som det mindste snit i netværket, hvis vi antager at alle kanter har enhedskapacitet. Af proposition C.2 fås derfor at den maksimale værdi af et $s - r$ flow er lig med antallet af disjunkte veje mellem s og r. Desuden gælder der, at den maksimale værdi af et flow er lig den største mængde af information der kan sendes igennem netværket. Heraf følger det, at hvis der i alt haves h disjunkte veje i netværket mellem s og r så kan der højest sendes h beskeder.

Bilag D

Eksempler

Dette bilag indeholder en gennemgang af metoder brugt i eksempler i hovedteksten. Desuden haves også Gröbner-basen hørende til eksempel 4.4.

Eksempel D.1 (Udregning af Gröbner-basis ved Maple)**.** Lad idealet $\mathbf{I} = \langle x + 2y, 3y^2 + z, y^2 \rangle$ i $\mathbb{F}[x, y, z]$ være givet. Vi ønsker at bestemme en Gröbner-basis for $\mathbf{I}$ når der haves en leksikografisk ordning med $x >_{\text{leks}} y >_{\text{leks}} z$. Dette gøres ved hjælp af Maple ved følgende kode;

Definition af polynomierne i idealet $\mathbf{I}$
[> $f_1 := x + 2 \cdot y$
[> $f_2 := 3 \cdot y^2 + z$
[> $f_3 := y^2$
Pakke til at bestemme den reducerede Gröbner-basis
[> $with\{Groebner\}$:
Mængden for hvilken basen ønskes fundet
[> $B := \{f_1, f_2, f_3\}$
Ordningen af de variable x, y, z
[> $T := plex(x, y, z)$
Gröbner-basen bestemmes ved funktionen $Basis$
[> $GB := Basis(B, T)$

$$GB := [x + 2y, y^2, z]$$

Det vil sige at Gröbner-basen for idealet $\mathbf{I}$ er $\{x + 2y, y^2, z\}$. ▲

Eksempel D.2 (Gröbner-basen hørende til eksempel 4.4)**.** I dette eksempel gives de 34 polynomier i Gröbner-basen fra eksempel 4.4.

$q_1 = -f_{47}f_{78}f_{59} + f_{47}f_{79}f_{58},$
$q_2 = f_{68}f_{37}f_{58}f_{79}^2 - f_{68}f_{37}f_{59}f_{79}f_{78} - f_{69}f_{37}f_{58}f_{79}f_{78} + f_{69}f_{37}f_{59}f_{78}^2,$
$q_3 = a_{42},$
$q_4 = a_{35}f_{58}f_{79} - a_{35}f_{59}f_{78},$
$q_5 = a_{32}f_{24}f_{47}f_{79} + a_{35}f_{59},$
$q_6 = a_{32}f_{24}f_{47}f_{78} + a_{35}f_{58},$
$q_7 = a_{23},$
$q_8 = f_{68}f_{37}a_{21}f_{79} - f_{69}f_{37}a_{21}f_{78},$
$q_9 = f_{37}a_{21}f_{79}f_{47},$
$q_{10} = f_{37}a_{21}f_{78}f_{47},$
$q_{11} = a_{21}f_{14},$
$q_{12} = a_{35}f_{37}a_{21},$
$q_{13} = a_{16}f_{68}f_{79} - a_{16}f_{69}f_{78},$
$q_{14} = a_{16}f_{47},$
$q_{15} = a_{16}a_{35},$
$q_{16} = -a_{26}a_{45}c_0b_{31}a_{16}f_{68}^2f_{59}^2b_{96}b_{88}b_{43}a_{32}f_{24} + 2a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}f_{59}f_{58}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}f_{69}^2f_{58}^2b_{96}b_{88}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{31}a_{16}f_{68}^2f_{59}^2b_{98}b_{86}b_{43}a_{32}f_{24} - 2a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}f_{59}f_{58}b_{98}b_{86}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{31}a_{16}f_{69}^2f_{58}^2b_{98}b_{86}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}f_{68}^2f_{59}^2b_{96}b_{88}b_{41}a_{32}f_{24} - 2a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}f_{59}f_{58}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}f_{69}^2f_{58}^2b_{96}b_{88}b_{41}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}f_{68}^2f_{59}^2b_{98}b_{86}b_{41}a_{32}f_{24} + 2a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}f_{59}f_{58}b_{98}b_{86}b_{41}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}f_{69}^2f_{58}^2b_{98}b_{86}b_{41}a_{32}f_{24} - f_{37}f_{58}f_{79} + f_{37}f_{59}f_{78},$
$q_{17} = a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}a_{21}f_{59}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}f_{69}^2a_{21}f_{58}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}a_{21}f_{59}b_{98}b_{86}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{31}a_{16}f_{69}^2a_{21}f_{58}b_{98}b_{86}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}a_{21}f_{59}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}f_{69}^2a_{21}f_{58}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}a_{21}f_{59}b_{98}b_{86}b_{41}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}f_{69}^2a_{21}f_{58}b_{98}b_{86}b_{41}a_{32}f_{24} - f_{37}a_{21}f_{79},$
$q_{18} = a_{26}a_{45}c_0b_{31}a_{16}f_{68}^2a_{21}f_{59}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}a_{21}f_{58}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}f_{68}^2a_{21}f_{59}b_{98}b_{86}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}a_{21}f_{58}b_{98}b_{86}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}f_{68}^2a_{21}f_{59}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}a_{21}f_{58}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}f_{68}^2a_{21}f_{59}b_{98}b_{86}b_{41}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}a_{21}f_{58}b_{98}b_{86}b_{41}a_{32}f_{24} - f_{37}a_{21}f_{78},$
$q_{19} = a_{26}a_{45}c_0b_{31}a_{16}^2f_{69}f_{68}f_{59}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}^2f_{69}^2f_{58}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}^2f_{69}f_{68}f_{59}b_{98}b_{86}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{31}a_{16}^2f_{69}^2f_{58}b_{98}b_{86}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}^2f_{69}f_{68}f_{59}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}^2f_{69}^2f_{58}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}^2f_{69}f_{68}f_{59}b_{98}b_{86}b_{41}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}^2f_{69}^2f_{58}b_{98}b_{86}b_{41}a_{32}f_{24} - a_{16}f_{37}f_{79},$
$q_{20} = a_{26}a_{45}c_0b_{31}a_{16}^2f_{68}^2f_{59}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}^2f_{69}f_{68}f_{58}b_{96}b_{88}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{31}a_{16}^2f_{68}^2f_{59}b_{98}b_{86}b_{43}a_{32}f_{24} + a_{26}a_{45}c_0b_{31}a_{16}^2f_{69}f_{68}f_{58}b_{98}b_{86}b_{43}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}^2f_{68}^2f_{59}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}^2f_{69}f_{68}f_{58}b_{96}b_{88}b_{41}a_{32}f_{24} + a_{26}a_{45}c_0b_{33}a_{16}^2f_{68}^2f_{59}b_{98}b_{86}b_{41}a_{32}f_{24} - a_{26}a_{45}c_0b_{33}a_{16}^2f_{69}f_{68}f_{58}b_{98}b_{86}b_{41}a_{32}f_{24} -$

$a_{16}f_{37}f_{78}$,
$q_{21} = f_{37}f_{58}a_{13}f_{79} - f_{37}f_{59}a_{13}f_{78} - a_{16}f_{68}f_{59} + a_{16}f_{69}f_{58}$,
$q_{22} = a_{26}a_{45}c_0b_{31}a_{35}f_{68}f_{59}^2b_{98}b_{86}b_{43}a_{13}f_{79}+f_{47}f_{79}^2-a_{26}a_{45}c_0b_{31}f_{69}f_{59}^2b_{98}b_{86}b_{43}a_{13}a_{35}f_{78}-$
$f_{79}a_{26}a_{45}c_0b_{31}a_{35}f_{68}f_{59}^2b_{96}b_{88}b_{43}a_{13} + a_{26}a_{45}c_0b_{31}f_{69}f_{59}^2b_{96}b_{88}b_{43}a_{13}a_{35}f_{78} +$
$f_{79}a_{26}a_{45}c_0b_{33}a_{35}f_{68}f_{59}^2b_{96}b_{88}b_{41}a_{13} - a_{26}a_{45}c_0b_{33}f_{69}f_{59}^2b_{96}b_{88}b_{41}a_{13}a_{35}f_{78} -$
$f_{79}a_{26}a_{45}c_0b_{33}a_{35}f_{68}f_{59}^2b_{98}b_{86}b_{41}a_{13} + a_{26}a_{45}c_0b_{33}f_{69}f_{59}^2b_{98}b_{86}b_{41}a_{13}a_{35}f_{78}$,
$q_{23} = a_{26}a_{45}c_0b_{31}a_{35}f_{68}f_{59}^2b_{96}b_{88}b_{43}a_{13}-a_{26}a_{45}c_0b_{31}a_{35}f_{69}f_{59}f_{58}b_{96}b_{88}b_{43}a_{13}-$
$a_{26}a_{45}c_0b_{31}a_{35}f_{68}f_{59}^2b_{98}b_{86}b_{43}a_{13} + a_{26}a_{45}c_0b_{31}a_{35}f_{69}f_{59}f_{58}b_{98}b_{86}b_{43}a_{13} -$
$a_{26}a_{45}c_0b_{33}a_{35}f_{68}f_{59}^2b_{96}b_{88}b_{41}a_{13} + a_{26}a_{45}c_0b_{33}a_{35}f_{69}f_{59}f_{58}b_{96}b_{88}b_{41}a_{13} +$
$a_{26}a_{45}c_0b_{33}a_{35}f_{68}f_{59}^2b_{98}b_{86}b_{41}a_{13}-a_{26}a_{45}c_0b_{33}a_{35}f_{69}f_{59}f_{58}b_{98}b_{86}b_{41}a_{13}-f_{47}f_{79}$,
$q_{24} = a_{26}a_{45}c_0b_{31}a_{35}f_{68}f_{59}f_{58}b_{96}b_{88}b_{43}a_{13}-a_{26}a_{45}c_0b_{31}a_{35}f_{69}f_{58}^2b_{96}b_{88}b_{43}a_{13}-$
$a_{26}a_{45}c_0b_{31}a_{35}f_{68}f_{59}f_{58}b_{98}b_{86}b_{43}a_{13} + a_{26}a_{45}c_0b_{31}a_{35}f_{69}f_{58}^2b_{98}b_{86}b_{43}a_{13} -$
$a_{26}a_{45}c_0b_{33}a_{35}f_{68}f_{59}f_{58}b_{96}b_{88}b_{41}a_{13} + a_{26}a_{45}c_0b_{33}a_{35}f_{69}f_{58}^2b_{96}b_{88}b_{41}a_{13} +$
$a_{26}a_{45}c_0b_{33}a_{35}f_{68}f_{59}f_{58}b_{98}b_{86}b_{41}a_{13}-a_{26}a_{45}c_0b_{33}a_{35}f_{69}f_{58}^2b_{98}b_{86}b_{41}a_{13}-f_{47}f_{78}$,
$q_{25} = c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{88}a_{26}f_{68}b_{96}a_{45}f_{59}+1-c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{96}a_{26}f_{69}b_{88}a_{45}f_{58}-$
$c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{86}a_{26}f_{68}b_{98}a_{45}f_{59} + c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{98}a_{26}f_{69}b_{86}a_{45}f_{58} -$
$c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{88}a_{26}f_{68}b_{96}a_{45}f_{59} + c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{96}a_{26}f_{69}b_{88}a_{45}f_{58} +$
$c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{86}a_{26}f_{68}b_{98}a_{45}f_{59} - c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{98}a_{26}f_{69}b_{86}a_{45}f_{58}$,
$q_{26} = -f_{37}f_{79}-a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}f_{59}b_{98}b_{86}b_{43}a_{32}f_{24}+a_{26}a_{45}c_0b_{31}a_{16}f_{69}^2f_{58}b_{98}b_{86}b_{43}a_{32}f_{24}+$
$c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{86}a_{26}f_{68}b_{98}a_{45}f_{59}f_{37}f_{79}-a_{26}a_{45}c_0b_{31}f_{69}f_{59}b_{98}b_{86}b_{43}f_{37}a_{13}a_{32}f_{78}f_{24}-$
$f_{37}a_{13}a_{32}f_{79}f_{24}a_{26}a_{45}c_0b_{31}f_{68}f_{59}b_{96}b_{88}b_{43}+a_{26}a_{45}c_0b_{31}f_{69}f_{59}b_{96}b_{88}b_{43}f_{37}a_{13}a_{32}f_{78}f_{24}+$
$a_{26}a_{45}c_0b_{31}a_{16}f_{69}f_{68}f_{59}b_{96}b_{88}b_{43}a_{32}f_{24}-a_{26}a_{45}c_0b_{31}a_{16}f_{69}^2f_{58}b_{96}b_{88}b_{43}a_{32}f_{24}+$
$f_{37}f_{79}c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{88}a_{26}f_{68}b_{96}a_{45}f_{59}-a_{26}a_{45}c_0b_{33}f_{69}f_{59}b_{96}b_{88}b_{41}f_{37}a_{13}a_{32}f_{78}f_{24}-$
$a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}f_{59}b_{96}b_{88}b_{41}a_{32}f_{24}+a_{26}a_{45}c_0b_{33}a_{16}f_{69}^2f_{58}b_{96}b_{88}b_{41}a_{32}f_{24}-$
$f_{37}f_{79}c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{86}a_{26}f_{68}b_{98}a_{45}f_{59}+a_{26}a_{45}c_0b_{33}f_{69}f_{59}b_{98}b_{86}b_{41}f_{37}a_{13}a_{32}f_{78}f_{24}+$
$a_{26}a_{45}c_0b_{33}a_{16}f_{69}f_{68}f_{59}b_{98}b_{86}b_{41}a_{32}f_{24}-a_{26}a_{45}c_0b_{33}a_{16}f_{69}^2f_{58}b_{98}b_{86}b_{41}a_{32}f_{24}$,
$q_{27} = -a_{35}f_{79}c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{88}a_{26}f_{68}b_{96}a_{45}f_{59}+a_{35}f_{79}c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{88}a_{26}f_{68}b_{96}a_{45}f_{59}-$
$c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{96}a_{26}f_{69}b_{88}a_{45}a_{35}f_{59}f_{78}-a_{35}f_{79}c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{86}a_{26}f_{68}b_{98}a_{45}f_{59}+$
$c_0a_{32}f_{24}b_{41}a_{13}b_{33}b_{98}a_{26}f_{69}b_{86}a_{45}a_{35}f_{59}f_{78}-c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{98}a_{26}f_{69}b_{86}a_{45}a_{35}f_{59}f_{78}+$
$a_{26}a_{45}c_0b_{31}f_{69}b_{96}b_{88}b_{43}a_{13}a_{32}f_{24}a_{35}f_{59}f_{78}+c_0a_{32}f_{24}b_{43}a_{13}b_{31}b_{86}a_{26}f_{68}b_{98}a_{45}f_{59}a_{35}f_{79}-$
$a_{35}f_{79}$,
$q_{28} = f_{37}a_{21}a_{13}f_{79} + a_{16}f_{69}a_{21}$,
$q_{29} = f_{37}a_{21}a_{13}f_{78} + a_{16}f_{68}a_{21}$,
$q_{30} = a_{16}f_{37}a_{13}f_{79} + a_{16}^2f_{69}$,
$q_{31} = a_{16}f_{37}a_{13}f_{78} + a_{16}^2f_{68}$,
$q_{32} = a_{11}f_{14}f_{47}f_{79} + a_{13}f_{37}f_{79} + a_{16}f_{69}$,
$q_{33} = a_{11}f_{14}f_{47}f_{78} + a_{13}f_{37}f_{78} + a_{16}f_{68}$,
$q_{34} = a_{11}a_{35}f_{14}-c_0a_{32}^2f_{24}^2b_{41}a_{13}^2b_{33}b_{98}a_{26}f_{69}b_{86}a_{45}f_{37}f_{78}+c_0a_{32}^2f_{24}^2b_{41}a_{13}^2b_{33}b_{96}a_{26}f_{69}b_{88}a_{45}f_{37}f_{78}+$
$c_0a_{32}^2f_{24}^2b_{43}a_{13}^2b_{31}b_{98}a_{26}f_{69}b_{86}a_{45}f_{37}f_{78}-c_0a_{32}^2f_{24}^2b_{43}a_{13}^2b_{31}b_{96}a_{26}f_{69}b_{88}a_{45}f_{37}f_{78}+$
$c_0a_{32}^2f_{24}^2b_{41}a_{13}^2b_{33}b_{86}a_{26}f_{68}b_{98}a_{45}f_{37}f_{79}-c_0a_{32}^2f_{24}^2b_{41}a_{13}^2b_{33}b_{88}a_{26}f_{68}b_{96}a_{45}f_{37}f_{79}-$
$c_0a_{32}^2f_{24}^2b_{43}a_{13}^2b_{31}b_{86}a_{26}f_{68}b_{98}a_{45}f_{37}f_{79}+f_{37}a_{13}^2a_{32}^2f_{79}f_{24}^2c_0b_{43}b_{31}b_{88}a_{26}f_{68}b_{96}a_{45}$

Potens af α	Polynomium	-	Potens af α	Polynomium
α^0	1		α^{16}	x^3+x^2
α^1	x		α^{17}	x^4+x^3
α^2	x^2		α^{18}	x^4+x^3+1
α^3	x^3		α^{19}	x^4+x^3+x+1
α^4	x^4		α^{20}	$x^4+x^3+x^2+x+1$
α^5	x^3+1		α^{21}	x^4+x^2+x+1
α^6	x^4+x		α^{22}	x^2+x+1
α^7	x^3+x^2+1		α^{23}	x^3+x^2+x
α^8	x^4+x^3+x		α^{24}	$x^4+x^3+x^2$
α^9	$x^4+x^3+x^2+1$		α^{25}	x^4+1
α^{10}	x^4+x+1		α^{26}	x^3+x+1
α^{11}	x^3+x^2+x+1		α^{27}	x^4+x^2+x
α^{12}	$x^4+x^3+x^2+x$		α^{28}	x^2+1
α^{13}	x^4+x^2+1		α^{29}	x^3+x
α^{14}	$x+1$		α^{30}	x^4+x^2
α^{15}	x^2+x		α^{31}	1

Tabel D.1: Elementer i $\mathbb{F}_{2^5}$.

D.1 Konstruktion af $\mathbb{F}_{2^5}$

I flere eksempler er fejlkorrigerende koder konstrueret over legemet $\mathbb{F}_{2^5}$. Vi konstruerer her $\mathbb{F}_{2^5}$ over det irreducible polynomium $x^5+x^3+1 \in \mathbb{F}_2[x]$, således at $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/\langle x^5+x^3+1\rangle$. Vi vælger α til at være det primitive element. I tabel D.1 ses alle potenser af α.

Eksempel D.3. Følgende metode benyttes i Maple til at regne med det endelige legeme $\mathbb{F}_{2^5}$.

Konstruktion af $\mathbb{F}_{2^5} = \mathbb{F}_2[x]/\langle x^5+x^3+1\rangle$
[> $alias\left(\alpha = RootOf\left(x^5+x^3+1\right)\right)$;

$$\alpha$$

Addition af to elementer fra $\mathbb{F}_{2^5}$
[> $evala(\alpha^{15}+\alpha^{21}) \mod 2$

$$\alpha^4+1$$

Multiplum af to elementer fra $\mathbb{F}_{2^5}$
[> $evala(\alpha^{15}\cdot\alpha^{21}) \mod 2$

$$\alpha^3+1$$

▲