Reed-Solomon og NTP-koder

- deres egenskaber og dekodning

af

Maria Sondrup Iversen
Jane Gravgård Knudsen

Juni 2004

INSTITUT FOR MATEMATISKE FAG
Aalborg Universitet
• Fredrik Bajers vej 7G • 9220 Aalborg Øst •

Institut for Matematiske Fag
Aalborg Universitet

Titel:
Reed-Solomon og NTP-koder
-deres egenskaber og dekodning

Projekt:
Mat 6/ speciale

Projektgruppe:
G4-105

Gruppemedlemmer:
Maria Sondrup Iversen
Jane Gravgård Knudsen

Vejledere:
Hans Olav Geil
Christian Thommesen

Antal eksemplarer: 14

Antal sider: 131

Synopsis:
I dette speciale betragtes Reed-Solomon og NTP-koder.
Først præsenteres Reed-Solomon koder, og deres egenskaber, hvorefter der ses på dekodning af disse koder i de tilfælde, hvor der er sket færre end $d/2$ fejl. Herefter gennemgås to listedekodningsalgoritmer, som gør det muligt at rette flere end $d/2$ fejl.
For at kunne benytte disse to listedekodningsalgoritmer skal der kunne bestemmes førstegradsfaktorer i interpolationspolynomiet, hvilket der opstilles forskellige algoritmer til at løse.
Før definitionen af NTP-koder introduceres gennemgås teori, som gør dette muligt. Herunder teori om Gröbner baser og fodaftryk af idealer.
Herefter bestemmes minimumsafstand, dimension og dualkode for NTP-koderne. Desuden præsenteres en dekodningsalgoritme for disse koder, som kan rette op til $\frac{d-g}{2}$ fejl.
Til slut gives en kort vurdering af de to koder, i forhold til hinanden, udfra kriteriet om, at koder bør have en høj hastighed samtidig med en høj relativ minimumsafstand.

Forord

Denne rapport er udarbejdet som speciale fra slutningen af januar til begyndelsen af juni 2004, ved det Teknisk-Naturvidenskabelige Fakultet, Institut for Matematiske Fag på Aalborg Universitet.

Der gøres opmærksom på, at den del af specialet, som omhandler NTP-koder, samt Appendiks A og Appendiks B, er udarbejdet i samarbejde med Elisabeth Kuhr Rasmussen, som på nuværende tidspunkt har barselsorlov.
Desuden er kapitlet om Gröbner baser udarbejdet på MAT-5 fra først i september til midt i december 2003, ligeledes i samarbejde med Elisabeth Kuhr Rasmussen.

Kildehenvisninger vil gennem specialet blive angivet således: [kilde, henvisning], hvor kilden er anført i litteraturlisten, se side 123. Henvisningen kan være til et kapitel, et afsnit eller en hel specifik sætning eller lignende.
I specialet vil kildehenvisninger, som er angivet i begyndelsen af et kapitel eller afsnit, referere til det overordnede indhold i det pågældende kapitel/afsnit, hvorimod kildehenvisninger, som er angivet inde i teksten, refererer til et specifikt resultat.
Et engelsk resume kan findes umiddelbart før appendiks.

Institut for Matematiske Fag, Aalborg Universitet, juni 2004.

Maria Sondrup Iversen	Jane Gravgård Knudsen

Indhold

Kapitel 1

Indledning

Det overordnede emne i dette speciale er diskret matematik, og det mere specifikke emne er kodningsteori.
Herindenfor har vi valgt at beskæftige os med Reed-Solomon koder, samt en generalisering af disse, hvilke vi i denne rapport kalder NTP-koder.

Der lægges ud med en definition af Reed-Solomon koder, hvorefter der følger en redegørelse for disses egenskaber, såsom minimumsafstand og dimension. Desuden gives der en dekodningsalgoritme for de tilfælde, hvor der er sket færre end $\frac{d}{2}$ fejl, hvor d er minimumsafstanden for koden.
Herefter introduceres yderligere to dekodningsalgoritmer for Reed-Solomon koderne, nemlig Sudans listedekodningsalgoritme, og Guruswami-Sudans listedekodningsalgoritme.
Herunder vil der være en vurdering af for hvilke hastigheder af koden der er sket en forbedring ved at benytte listedekodning fremfor almindelig dekodning. Det vil sige, for hvilke hastigheder af koden er det muligt at rette mere end $\frac{d}{2}$ fejl.
Gyldigheden af Sudans- og Guruswami-Sudans listedekodningsalgoritmer afhænger blandt andet af, at det er muligt at bestemme lineære faktorer til interpolationspolynomiet $Q(x, y)$, hvis disse eksisterer, hvilket Kapitel 3 derfor omhandler.

Herefter ønsker vi at definere NTP-koderne, der, som tidligere nævnt, er en generalisering af Reed-Solomon koderne.

Altså skal der ligesom for Reed-Solomon koderne bestemmes punkter og polynomier, således at vi ved at evaluere polynomierne i de forskellige punkter får kodeordene i NTP-koden.
Punkterne skal tilhøre varieteten $\mathbf{V}(\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle)$, hvilket vil sige, at de skal være nulpunkter til norm- trace polynomiet tilhørende $\mathbb{F}_{q^m}^2$.
Polynomierne er en linearkombination af monomierne i fodaftrykket af idealet $\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$.
For at bestemme fodaftrykket skal der først kunne bestemmes en Gröbner basis for idealet, og Kapitel 4 indeholder derfor generel teori vedrørende Gröbner baser.

For NTP-koderne bestemmes både minimumsafstand, dimension og dualkode, hvortil det blandt andet benyttes, at monomierne i fodaftrykket af $J = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y\rangle$ alle har forskellig vægt, samt at alle vægte er repræsenteret ved et monomium heri. Desuden introduceres generel teori vedrørende genus og kondukter til bestemmelse af kodens dimension.
Herefter gives en dekodningsalgoritme for NTP-koderne, som kan rette færre end $\frac{d-g}{2}$ fejl, hvor d igen betegner minimumsafstanden og g er genus.

Efter at have introduceret både Reed-Solomon koderne og NTP-koderne ønsker vi at foretage en kort vurdering af de to koder i forhold til hinanden. Her betragtes koderne som gode, hvis de både har høj hastighed samtidig med, at de kan rette mange fejl i forhold til længden af kodeordene.

Sidst i rapporten er et appendiks, som består af Appendiks A og Appendiks B.
Appendiks A består af uddybende teori, som primært knytter sig til Kapitel 5, hvori der er en redegørelse, som bygger på [6], for at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ og $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ tilhører $\mathbb{F}_q$.
Appendiks B er ligeledes uddybende teori til Kapitel 5 og Kapitel 3, hvor det skal benyttes, at ækvivalensklasserne i $\mathbb{F}_{q^m}$, med hensyn til traceafbildningen, alle har samme størrelse.

Kapitel 2

Reed-Solomon koder

I dette kapitel introduceres Reed-Solomon koderne. Dette er koder, hvor kodeordene er genereret af polynomier, som er evalueret i en række forskellige punkter tilhørende et endeligt legeme.
Der lægges ud med en definition af koderne, hvorefter der gøres rede for forskellige egenskaber ved disse. Herefter gives først en dekodningsalgoritme, som gør det muligt at rette op til $\frac{d}{2}$ fejl, hvor d er minimumsafstanden for koden. Dernæst følger to listedekodningsalgoritmer, som er forbedringer af den foregående algoritme, idet disse kan rette mere end $\frac{d}{2}$ fejl.

Afsnit 2.1 og 2.2 bygger primært på [5, Afsnit 5.1 og 5.2], og Afsnit 2.3 bygger på [5, Kapitel 12].

2.1 Egenskaber ved Reed-Solomon koder

Definition 1 (Reed-Solomon koder) *Lad $x_1, \ldots, x_n$ være forskellige elementer i et endeligt legeme $\mathbb{F}_q$. Lad desuden $\mathbb{P}_k$ være mængden af polynomier tilhørende $\mathbb{F}_q[x]$ med grad mindre end k, hvor $k \leq n$.*
En (n, k) Reed-Solomon kode består da af kodeordene

$$(f(x_1), \ldots, f(x_n)), \text{ hvor } f \in \mathbb{P}_k.$$

2. Reed-Solomon koder

En Reed-Solomon kode vil fremover blive refereret til som en RS-kode.

For at sikre at RS-koderne er veldefinerede, skal det vises, at ethvert kodeord er genereret af præcis ét polynomium tilhørende $\mathbb{P}_k$, og at der til ethvert polynomium i $\mathbb{P}_k$ svarer netop ét kodeord.
Det er klart udfra definitionen, at ethvert kodeord er genereret af mindst et polynomium i $\mathbb{P}_k$.
Hvis to polynomier, $g, f \in \mathbb{P}_k$, genererer det samme kodeord, så vil samtlige $x_1, \ldots, x_n \in \mathbb{F}_q$ være rødder i $g(x) - f(x)$. Men da $g(x) - f(x)$ er et polynomium af grad strengt mindre end $k \leq n$, kan dette højst have $k - 1$ rødder. Hermed er der opnået en modstrid, og ethvert kodeord er derfor genereret af netop ét polynomium i $\mathbb{P}_k$.
Ligeledes kan der kun svare ét kodeord til hvert polynomium i $\mathbb{P}_k$, da der ved indsættelse af samme element i et polynomium ikke kan opstå to forskellige resultater.
Dermed gælder der alt i alt, at RS-koden er veldefineret.

Da RS-koden er veldefineret, så sendes en basis for $\mathbb{P}_k$ over i en basis for RS-koden, og da polynomierne i $\mathbb{P}_k$ udgør et k-dimensionalt vektorrum over $\mathbb{F}_q$, så er dimensionen af RS-koden lig k.

Idet $x_1, \ldots, x_n$ er forskellige elementer i $\mathbb{F}_q$, er længden af RS-koden, n, mindre end eller lig q. Koden er desuden lineær, da det for to kodeord, $\overline{c}_1 = (f_1(x_1), \ldots, f_1(x_n))$ og $\overline{c}_2 = (f_2(x_1), \ldots, f_2(x_n))$, $f_1, f_2 \in \mathbb{P}_k$, gælder, at $a\overline{c}_1 + b\overline{c}_2 = (g(x_1), \ldots, g(x_n))$, hvor $a, b \in \mathbb{F}_q$ og $g(x) = af_1(x) + bf_2(x)$ tilhører $\mathbb{P}_k$.
Dermed gælder det, at minimumsafstanden er lig minimumsvægten for en RS-kode.

For at bestemme minimumsafstanden for RS-koden, introduceres først en øvre grænse, som gør sig gældende for enhver lineær kode.

Sætning 2 (Singleton grænsen) *Lad C være en lineær kode af længde n, dimension k og minimumsafstand d. Så er*

$$d \leq n - k + 1.$$

Bevis: En lineær kode over $\mathbb{F}_q$ af dimension k består af q^k kodeord.
Ved at eliminere $d - 1$ fastholdte positioner i hvert af de q^k kodeord, vil disse stadig være forskellige, idet hvert par af kodeord er forskellige på mindst d

positioner.
Antallet af vektorer hvor kun disse $n-d+1$ positioner kan variere er q^{n-d+1}, og dermed er $k \leq n-d+1$, hvoraf resultatet følger. □

Herefter kan den eksakte minimumsafstand for RS-koderne bestemmes.

Sætning 3 *Minimumsafstanden for en (n,k) RS-kode er $n-k+1$.*

Bevis: Idet polynomierne i $\mathbb{P}_k$ højst kan have $k-1$ nulpunkter blandt $x_1, \ldots, x_n$, så har kodeordene en Hamming vægt, ω_H, på mindst $n-k+1$. Det vil sige, at $d \geq n-k+1$.
Ved at sammenholde dette med Sætning 2 fås det, at $d = n-k+1$ for en (n,k) RS-kode. □

Minimumsafstanden kan benyttes til at afgøre, hvor mange fejl det er muligt for koden at rette.
Lad $\overline{r} = \overline{c} + \overline{e}$, hvor $\overline{c}$ er et kodeord, være et modtaget ord. Så er antallet af fejl lig Hammingvægten af fejlvektoren $\overline{e}$.
Hvis Hammingvægten af alle fejlvektorer, $\overline{e}$, er mindre end eller lig t, for $t \in \mathbb{N}_0$, så vil koden, hvis denne er t-fejlkorrigerende, give præcis ét kodeord ved dekodning. At være t-fejlkorrigerende defineres således:

Definition 4 (t-fejlkorrigerende) *En kode er t-fejlkorrigerende, hvis det for to vilkårlige kodeord, $\overline{c}_i \neq \overline{c}_j$, og for alle fejlvektorer, $\overline{e}_1$ og $\overline{e}_2$, med Hamming vægt mindre end eller lig t, gælder, at $\overline{c}_i + \overline{e}_1 \neq \overline{c}_j + \overline{e}_2$.*

Proposition 5 *En lineær kode af længde n, dimension k og minimumsafstand d er t-fejlkorrigerende hvis og kun hvis $t < \frac{d}{2}$.*

Bevis: Antag først, at $t < \frac{d}{2}$, og at vi har givet to kodeord, $\overline{c}_i$ og $\overline{c}_j$, samt to fejlvektorer, $\overline{e}_1$ og $\overline{e}_2$, begge med Hamming vægt mindre end eller lig t, sådan at $\overline{c}_i + \overline{e}_1 = \overline{c}_j + \overline{e}_2$.
Idet koden er lineær, er $\overline{c}_i - \overline{c}_j = \overline{e}_1 - \overline{e}_2$ et kodeord, og $\omega_H(\overline{c}_i - \overline{c}_j) = \omega_H(\overline{e}_1 -$

$\overline{e}_2) \leq 2t < d$. Da dette er i modstrid med, at kodens minimumsafstand er lig d, er koden t-fejlkorrigerende.

Anden del af beviset føres ved kontraposition. Antag, at $t \geq \frac{d}{2}$, og lad $\overline{c}$ have vægt d. Konstruer en ny vektor, $\overline{y}$, ved at erstatte t positioner i $\overline{c}$ forskellige fra nul med nuller.
Dermed er $\omega_H(\overline{y}) \leq d - t \leq t$ og $\omega_H(\overline{y} - \overline{c}) \leq t$. Men da $\overline{0}$ er et kodeord gælder det, idet $\overline{0} + \overline{y} = \overline{c} + (\overline{y} - \overline{c})$, at koden ikke er t-fejlkorrigerende. □

Idet Reed-Solomon koder er lineære er disse t-fejlkorrigerende, hvis $t < \frac{d}{2}$. I næste afsnit beskrives en dekodningsalgoritme for Reed-Solomon koder, som kan rette op til $\frac{d}{2}$ fejl i et modtaget ord.

2.2 Dekodning af Reed-Solomon koder

Lad $\overline{r}$ være et modtaget ord, som er summen af et kodeord $\overline{c}$, tilhørende (n, k) RS-koden, og en fejlvektor $\overline{e}$ med Hammingvægt mindre end eller lig $t = \lfloor \frac{n-k}{2} \rfloor < \frac{d}{2}$. For at finde det afsendte kodeord $\overline{c}$ er ideen at bestemme interpolationspolynomiet

$$Q(x, y) = Q_0(x) + yQ_1(x) \quad \in \mathbb{F}_q[x, y] \backslash \{0\},$$

sådan at

1. $Q(x_i, r_i) = 0, \quad i = 1, \ldots, n.$
2. $\deg(Q_0(x)) \leq n - 1 - t.$
3. $\deg(Q_1(x)) \leq n - 1 - t - (k - 1).$

Det skal nu vises, at der vil eksistere sådan et poynomium.

Sætning 6 *Hvis der er sket færre end $\frac{d}{2}$ fejl i det modtagne ord $\overline{r}$, så eksisterer der et polynomium $Q(x, y)$, forskelligt fra nulpolynomiet, som opfylder de tre betingelser ovenfor.*

Bevis: Den første betingelse giver n homogene lineære ligninger, og antallet af ubekendte er $\deg(Q_0)+1+\deg(Q_1)+1 = n-t+n-t-(k-1)$. Idet $t = \lfloor \frac{n-k}{2} \rfloor$, giver dette, at $n-t+n-t-(k-1) = 2n-2t-(k-1) \geq n+1$, hvormed der vil eksistere en ikke-triviel løsning. □

Følgende sætning giver en metode til bestemmelse af det afsendte kodeord $\overline{c}$.

Sætning 7 *Lad det afsendte kodeord være genereret af polynomiet $g(x)$, og lad antallet af fejl, t, være mindre end $\frac{d}{2}$. Så er $g(x) = -\frac{Q_0(x)}{Q_1(x)}$.*

Bevis: Lad $\overline{c} = (g(x_1), \ldots, g(x_n))$, og $\overline{r} = \overline{c} + \overline{e}$, hvor $\omega_H(\overline{e}) \leq t$. Interpolationspolynomiet $Q(x,y)$ opfylder, at $Q(x_i, g(x_i) + e_i) = 0$, og idet $e_i = 0$ for mindst $n-t$ i'er, så har $Q(x, g(x))$ mindst $n-t$ nulpunkter, som præcis er de x_i'er, hvor $g(x_i) = r_i$. Desuden ses det, at polynomiet $Q(x, g(x))$ har grad højst $n-1-t$, og det kan derfor konkluderes, at $Q(x, g(x))$ er nulpolynomiet. Det vil sige, at $Q_0(x) + g(x)Q_1(x) = 0$, hvormed $g(x) = -\frac{Q_0(x)}{Q_1(x)}$. □

Hvis $Q(x_i, r_i)$ opskrives på følgende måde:

$$Q(x_i, r_i) = Q_1(x_i)(r_i + \frac{Q_0(x_i)}{Q_1(x_i)}) = Q_1(x_i)(r_i - g(x_i)),$$

ses det, at på de positioner, der er sket fejl, da må det være Q_1, som giver nul. Polynomiet $Q_1(x)$ kaldes derfor for fejllokaliseringspolynomiet.

Det er nu muligt at opstille en dekodningsalgoritme for RS-koder. Til dette formål defineres

$$l_0 = n-1-t \text{ og } l_1 = n-1-t-(k-1).$$

Algoritme 8
Input: Et modtaget ord $\overline{r} = (r_1, \ldots, r_n)$.
Hvis $g(x) \in \mathbb{F}_q[x]$, så er

$$Output : (g(x_1), \ldots, g(x_n)),$$

ellers

$$Output : failure.$$

1. *Løs det lineære ligningssystem:*

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{l_0} & r_1 & r_1x_1 & \dots & r_1x_1^{l_1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{l_0} & r_2 & r_2x_2 & \dots & r_2x_2^{l_1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{l_0} & r_n & r_nx_n & \dots & r_nx_n^{l_1} \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ \vdots \\ Q_{0,l_0} \\ Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

2. *Sæt*

$$\begin{aligned} Q_0(x) &= \sum_{j=0}^{l_0} Q_{0,j}x^j, \\ Q_1(x) &= \sum_{j=0}^{l_1} Q_{1,j}x^j, \\ g(x) &= -\frac{Q_0(x)}{Q_1(x)}. \end{aligned}$$

2.3 Listedekodning af Reed-Solomon koder

I forrige afsnit blev en dekodningsalgoritme for Reed-Solomon koder introduceret. Denne algoritme gjorde det muligt at rette op til og med $t < \frac{d}{2}$ fejl i et modtaget ord, og derved dekode til ét bestemt kodeord.
I dette afsnit bestemmes en dekodningsalgoritme, som kan rette mere end $\frac{d}{2}$ fejl i et modtaget ord, hvilket muligvis vil resultere i, at der eksisterer mere end et kodeord, som det er muligt at dekode til. Deraf ordet listedekodning.

2.3.1 Sudan listedekodning

Lad $\overline{r} = \overline{c} + \overline{e}$ være et modtaget ord, og lad $\omega_H(\overline{e}) \leq \tau$. Ideen er, som i forrige afsnit, at bestemme et polynomium i to variable. Vi ønsker at bestemme

$$Q(x, y) = Q_0(x) + yQ_1(x) + y^2Q_2(x) + \cdots + y^lQ_l(x),$$

sådan, at

1. $Q(x_i, r_i) = 0$, $i = 1, \ldots, n$.
2. $\deg(Q_j(x)) \leq n - \tau - 1 - j(k-1)$, $j = 0, 1, \ldots, l$.
3. $Q(x, y) \neq 0$.

For at sikre at et sådant polynomium eksisterer, skal antallet af ubekendte overstige antallet af de n homogene lineære ligninger fra betingelse 1 ovenfor. De ubekendte er koefficienterne i $Q(x, y)$, og antallet af disse er

$$(n - \tau) + (n - \tau - (k-1)) + \cdots + (n - \tau - l(k-1)). \tag{2.1}$$

Udfra Gauss' tællemetode giver dette

$$(l+1)(n-\tau) - \frac{l(l+1)(k-1)}{2}.$$

Dermed bliver betingelsen, at

$$(l+1)(n-\tau) - \frac{l(l+1)(k-1)}{2} > n,$$

hvilket er ækvivalent med

$$\tau < n\frac{l}{l+1} - \frac{l}{2}(k-1). \tag{2.2}$$

Det skal desuden sikres, at $\deg(Q_j(x))$ er større end eller lig nul, da (2.1) i modsat fald ikke ville tælle antallet af koefficienter i $Q(x, y)$. Da $\deg(Q_l(x))$ er mindre end eller lig $\deg(Q_j(x))$ for $j = 1, \ldots, l-1$ er det nok, at

$$(n - \tau) - l(k-1) \geq 0$$

eller ækvivalent, at

$$\tau \leq n - l(k-1). \tag{2.3}$$

Det vil sige, at hvis (2.2) og (2.3) er opfyldt, så eksisterer der et polynomium $Q(x,y)$ som opfylder betingelserne 1-3 ovenfor.

Lemma 9 *Hvis $Q(x,y)$ opfylder betingelserne 1-3, og $\overline{c} = (f(x_1), \ldots, f(x_n))$, hvor $\deg(f(x)) < k$, så gælder det, at $(y - f(x))|Q(x,y)$.*

Bevis: Betragt polynomiet $Q(x, f(x))$.
Idet $\deg(f(x)) < k$, så er $\deg(Q_j(x)(f(x))^j) \leq n - \tau - 1$, for alle j=1, ..., l. Det vil sige, at $Q(x, f(x))$ højst har grad $n - \tau - 1$.
Da r_i er forskellig fra $f(x_i)$ på højst τ positioner, så er $Q(x_i, f(x_i)) = 0$ for mindst $n - \tau$ x_i'er, ifølge betingelse 1.
Dermed overstiger antallet af nulpunkter til $Q(x, f(x))$ graden af $Q(x, f(x))$, hvilket medfører, at $Q(x, f(x))$ er nulpolynomiet.
Ved nu at betragte polynomiet $Q(x,y)$ som et polynomium i y over $\mathbb{F}_q[x]$, ses det, da $Q(x, f(x)) = 0$, at $f(x)$ er rod i $Q(x,y)$. Det vil sige, at $(y - f(x))|Q(x,y)$.

□

Da $f(x)$ genererer et kodeord, er det muligt at bestemme samtlige kodeord indenfor en afstand τ ved at finde alle faktorer til $Q(x,y)$ på formen $(y - f(x))$, hvor $\deg(f(x)) < k$.
Hvis $\tau > \frac{d}{2}$, er det muligt at få en hel liste af kodeord. Dog kan der højst være l, da dette er graden af y.

Det er nu muligt at opstille en algoritme til bestemmelse af en liste bestående af kodeord, som ligger indenfor en afstand τ fra et modtaget ord $\overline{r}$.

Algoritme 10
Input: Et modtaget ord $\overline{r} = (r_1, \ldots, r_n)$, og et naturligt tal τ.
Output: En liste af faktorer $f(x)$, som opfylder, at

$$d(f(x_1), \ldots, f(x_n), (r_1, \ldots, r_n)) \leq \tau.$$

1. *Løs det lineære ligningssystem, hvor* $l_j = n - \tau - 1 - j(k-1)$*:*

$$\sum_{j=0}^{l} \begin{bmatrix} r_1^j & \dots & 0 & 0 \\ 0 & r_2^j & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & r_n^j \end{bmatrix} \begin{bmatrix} 1 & x_1 & \dots & x_1^{l_j} \\ 1 & x_2 & \dots & x_2^{l_j} \\ \vdots & \vdots & \dots & \vdots \\ 1 & x_n & \dots & x_n^{l_j} \end{bmatrix} \begin{bmatrix} Q_{j,0} \\ Q_{j,1} \\ Q_{j,2} \\ \vdots \\ Q_{j,l_j} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

2. *Sæt*

$$Q_j(x) \quad = \quad \sum_{r=0}^{l_j} Q_{j,r} x^r$$

og

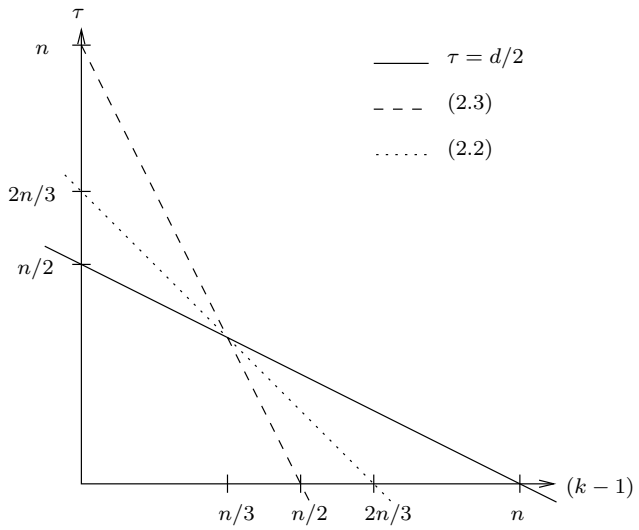
$$Q(x,y) = \sum_{j=0}^{l} Q_j(x) y^j.$$

3. *Find samtlige faktorer* $(y - f(x))$ *i* $Q(x,y)$*, hvor* $\deg(f(x)) < k$*.*

Det ønskes nu bestemt for hvilke hastigheder af koden denne dekodningsalgoritme er forbedret i forhold til den oprindelige dekodningsalgoritme for Reed-Solomon koder, beskrevet i Algoritme 8.
Det vil sige, for hvilke hastigheder er det muligt for koden at rette mere end $\frac{d}{2}$ fejl.

Vi deler denne analyse op i tre tilfælde:
$l = 1$: Idet både (2.2) og (2.3) skal være opfyldt, er $\tau < \frac{n-k+1}{2}$ i dette tilfælde, og der er altså ingen forbedring i forhold til Algoritme 8.

$l = 2$: Her får (2.2) og (2.3) henholdsvis udseendet $\tau < n\frac{2}{3} - (k-1)$ og $\tau \leq n - 2(k-1)$.
Ved nu at betragte $\tau = n\frac{2}{3} - (k-1)$ og $\tau = n - 2(k-1)$ som lineære i $(k-1)$ kan vi sammenligne med $\tau = \frac{d}{2} = \frac{n}{2} - \frac{k-1}{2}$.
Først bestemmes skæringspunktet mellem de tre rette linier til at være $k-1 = \frac{n}{3}$.
Det ses desuden at de tre rette linier skærer τ-aksen i henholdsvis $n\frac{2}{3}$, n og $\frac{n}{2}$.
Det vil sige, at både (2.2) og (2.3) ligger over $\tau = \frac{d}{2}$ for $k - 1 < \frac{n}{3}$, se Figur 2.1.
Altså er der sket en forbedring for hastigheder $\frac{k}{n} < \frac{1}{3} + \frac{1}{n}$.



Figur 2.1: *Sammenligning af ligning* (2.2) *og* (2.3) *med* $\tau = \frac{d}{2}$ *for* $l = 2$.

Idet (2.2) ligger under (2.3) for disse hastigheder, er det muligt at finde samtlige kodeord, som ligger i afstand τ væk fra det modtagne ord, for $\tau < n\frac{2}{3} - (k-1)$.

$l > 2$: Her benyttes samme strategi som for $l = 2$, hvor de tre udtryk betragtes som lineære i $(k-1)$.
Skæringspunkterne med τ-aksen er for henholdsvis (2.2), (2.3) og $\tau = \frac{d}{2}$ lig $n\frac{l}{l+1}$, n og $\frac{n}{2}$, hvilket vil sige, at indtil nogle af linierne skærer hinanden, så ligger (2.3) øverst og $\tau = \frac{d}{2}$ nederst, idet $l > 2$.
Skæringspunktet mellem $\tau = n\frac{l}{l+1} - \frac{l}{2}(k-1)$ og $\tau = n - l(k-1)$ er

$$k - 1 = n\left(\frac{2}{l} \cdot \frac{1}{l+1}\right),$$

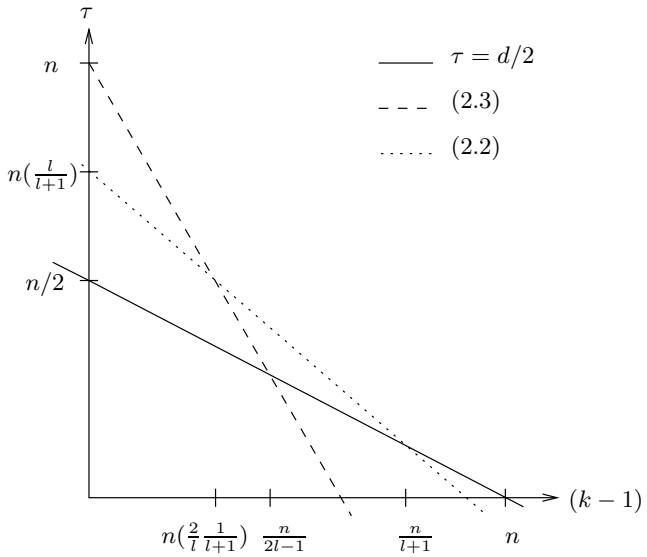
skæringspunktet mellem $\tau = n\frac{l}{l+1} - \frac{l}{2}(k-1)$ og $\tau = \frac{d}{2}$ er

$$k - 1 = n\left(\frac{1}{l+1}\right),$$

og skæringspunktet mellem $\tau = n - l(k-1)$ og $\tau = \frac{d}{2}$ er

$$k - 1 = n\left(\frac{1}{2l-1}\right).$$

Da $l > 2$ er $n\left(\frac{2}{l} \cdot \frac{1}{l+1}\right) < n\left(\frac{1}{l+1}\right)$, hvilket vil sige, at (2.2) og (2.3) skærer hinanden tidligere end $\tau = \frac{d}{2}$ skærer (2.2). Da der derudover gælder, at (2.2) ligger over (2.3) efter skæring med denne, så vil $\tau = \frac{d}{2}$ først skære (2.3) og derpå (2.2), se Figur 2.2.
Det vil sige, at $n\left(\frac{2}{l} \cdot \frac{1}{l+1}\right) < n\left(\frac{1}{2l-1}\right) < n\left(\frac{1}{l+1}\right)$. Idet både betingelse (2.2) og



Figur 2.2: *Sammenligning af ligning* (2.2) *og* (2.3) *med* $\tau = \frac{d}{2}$ *for* $l > 2$.

(2.3) skal være opfyldt, er der sket en forbedring med hensyn til størrelsen af τ i forhold til Algoritme 8 for hastigheder givet ved $\frac{k}{n} < \frac{1}{2l-1} + \frac{1}{n}$.

For hastigheder $\frac{k}{n} \leq \frac{2}{l} \cdot \frac{1}{l+1} + \frac{1}{n}$ kan samtlige kodeord, indenfor en afstand τ, $\tau < n\frac{l}{l+1} - \frac{1}{2}(k-1)$, fra det modtagne ord bestemmes. Mens for hastigheder $\frac{2}{l} \cdot \frac{1}{l+1} + \frac{1}{n} < \frac{k}{n} < \frac{1}{2l-1} + \frac{1}{n}$ skal det gælde, at $\tau \leq n - l(k-1)$.

Som det heraf ses, er der kun sket forbedringer, med hensyn til hvor mange fejl det er muligt at rette, for meget små hastigheder for koden, hvilket vi ønsker at forbedre yderligere i næste afsnit.

2.3.2 Guruswami og Sudan listedekodning

Der vil i det følgende blive beskrevet en udvidelse af foregående afsnits listedekodning af RS-koder.

Først defineres multiplicitet af rødder.

Definition 11 (Multiplicitet af rødder) *Lad $Q(x,y) = \sum_{k,j} q_{k,j} x^k y^j$ være et polynomium i $\mathbb{F}_q[x,y]$. Lad desuden $(a,b) \in \mathbb{F}_q^2$ og*

$$Q^*(x,y) = Q(x+a, y+b) = \sum_{k,j} q^*_{k,j} x^k y^j.$$

Hvis $q^*_{k,j} = 0$ for $k+j < s$, hvor s er den største af sådanne værdier, så kaldes (a,b) en rod til $Q(x,y)$ af multiplicitet s.

Lad $\overline{r} = \overline{c} + \overline{e}$ være et modtaget ord, hvor $\omega_H(\overline{e}) \leq \tau$, der søges da igen et interpolationspolynomium i to variable:

$$Q(x,y) = Q_0(x) + yQ_1(x) + y^2Q_2(x) + \cdots + y^lQ_l(x),$$

sådan at

1. (x_i, r_i), $i = 1, \ldots, n$, er rødder af multiplicitet s.
2. $\deg(Q_j(x)) \leq s(n-\tau) - 1 - j(k-1)$, $j = 0, 1, \ldots, l$.
3. $Q(x,y) \neq 0$.

Igen skal antallet af koefficienter være større end antallet af homogene lineære ligninger, for at $Q(x,y)$ eksisterer.
Antallet af koefficienter er

$$\begin{aligned} & s(n-\tau) + s(n-\tau) - (k-1) + \cdots + s(n-\tau) - l(k-1) \\ = \quad & s(l+1)(n-\tau) - \frac{l(l+1)(k-1)}{2}. \end{aligned}$$

For hvert (x_i, r_i) er der, ifølge definitionen af multiplicitet, $\frac{(s+1)^2-(s+1)}{2} = \binom{s+1}{2}$ homogene lineære ligninger, og da der er n rødder af multiplicitet s, så er antallet af homogene lineære ligniger $n\binom{s+1}{2}$. Altså skal det være opfyldt, at

$$s(n-\tau) + s(n-\tau) - (k-1) + \cdots + s(n-\tau) - l(k-1) > n\binom{s+1}{2},$$

hvilket svarer til, at

$$\tau < n\frac{2l-s+1}{2(l+1)} - \frac{l}{2s}(k-1). \tag{2.4}$$

Af samme argument som tidligere skal det sikres, at $\deg(Q_j(x))$ er større end eller lig nul, eller at

$$s(n-\tau) - l(k-1) \geq 0,$$

hvilket er ækvivalent med

$$\tau \leq n - \frac{l(k-1)}{s}. \tag{2.5}$$

Det vil sige, at hvis (2.4) og (2.5) samtidig er opfyldt, så eksisterer der et polynomium $Q(x, y)$ som opfylder ovenstående tre betingelser.

Der gælder nu følgende:

Lemma 12 *Hvis $Q(x, y)$ opfylder betingelse 1-3 ovenfor og $\overline{c} = (f(x_1), \ldots, f(x_n))$, hvor $\deg(f(x)) < k$, så vil $(y - f(x))|Q(x, y)$.*

Bevis: Vi ved fra betingelse 1, at (x_i, r_i), $i = 1, \ldots, n$, er en rod til $Q(x, y)$ med multiplicitet s. Dermed har vi, at

$$Q(x, y) = Q^*(x - x_i, y - r_i) = \sum_{k+j \geq s} q^*_{k,j}(x - x_i)^k (y - r_i)^j.$$

Det vil sige, at

$$Q(x, f(x)) = \sum_{k+j \geq s} q^*_{k,j}(x - x_i)^k (f(x) - r_i)^j.$$

Betragt nu de tilfælde, hvor $f(x_i) = r_i$, da er

$$Q(x, f(x)) = \sum_{k+j \geq s} q^*_{k,j}(x - x_i)^k (f(x) - f(x_i))^j,$$

og da x_i er en rod heri, fås

$$Q(x, f(x)) = \sum_{k+j \geq s} q^*_{k,j}(x - x_i)^k((x - x_i)p_i(x))^j,$$

hvor $p_i(x) \in \mathbb{F}_q[x]$. Idet $k + j \geq s$ kan ovenstående omskrives til

$$\sum_{k+j \geq s} q^*_{k,j}(x - x_i)^k((x - x_i)p_i(x))^j = (x - x_i)^s P(x),$$

hvor $P(x) \in \mathbb{F}_q[x]$.

Det er nu muligt at bestemme antallet af rødder i $Q(x, f(x))$.
Da $f(x_i) = r_i$ for mindst $n - \tau$ i'er, så har $Q(x, f(x))$ $n - \tau$ s-dobbelte rødder.
Det vil sige, at $Q(x, f(x))$ har mindst $s(n - \tau)$ rødder.
Graden af f er højst $k - 1$, og dermed fremgår det af betingelse 2, at graden af $Q(x, f(x))$ højst er $s(n - \tau) - 1$.
Altså er $\deg(Q(x, f(x))) < s(n - \tau)$, hvilket kun er muligt, hvis $Q(x, f(x)) = 0$.
Dermed er $f(x)$ rod i $Q(x, y)$ og $(y - f(x))|Q(x, y)$. □

Alle kodeord i afstand τ fra det modtagne ord kan altså findes ved at bestemme faktorerne $(y - f(x))$ til $Q(x, y)$, hvor $\deg(f(x)) < k$.
Før en dekodningsalgoritme kan formuleres opskrives interpolationspolynomiet således:

$$Q(x, y) = \sum_{k,j} q_{k,j} x^k y^j,$$

hvor $q_{k,j} \neq 0$, hvis $j \leq l$ og $k \leq s(n - \tau) - 1 - j(k - 1)$.
Dermed kan der foretages følgende omskrivning af $Q^*(x, y)$

$$\begin{aligned} Q^*(x, y) = Q(x + x_i, y + r_i) &= \sum_{k,j} q_{k,j}(x + x_i)^k(y + r_i)^j \\ &= \sum_{k,j} \sum_{h,r} q_{k,j} \binom{k}{h} x^h x_i^{k-h} \binom{j}{r} y^r r_i^{j-r} \\ &= \sum_{h,r} \left(\sum_{\substack{k \geq h \\ j \geq r}} q_{k,j} \binom{k}{h} \binom{j}{r} x_i^{k-h} r_i^{j-r} \right) x^h y^r. \end{aligned}$$

Algoritme 13 (Guruswami-Sudan)
Input: Et modtaget ord $\overline{r} = (r_1, \ldots, r_n)$*, og naturlige tal* τ *og* s*.*
Output: En liste af faktorer $f(x)$*, som opfylder, at*

$$d(f(x_1), \ldots, f(x_n), (r_1, \ldots, r_n)) \leq \tau.$$

1. *Løs for* $q_{k,j}$ *systemet af lineære ligninger, hvor* $h + r < s$*,* $i = 1, 2, \ldots, n$ *og* $q_{k,j} \neq 0$*, hvis* $j \leq l$ *og* $k \leq s(n-\tau) - 1 - j(k-1) = l_j$*:*

$$\left(\sum_{\substack{k \geq h \\ j \geq r}} q_{k,j} \binom{k}{h} \binom{j}{r} x_i^{k-h} r_i^{j-r} \right) = 0.$$

2. *Sæt*

$$Q_j(x) \quad = \quad \sum_{k=0}^{l_j} q_{k,j} x^k$$

og

$$Q(x, y) = \sum_{j=0}^{l} Q_j(x) y^j.$$

3. *Find samtlige faktorer* $(y - f(x))$ *i* $Q(x, y)$*, hvor* $\deg(f(x)) < k$*.*

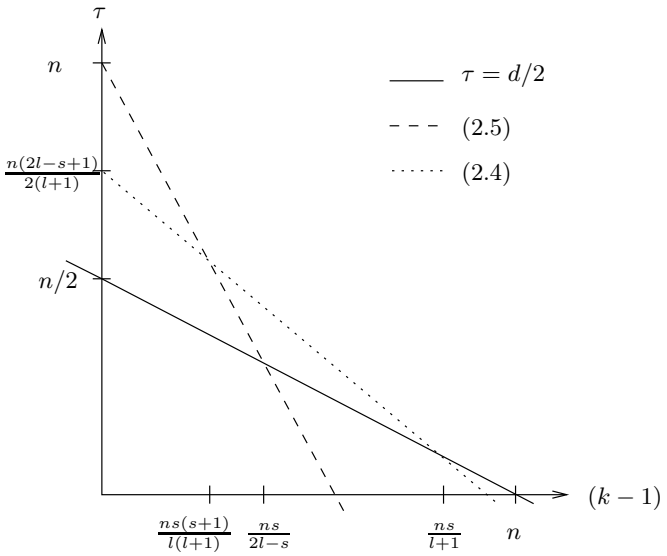
Det ønskes også for denne algoritme bestemt, for hvilke hastigheder af koden denne er forbedret i forhold til dekodningsalgoritmen for Reed-Solomon koder, beskrevet i Algoritme 8.
Så igen skal det afgøres for hvilke hastigheder det er muligt for koden at rette mere end $\frac{d}{2}$ fejl.

Vi betragter nu $\tau = n\frac{2l-s+1}{2(l+1)} - \frac{l}{2s}(k-1)$, $\tau = n - \frac{l(k-1)}{s}$ og $\tau = \frac{d}{2} = \frac{n}{2} - \frac{k-1}{2}$ som lineære i $(k-1)$.

Ved udelukkende at se på det tilfælde hvor $s < l$, vil disse tre liniers skæring med τ-aksen fordele sig således:

$$\frac{n}{2} < n\frac{2l-s+1}{2(l+1)} < n.$$

Som under Sudan listedekodning bestemmes skæringspunkterne mellem de tre linier.
Skæringspunktet mellem $\tau = \frac{d}{2}$ og (2.4) er $k - 1 = n\frac{s}{l+1}$, og skæringspunktet mellem $\tau = \frac{d}{2}$ og (2.5) er $k - 1 = n\frac{s}{2l-s}$, se Figur 2.3.



Figur 2.3: *Sammenligning af ligning* (2.4) *og* (2.5) *med* $\tau = \frac{d}{2}$ *for* $s < l$.

Hvis $s = l-1$ er $n\frac{s}{l+1} = n\frac{s}{2l-s}$, hvilket vil sige, at alle tre linier skærer hinanden i $k - 1 = n\frac{s}{l+1}$. Dette medfører, at der for hastigheder, $\frac{k}{n} < \frac{s}{l+1} + \frac{1}{n}$ er sket en forbedring således, at det er muligt for koden at rette mere end $\frac{d}{2}$ fejl. For disse hastigheder kan samtlige kodeord indenfor en afstand $\tau < n\frac{2l-s+1}{2(l+1)} - \frac{l}{2s}(k-1)$ fra det modtagne ord bestemmes.

Gælder det derimod, at $s < l - 1$, så er $n\frac{s}{l+1} > n\frac{s}{2l-s}$. Det vil sige, at $\tau = \frac{d}{2}$ først skærer (2.5) og derpå (2.4), se Figur 2.3. Dermed er der sket en forbedring med hensyn til τ, i forhold til Algoritme 8, for hastigheder, $\frac{k}{n} < \frac{s}{2l-s} + \frac{1}{n}$.

Skæringspunktet mellem (2.4) og (2.5) er $k - 1 = n\frac{s(s+1)}{l(l+1)}$.
Altså er det muligt for hastigheder, $\frac{k}{n} \leq \frac{s(s+1)}{l(l+1)} + \frac{1}{n}$, at bestemme samtlige

kodeord, indenfor en afstand τ, $\tau < n\frac{2l-s+1}{2(l+1)} - \frac{l}{2s}(k-1)$, fra det modtagne ord. Mens det for hastigheder $\frac{s(s+1)}{l(l+1)} + \frac{1}{n} < \frac{k}{n} < \frac{s}{2l-s} + \frac{1}{n}$ skal gælde, at $\tau \leq n - \frac{l(k-1)}{s}$.

Det ses desuden, at der er sket en forbedring med hensyn til størrelsen af hastighederne i forhold til Sudan listedekodning af RS-koder beskrevet i forrige afsnit, idet det nu er muligt at regulere på parameteren s.

Det vil sige, at det ved hjælp af Algoritme 13 er muligt at rette mere end $\frac{d}{2}$ fejl i et modtaget ord for forholdsvis store hastigheder af Reed-Solomon koden.

Kapitel 3

Bestemmelse af førstegradsfaktorer i $Q(x, y)$

For at kunne benytte de to listedekodningsalgoritmer for Reed-Solomon koder, beskrevet i forrige kapitel, er det en forudsætning, at der kan bestemmes faktorer til interpolationspolynomiet på formen $(y - f(x))$, hvor $\deg(f(x)) < k$. At dette er muligt, vil der derfor blive gjort rede for igennem dette kapitel.

Afsnit 3.1 er baseret på [7, Kapitel 3], mens hele Afsnit 3.2 er baseret på udvalgte dele af [3].

3.1 Reducering af problem

Problemet reduceres først til udelukkende at omhandle polynomier i én variabel. Til dette formål defineres det endelige legeme bestående af q^k elementer $\mathbf{E} = \mathbb{F}_{q^k} = \mathbb{F}_q[x]/\langle e(x)\rangle$, hvor $e(x)$ er et irreducibelt polynomium i $\mathbb{F}_q[x]$ af grad k. Herefter betragtes afbildningen $\varphi\colon \mathbb{F}_q[x, y] \to \mathbf{E}[y]$, givet ved:

$$\varphi\left(\sum_i p_i(x)y^i\right) = \sum_i [p_i(x)]_{\mathbf{E}} \cdot y^i, \tag{3.1}$$

hvor $[p_i(x)]_{\mathbf{E}}$ repræsenterer ækvivalensklasserne i $\mathbf{E}$.
Denne afbildning skal vises, at være en ringhomomorfi.

Lemma 14 *φ er en ringhomomorfi.*

Bevis: Det vises først, at

$$\varphi\left(\sum_{i=0}^{N} p_i(x)y^i + \sum_{i=0}^{M} q_i(x)y^i\right) = \varphi\left(\sum_{i=0}^{N} p_i(x)y^i\right) + \varphi\left(\sum_{i=0}^{M} q_i(x)y^i\right).$$

Antages det, at $M \geq N$ så er

$$\sum_{i=0}^{N} p_i(x)y^i + \sum_{i=0}^{M} q_i(x)y^i = \sum_{i=0}^{M}(p_i(x) + q_i(x))y^i,$$

hvor $p_i(x) = 0$ for $N+1 \leq i \leq M$.
Altså gælder det, at

$$\begin{aligned}
\varphi\left(\sum_{i=0}^{N} p_i(x)y^i + \sum_{i=0}^{M} q_i(x)y^i\right) &= \varphi\left(\sum_{i=0}^{M}(p_i(x) + q_i(x))y^i\right) \\
&= \sum_{i=0}^{M}[p_i(x) + q_i(x)]_{\mathbf{E}} \cdot y^i \\
&= \sum_{i=0}^{M}[p_i(x)]_{\mathbf{E}} \cdot y^i + \sum_{i=0}^{M}[q_i(x)]_{\mathbf{E}} \cdot y^i \\
&= \varphi\left(\sum_{i=0}^{N} p_i(x)y^i\right) + \varphi\left(\sum_{i=0}^{M} q_i(x)y^i\right).
\end{aligned}$$

Det vil sige φ er lukket under addition. For at φ er en ringhomomorfi skal det desuden gælde, at

$$\varphi\left(\sum_i p_i(x)y^i \sum_j q_j(x)y^j\right) = \varphi\left(\sum_i p_i(x)y^i\right)\varphi\left(\sum_j q_j(x)y^j\right).$$

Dette er opfyldt, idet:

$$\varphi\left(\sum_i p_i(x)y^i \sum_j q_j(x)y^j\right) = \varphi\left(\sum_i \sum_j p_i(x)q_j(x)y^j y^i\right)$$

Da φ er en homomorfi med hensyn til addition, kan dette skrives som

$$\begin{aligned} &= \sum_i \sum_j [p_i(x)q_j(x)]_{\mathbf{E}} \cdot y^j y^i \\ &= \sum_i \sum_j [p_i(x)]_{\mathbf{E}} [q_j(x)]_{\mathbf{E}} \cdot y^j y^i \\ &= \sum_i [p_i(x)]_{\mathbf{E}} \cdot y^i \sum_j [q_j(x)]_{\mathbf{E}} \cdot y^j \\ &= \varphi\left(\sum_i p_i(x)y^i\right) \varphi\left(\sum_j q_j(x)y^j\right). \end{aligned}$$

Hermed er φ en ringhomomorfi. □

Dette lemma benyttes til at vise følgende sætning.

Sætning 15 *Hvis $f(x,y)$ går op i $Q(x,y)$, så går $\varphi(f(x,y))$ op i $\varphi(Q(x,y))$.*

Bevis: Resultatet følger af Lemma 14, idet

$$\begin{aligned} f(x,y)|Q(x,y) &\Rightarrow Q(x,y) = f(x,y)g(x,y) \\ &\Rightarrow \varphi(Q(x,y)) = \varphi(f(x,y)g(x,y)) = \varphi(f(x,y))\varphi(g(x,y)) \\ &\Rightarrow \varphi(f(x,y))|\varphi(Q(x,y)), \end{aligned}$$

for et $g(x,y) \in \mathbb{F}_q[x,y]$. □

Korollar 16 *Hvis $(y - f(x))|Q(x,y)$ så er $y - [f(x)]_{\mathbf{E}}$ en irreducibel faktor i $\varphi(Q(x,y))$.*

Bevis: Hvis $(y - f(x))|Q(x,y)$, så er $y - [f(x)]_{\mathbf{E}}$, ifølge Sætning 15, en faktor i $\varphi(Q(x,y))$. Idet $y - [f(x)]_{\mathbf{E}}$ er af grad 1 er polynomiet irreducibelt. □

Altså er det vist, at hvis $Q(x,y)$ har en faktor på formen $(y - f(x))$, så er $(y - [f(x)]_{\mathbf{E}})$ en irreducibel faktor af $\varphi(Q(x,y))$, hvor $\deg([f(x)]_{\mathbf{E}}) < k$.
Det vil sige, at hvis der er fundet en faktor $(y - [f(x)]_{\mathbf{E}})$ til $\varphi(Q(x,y))$, så kan man ved indsættelse af roden, $[f(x)]_{\mathbf{E}}$, i $Q(x,y)$ afgøre, hvorvidt denne også er rod hertil eller ej. Er dette tilfældet, har vi fundet en faktor til $Q(x,y)$ på formen $(y - f(x))$, hvor $\deg(f(x)) < k$.
Hermed er problemet reduceret til at bestemme førstegradsfaktorer i én variabel til $\varphi(Q(x,y))$.

3.2 Bestemmelse af rødder til $\varphi(Q(x,y))$ i E

At bestemme rødderne til polynomiet $\varphi(Q(x,y)) \in \mathbf{E}[y]$, i $\mathbf{E}$, svarer netop til at bestemme alle førstegradsfaktorer i $\varphi(Q(x,y))$ tilhørende $\mathbf{E}[y]$. Idet $y^{q^k} - y = \prod_{\alpha \in \mathbf{E}}(y - \alpha)$, er foregående ækvivalent med at faktorisere $\gcd(y^{q^k} - y, \varphi(Q(x,y)))$ i irreducible faktorer.
Til dette formål introduceres efterfølgende algoritmer.

Algoritme 17 (Gentagen kvadrering)
Input: $a \in R$, hvor R er en kommutativ ring, og $n \in \mathbb{N}$.
Output: $a^n \in R$.

1. *(Binær repræsentation af n)*
   Skriv $n = 2^k + n_{k-1} \cdot 2^{k-1} + \cdots + n_1 \cdot 2 + n_0$, hvor alle $n_i \in \{0,1\}$
   $b_k := a$

2. **for** $i = k-1, k-2, \ldots, 0$ **do**
   if $n_i = 1$ **then** $b_i := b_{i+1}^2 a$ **else** $b_i := b_{i+1}^2$

3. **return** b_0

Algoritme 17 virker, idet $b_i = a^{\lfloor \frac{n}{2^i} \rfloor}$, hvilket vises ved induktion i i.
Basistrin: $i = k$. Ifølge algoritmen er $b_k = a$, og udfra den binære repræsentation af n ses det, at $\lfloor \frac{n}{2^k} \rfloor$ er lig 1. Dermed er $b_k = a = a^{\lfloor \frac{n}{2^k} \rfloor}$.
Induktionshypotese: Det antages, at $b_1 = a^{\lfloor \frac{n}{2} \rfloor}$.

Induktionstrin: $i = 0$. Ifølge algoritmen gælder det, at:

$$b_0 = \begin{cases} b_1^2 \cdot a & for \quad n_0 = 1 \\ b_1^2 & for \quad n_0 = 0. \end{cases}$$

Hermed følger det af induktionshypotesen, at:

$$b_0 = \begin{cases} (a^{\lfloor \frac{n}{2} \rfloor})^2 \cdot a & for \quad n_0 = 1 \\ (a^{\lfloor \frac{n}{2} \rfloor})^2 & for \quad n_0 = 0. \end{cases}$$

Idet $n_0 = 1$ vil medføre, at n er ulige, og $n_0 = 0$ vil medføre, at n er lige, så er $(a^{\lfloor \frac{n}{2} \rfloor})^2 \cdot a = a^n = a^{\lfloor \frac{n}{2^0} \rfloor}$ og $(a^{\lfloor \frac{n}{2} \rfloor})^2 = a^n = a^{\lfloor \frac{n}{2^0} \rfloor}$. Hvormed det er vist, at $b_i = a^{\lfloor \frac{n}{2^i} \rfloor}$

Der deles nu op i de to tilfælde, hvor karakteristikken af $\mathbb{F}_q$ er ulige, og hvor karakteristikken af $\mathbb{F}_q$ er lig to.

3.2.1 Equal degree spaltning -ulige karakteristik

Før det er muligt at opstille en algoritme, der bestemmer faktorer til et polynomium bestående af irreducible faktorer af samme grad, introduceres følgende resultater.

Lad i det efterfølgende R være et Euklidisk område. Lad desuden $m_1, \ldots, m_r \in R$ være parvis primiske, og $m = m_1 \cdots m_r$, hvormed $m = \texttt{lcm}(m_1, \ldots, m_r)$.
Vi har da for $1 \leq i \leq r$ ring homomorfierne:

$$\begin{aligned} \chi_i \colon R &\to R/\langle m_i \rangle, \\ f &\mapsto f \mod m_i. \end{aligned}$$

Ved at kombinere disse ringhomomorfier for alle i, fås ringhomomorfien givet ved:

$$\begin{aligned} \chi = \chi_1 \times \cdots \times \chi_r \colon \quad R \to &\quad R/\langle m_1 \rangle \times \ldots \times R/\langle m_r \rangle, \\ f \mapsto &\quad (f \mod m_1, \ldots, f \mod m_r). \end{aligned}$$

Lemma 18 *χ er en surjektiv afbildning, og kernen af χ er lig $\langle m \rangle$.*

Bevis: Lad $f \in R$. Dermed gælder det, at

$$\begin{aligned} f \in \ker\chi &\Leftrightarrow \chi(f) = (f \mod m_1, \ldots, f \mod m_r) = (0,\ldots,0) \\ &\Leftrightarrow m_i | f \text{ for } 1 \leq i \leq r \Leftrightarrow \texttt{lcm}(m_1,\ldots,m_r) | f \Leftrightarrow m | f. \end{aligned}$$

Heraf fås, at $\ker\chi = \langle m \rangle$.
For at bevise surjektivitet, skal det først vises, at der for $1 \leq i \leq r$, eksisterer $l_i \in R$, sådan at $\chi(l_i) = \overline{e}_i$, hvor $\overline{e}_i = (0,\ldots,0,1,0,\ldots,0) \in R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle$ repræsenterer den i'te enhedsvektor.
For at indse, at dette er tilstrækkeligt, opskrives først et vilkårligt element i $R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle$:

$$v = (\tilde{v} \mod m_1, \ldots, \tilde{v} \mod m_r) \in R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle,$$

hvor $\tilde{v} \in R$.

Hermed gælder det, idet χ er en ring homomorfi, at

$$\begin{aligned} \chi\left(\sum_{1\leq i\leq r} \tilde{v} l_i\right) &= \sum_{1\leq i\leq r} \chi(\tilde{v})\chi(l_i) \\ &= \sum_{1\leq i\leq r} (\tilde{v} \mod m_1, \ldots, \tilde{v} \mod m_r) \cdot \overline{e}_i \\ &= \sum_{1\leq i\leq r} (0,\ldots,0,\tilde{v} \mod m_i, 0,\ldots,0) = v. \end{aligned}$$

Idet $v \in R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle$ var vilkårligt valgt, er ethvert element i $R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle$ ramt af et element i R, hvorved χ er surjektiv.

Det skal nu vises, at der eksisterer sådanne $l_i \in R$. Antag, at $i = 1$. Ved at benytte "den udvidede Euklids algoritme" på $m_2 \cdots m_r = \frac{m}{m_1}$ og m_1, fås $s,t \in R$, således at $s\frac{m}{m_1} + tm_1 = 1 = \gcd(\frac{m}{m_1}, m_1)$.
Lad nu $l_1 = s\frac{m}{m_1}$. Dermed er

$$l_1 \equiv 0 \mod m_i \quad \textit{for} \quad 2 \leq i \leq r$$

og

$$l_1 = s\frac{m}{m_1} \equiv s\frac{m}{m_1} + tm_1 = 1 \mod m_1.$$

Altså er $\chi(l_1) = \overline{e}_1$ som ønsket. Hvormed lemmaet er bevist. □

Herudfra følger nu den kinesiske restsætning.

Korollar 19 (Kinesisk restsætning) *Der gælder følgende ring isomorfi:*

$$R/\langle m\rangle \cong R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle.$$

Bevis: Ifølge Lemma 18 er χ en surjektiv afbildning fra R til $R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle$, med kernen $\langle m\rangle$. Dermed følger det af homomorfisætningen for ringe, [6, Theorem 1.40, side 14], at $R/\langle m\rangle \cong R/\langle m_1\rangle \times \cdots \times R/\langle m_r\rangle$. □

Det vi ønsker, er at bestemme de irreducible faktorer, $f_1, \ldots, f_r \in \mathbb{F}_q[x]$, til et monisk polynomium $f = f_1 \cdots f_r \in \mathbb{F}_q[x]$, hvor $\deg f = n$ og $\deg f_1 = \cdots = \deg f_r = d$, hvormed $r = \frac{n}{d}$.
I vores tilfælde er vi kun interesseret i førstegradsfaktorerne, og vi har derfor $d = 1$ og $r = n$.
Det antages, at $r \geq 2$, da f ellers selv ville være en irreducibel faktor af grad 1.

Idet $\gcd(f_i, f_j) = 1$ for $i \neq j$, fås ringhomomorfien fra den kinesiske restsætning, Korollar 19,

$$\chi\colon \tilde{R} = \mathbb{F}_q[x]/\langle f\rangle \to \mathbb{F}_q[x]/\langle f_1\rangle \times \cdots \times \mathbb{F}_q[x]/\langle f_n\rangle = \tilde{R}_1 \times \cdots \times \tilde{R}_n.$$

Da f_i'erne er irreducible for alle $1 \leq i \leq n$, så er $\tilde{R}_i$'erne endelige legemer med q elementer.
For ethvert $a \in \mathbb{F}_q[x]$ gælder det, at $a \mod f \in \tilde{R}$ og $\chi(a \mod f) = (a \mod f_1, \ldots, a \mod f_n) = (\chi_1(a), \ldots, \chi_n(a))$, hvor $\chi_i(a) = a \mod f_i \in \tilde{R}_i$.
For $a \in \mathbb{F}_q[x]$ og $1 \leq i \leq n$ gælder det, at f_i går op i a hvis og kun hvis $\chi_i(a) = 0$. Det vil altså sige, at hvis $\chi_i(a) = 0$ for alle $1 \leq i \leq n$, så er $\gcd(a, f) = \texttt{lcm}(f_1, \ldots, f_n) = f$, og hvis $\chi_i(a) \neq 0$ for alle $1 \leq i \leq n$, så er $\gcd(a, f) = 1$.
I tilfælde af, at vi har valgt et polynomium, $a \in \mathbb{F}_q[x]$, $\deg(a) < n$ hvor $\gcd(a, f) = 1$, ønsker vi at finde en procedure, som omdanner a til et polynomium $\alpha \in \mathbb{F}_q[x]$, hvor $\gcd(\alpha, f)$ med stor sandsynlighed er en ikke-triviel faktor i f.

For at beskrive en sådan procedure, betragtes først den stokastiske variable Y, som angiver et vilkårligt polynomium $a \in \mathbb{F}_q[x]/\langle f\rangle$ med lige stor sandsynlighed. Det vil sige, at Y er ligefordelt på $\mathbb{F}_q[x]/\langle f\rangle$, hvormed sandsynligheden for

at udtage et element i $\mathbb{F}_q[x]/\langle f\rangle$ er $P(Y=a)=\frac{1}{q^n}$.
Det ønskes herefter bevist, at de stokastiske variable $\chi_1(Y),\ldots,\chi_n(Y)$ er uafhængige og ligefordelte på $\mathbb{F}_q$.

Vi betragter derfor de marginale sandsynligheder

$$P(\chi_1(Y)=\tilde{a}_1),\ldots,P(\chi_n(Y)=\tilde{a}_n).$$

Idet χ er en isomorfi og Y er ligefordelt på $\mathbb{F}_q^n$. så er

$$P(\chi(Y)=(\tilde{a}_1,\ldots,\tilde{a}_n))=\frac{1}{q^n}. \tag{3.2}$$

Det gælder da for ethvert $1\leq i\leq n$, at

$$\begin{aligned} P(\chi_i(Y)=\tilde{a}_i) &= \sum_{\substack{\tilde{a}_k\in\tilde{R}_k,\\ k\in\{1\ldots,i-1,\\ i+1,\ldots,n\}}} P(\chi(Y)=(\tilde{a}_1,\ldots,\tilde{a}_n)) \\ &= \frac{1}{q^n}\cdot q^{n-1}=\frac{1}{q}, \end{aligned}$$

og da $\tilde{R}_i$ består af q elementer, er $\chi_i(Y)$ ligefordelt på $\mathbb{F}_q$ for alle $1\leq i\leq n$.

Det skal nu vises, at $\chi_1(Y),\ldots,\chi_n(Y)$ er uafhængige på $\mathbb{F}_q$.
Dette er tilfældet, hvis

$$P(\chi(Y)=(\tilde{a}_1,\ldots,\tilde{a}_n))=P(\chi_1(Y)=\tilde{a}_1)\cdots P(\chi_n(Y)=\tilde{a}_n).$$

Da vi lige har vist, at $\chi_1(Y),\ldots,\chi_n(Y)$ alle er ligefordelte er

$$P(\chi_1(Y)=\tilde{a}_1)\cdots P(\chi_n(Y)=\tilde{a}_n)=\frac{1}{q}\cdots\frac{1}{q}=\frac{1}{q^n},$$

og ved at sammenholde dette med (3.2) ses det, at $\chi_1(Y),\ldots,\chi_n(Y)$ er uafhængige stokastiske variable i $\tilde{R}_i=\mathbb{F}_q$.

I føromtalte procedure benyttes desuden følgende resultater:

Lemma 20 *Lad q være en primtalspotens, k en divisor i $q-1$ og $S=\{b^k : b\in\mathbb{F}_q^*=\mathbb{F}_q\backslash\{0\}\}$. Da gælder det, at*

(*i*) *S er en undergruppe af orden* $(q-1)/k$.

(*ii*) $S = \{a \in \mathbb{F}_q^* : a^{\frac{q-1}{k}} = 1\}$.

Bevis: S er billedet af gruppehomomorfien $\sigma_k \colon \mathbb{F}_q^* \to \mathbb{F}_q^*$ givet ved $\sigma_k(b) = b^k$, hvorved S, ifølge Sætning 92, er en multiplikativ undergruppe af $\mathbb{F}_q^*$.
Kernen af σ_k er:

$$\ker \sigma_k = \{a \in \mathbb{F}_q^* \,:\, \sigma_k(a) = 1\} = \{a \in \mathbb{F}_q^* \,:\, a^k = 1\}.$$

Da $\mathbb{F}_q$ er et legeme, så har polynomiet $x^k - 1 \in \mathbb{F}_q[x]$ højst k rødder i $\mathbb{F}_q$, hvormed $\#\ker \sigma_k \leq k$.
Idet $(b^k)^{\frac{q-1}{k}} = b^{q-1} = 1$ for alle b tilhørende $\mathbb{F}_q^*$, så er $S \subseteq \ker \sigma_{(q-1)/k}$. Analogt til forklaringen ovenfor gælder det derfor, at $\#S \leq \#\ker \sigma_{(q-1)/k} \leq \frac{q-1}{k}$.
Idet σ er en gruppehomomorfi, gælder det, ifølge Sætning 93, at ækvivalensklasserne i $\mathbb{F}_q^*$, er lige store. Dermed har vi, at

$$q - 1 = \#\mathbb{F}_q^* = \#\ker \sigma_k \cdot \#\mathrm{im}\, \sigma_k = \#\ker \sigma_k \cdot \#S \leq k \cdot \frac{q-1}{k} = q - 1.$$

Det må hermed gælde, at $\#\ker \sigma_k \cdot \#S = k \cdot \frac{q-1}{k}$, og altså er $\#\ker \sigma_k = k$ og $\#S = \frac{q-1}{k}$. Da vi tidligere viste, at $S \subseteq \ker \sigma_{(q-1)/k}$ og $\#\ker \sigma_{(q-1)/k} \leq \frac{q-1}{k}$, så er $S = \{a \in \mathbb{F}_q^* : a^{\frac{q-1}{k}} = 1\}$. □

Ved at sætte $k = 2$ fås følgende korollar:

Korollar 21 *Lad q være en primtalspotens, p^r, med ulige karakteristik p, og $S = \{a \in \mathbb{F}_q^* : \exists\, b \in \mathbb{F}_q^*,\ \text{så } a = b^2\}$, så er*

(*i*) *S en undergruppe af orden* $(q-1)/2$.

(*ii*) *og* $S = \{a \in \mathbb{F}_q^* : a^{\frac{q-1}{2}} = 1\}$.

(*iii*) $a^{\frac{q-1}{2}} \in \{1, -1\}$ *for alle* $a \in \mathbb{F}_q^*$.

Bevis: Punkt (*i*) og (*ii*) følger umiddelbart af Lemma 20 ved at erstatte k med 2.

Punkt (iii) følger af, at $a^{\frac{q-1}{2}}$ er rod i $x^2-1=(x-1)(x+1)$ for alle $a\in\mathbb{F}_q^*$. $\square$

Antag nu, at q er ulige og lad $e=\frac{q-1}{2}$.
Hvis $a\in\mathbb{F}_q[x]$, med $\deg a<n$, så gælder det, idet χ_i'erne er homomorfier, at

$$\chi_i(a^e)=\chi_i(a)^e=\varepsilon_i\in\tilde{R}_i.$$

Eftersom $\chi_i(Y)$'erne er ligefordelte på $\tilde{R}_i$'erne, vil $\chi_i(Y)$ antage alle værdier på $\tilde{R}_i$ med lige stor sandsynlighed. Dermed er $\chi_i(Y)=0$ med sandsynlighed $\frac{1}{q}$ og sandsynligheden for at $\chi_i(Y)\in\tilde{R}_i^*$ er $\frac{q-1}{q}$.
Hvis $\chi_i(a)=0$, er $\varepsilon_i=0$, men idet vi udelukkende vil koncentrere os om de tilfælde, hvor $\gcd(a,f)=1$, så betragter vi kun de situationer, hvor $\chi_i(a)\neq 0$ for alle $1\leq i\leq n$, hvorved $\varepsilon_i\in\{1,-1\}$ ifølge Korollar 21. Dette korollar giver desuden, at ε_i vil antage disse værdier lige ofte, hvilket er med sandsynlighed

$$P(\varepsilon_i=1)=P(\varepsilon_i=-1)=\frac{q-1}{2q}.$$

Betragt nu

$$\chi(a^e-1)=(\varepsilon_1-1,\ldots,\varepsilon_n-1).$$

Det gælder hermed, at $\gcd(a^e-1,f)$ er en ikke-triviel faktor for f medmindre $\varepsilon_1=\cdots=\varepsilon_n$. Dette sker med sandsynlighed $2\cdot\left(\frac{q-1}{2q}\right)^n$, da $\chi_1(Y),\ldots,\chi_n(Y)$ er uafhængige i $\mathbb{F}_q$.
Altså har vi fundet en procedure, som omdanner $a\in\mathbb{F}_q[x]$ til et polynomium $\alpha=a^e-1\in\mathbb{F}_q[x]$, således at $\gcd(\alpha,f)$ er en ikke-triviel faktor for f med sandsynlighed $1-2\cdot\left(\frac{q-1}{2q}\right)^n>\frac{1}{2}$.

Før algoritmen kan opstilles mangler vi nu kun at vise følgende lemma:

Lemma 22 *Lad $f,p,r,h\in\mathbb{F}_q[x]$. Hvis $h=p \mod f$, da er*

$$\gcd(p-r,f)=\gcd(h-r,f).$$

Bevis: Det gælder, at $h=p \mod f$. Det vil sige, at $p=qf+h$, hvor $q\in\mathbb{F}_q[x]$ og $\deg h<\deg q$.
Dermed er $p-r=qf+(h-r)$.

Antag, at $d_1 = \gcd(p-r, f)$ og $d_2 = \gcd(h-r, f)$.
Dermed gælder det udfra ovenstående, at d_1 går op i $h-r$ og d_2 går op i $p-r$. Da $\mathbb{F}_q[x]$ er et entydigt faktoriseringsområde, gælder der, idet $d_1|(h-r)$ og $d_1|f$, at $d_1|(\gcd(h-r, f) = d_2)$. Tilsvarende vil $d_2|d_1$, hvormed $d_1 = d_2$. □

I Algoritme 23 er $p = a^{\frac{q-1}{2}}$, $r = 1$ og $h = b$.

Algoritme 23 (Equal-degree spaltning)
Input: Et kvadratfrit monisk polynomium $f \in \mathbb{F}_q[x]$ af grad $n > 0$, med $q = p^r$, hvor q har ulige karakteristik p, sådan at alle irreducible faktorer i f har grad 1.
Output: En ikke-triviel monisk faktor $g \in \mathbb{F}_q[x]$ i f eller "failure".

1. *Vælg $a \in \mathbb{F}_q[x]$, hvor $\deg a < n$, tilfældigt*
   if $a \in \mathbb{F}_q$ **then return** *"failure"*
2. $g_1 := \gcd(a, f)$
   if $g_1 \neq 1$ **then return** g_1 **else**
3. **call** *Algoritme 17 i $\tilde{R} = \mathbb{F}_q[x]/\langle f \rangle$ for at beregne $b = a^{\frac{q-1}{2}} \mod f$*
4. $g_2 := \gcd(b-1, f)$
   if $g_2 \neq 1$ *og* $g_2 \neq f$ **then return** g_2 **else return** *"failure"*

Sandsynligheden for at denne algoritme giver en ikke-triviel faktor for f er

$$P(E) + \left(1 - 2 \cdot \left(\frac{q-1}{2q}\right)^n\right) > \frac{1}{2},$$

hvor $P(E)$ er sandsynligheden for at algoritmen giver en ikke-triviel faktor for f i trin 2, og $1-2\cdot\left(\frac{q-1}{2q}\right)^n$ er sandsynligheden for at algorimen giver en ikke-triviel faktor for f i trin 4.
Sandsynligheden for, at vores output bliver failure er

$$P(F) = 1 - \left(P(E) + \left(1 - 2 \cdot \left(\frac{q-1}{2q}\right)^n\right)\right) < \frac{1}{2}.$$

Dermed bliver sandsynligheden for failure, efter at have gentaget algoritmen t gange, mindre end $\left(\frac{1}{2}\right)^t$, idet valgene af polynomier i $\mathbb{F}_q[x]$ er uafhængige.

3.2.2 Equal degree spaltning -karakteristik 2

I forrige afsnit blev der opstillet en algoritme til at bestemme faktorer i et polynomium bestående af irreducible faktorer af samme grad, $f = f_1 \cdots f_n \in \mathbb{F}_q[x]$, hvor $\deg f_i = \deg f_j = 1$ for $1 \leq i < j \leq n$.
Denne algoritme virker kun i de tilfælde, hvor karakteristikken af legemet, $\mathbb{F}_q$, er ulige, så i dette afsnit vil vi opstille en algoritme, som kan benyttes når karakteristikken af legemet er 2.
Princippet, for at opstille denne algoritme, er den samme som i forrige afsnit. Vi ønsker endnu engang at benytte den isomorfe afbildning

$$\chi : \tilde{R} \to \tilde{R}_1 \times \cdots \times \tilde{R}_n,$$

hvor $\tilde{R} = \mathbb{F}_q[x]/\langle f \rangle$, og $\tilde{R}_i = \mathbb{F}_q[x]/\langle f_i \rangle$, og

$$\chi(a \mod f) = (\chi_1(a), \ldots, \chi_n(a)) = (a \mod f_1, \ldots, a \mod f_n),$$

for $a \in \mathbb{F}_q[x]$.

Er $\chi_i(a) = 0$, for $a \in \mathbb{F}_q[x]$ og $1 \leq i \leq n$, så er dette ækvivalent med, at polynomiet f_i går op i a. Det vil sige, at hvis $\chi_i(a) = 0$ for alle $i \in \{1, \ldots, n\}$, da er $\gcd(a, f) = f_1 \cdots f_n = f$.
Gælder det derimod, at $\chi_i(a) \neq 0$, for alle $i \in \{1, \ldots, n\}$, så har polynomierne f og a ingen fælles ikke-trivielle faktorer.
Hvis der er valgt et polynomium $a \in \mathbb{F}_q[x]$ med $\deg(a) < k$, hvor $\gcd(a, f) = 1$, ønsker vi som tidligere at bestemme en procedure, som omdanner polynomiet a til et polynomium α, hvor største fællesdivisor mellem f og α med stor sandsynlighed ikke er en triviel faktor i f.

Vi ønsker at bestemme en funktion, T, sådan, at

1. $T(c) \in \mathbb{F}_2$ for alle $c \in \tilde{R}_i = \mathbb{F}_q = \mathbb{F}_{2^r}$.
2. Elementerne 0 og 1 bliver ramt lige mange gange af $T(c)$, for $c \in \mathbb{F}_q = \tilde{R}_i$. Det vil sige, at der er 2^{r-1} c'er, som rammer 0, og 2^{r-1} c'er, der rammer 1.

Det skal nu vises, at trace afbildningen, givet som i Definition 45, hvor c tilhører $\mathbb{F}_{2^r} = \mathbb{F}_q$, opfylder de to betingelser.

Det vil sige, at vi har afbildningen

$$\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x) = x^{2^{r-1}} + x^{2^{r-2}} + \cdots + x^2 + x,$$

Der gælder da, ifølge Lemma 80, og da vi regner over $\mathbb{F}_{2^r}$, at

$$\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)+1) = \mathtt{Tr}^2_{\mathbb{F}_q/\mathbb{F}_2}(x) + \mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x) = x^{2^r} - x.$$

Udfra kommentaren efter Lemma 79 er rødderne til $x^{2^r} - x$ alle elementerne i $\mathbb{F}_{2^r}$, og hermed er alle c'er tilhørende $\mathbb{F}_q$ rod i enten $\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)$ eller $\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)+1$. Dette vil sige, at $\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c) = 0$ eller $\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c) = 1$, hvormed punkt 1 er vist.

Punkt 2 er opfyldt, idet alle $c \in \mathbb{F}_q$ er rod i enten $\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)$ eller $\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)+1$, og $\deg(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)) = \deg(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(x)+1) = 2^{r-1}$.
Hermed må der være 2^{r-1} c'er, som rammer 0, og ligeledes 2^{r-1} c'er, der rammer 1.

Der gøres i Afsnit 5.1 rede for, at disse to punkter er opfyldt for en vilkårlig traceafbildning givet ved

$$\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x^{q^{m-1}} + x^{q^{m-2}} + \cdots + x^q + x.$$

Altså vises det, at billedet af $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)$ er $\mathbb{F}_q$, og at disse q elementer rammes lige ofte.

Lad a tilhøre $\mathbb{F}_q[x]$, så er

$$\chi(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a) \mod f) = (\chi_1(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)), \ldots, \chi_n(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a))).$$

Idet χ_i, for alle $i \in \{1, \ldots, n\}$, er en homomorfi gælder følgende:

$$\begin{aligned}
\chi_i(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)) &= \chi_i(a^{2^{r-1}} + a^{2^{r-2}} + \cdots + a^2 + a) \\
&= \chi_i(a^{2^{r-1}}) + \chi_i(a^{2^{r-2}}) + \cdots + \chi_i(a) \\
&= (\chi_i(a))^{2^{r-1}} + (\chi_i(a))^{2^{r-2}} + \cdots + \chi_i(a) \\
&= \mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\chi_i(a)),
\end{aligned}$$

og da $\chi_i(a)$, for $a \in \mathbb{F}_q[x]$, tilhører $\tilde{R}_i = \mathbb{F}_q$, så vil $(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(\chi_i(a)) \in \{0,1\}$.
Herved vil n-tuplen $(\chi_1(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)), \ldots, \chi_n(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a)))$ bestå af 0 eller 1 på hver plads.

Hvis ikke der tages højde for, at $\gcd(a, f) = 1$, så vil $\chi_i(\mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a))$ antage værdierne 0 og 1 med sandsynlighed en halv hver. Dette følger af punkt 2 samt af, at de stokastiske variable $\chi_1(Y), \ldots, \chi_n(Y)$ er ligefordelte i $\mathbb{F}_q$, hvilket blev vist i forrige afsnit.
Endvidere blev det vist, at de stokastiske variable $\chi_1(Y), \ldots, \chi_n(Y)$ er uafhængige, hvormed sandsynligheden for, at alle pladser i n-tuplen har samme værdi er $2(\frac{1}{2})^n$.

Det er nu muligt at opstille en algoritme til at bestemme en ikke-triviel faktor i polynomiet $f = f_1 \cdots f_n \in \mathbb{F}_q[x]$, hvor f_i er irreducibel og af grad 1 når $\mathbb{F}_q = \mathbb{F}_{2^r}$. I Algoritmens punkt 3 og 4 benyttes Lemma 22 endnu engang.

Algoritme 24 (Equal-degree spaltning)
Input: Et kvadratfrit monisk polynomium $f \in \mathbb{F}_q[x]$ af grad $n > 0$, hvor $q = 2^r$, sådan at alle irreducible faktorer i f har grad 1.
Output: En ikke-triviel monisk faktor $g \in \mathbb{F}_q[x]$ i f eller "failure".

1. *Vælg $a \in \mathbb{F}_q[x]$, hvor $\deg a < n$, tilfældigt*
   if $a \in \mathbb{F}_q$ **then return** *"failure"*

2. $g_1 := \gcd(a, f)$
   if $g_1 \neq 1$ **then return** g_1 **else**

3. **call** *Algoritme 17 i $\tilde{R} = \mathbb{F}_q[x]/\langle f \rangle$ gentagne gange for at beregne $b = \mathtt{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a) \operatorname{rem} f$*

4. $g_2 := \gcd(b, f)$
   if $g_2 \neq 1$ *og* $g_2 \neq f$ **then return** g_2 **else return** *"failure"*

Sandsynligheden for, at algoritmen giver en ikke-triviel faktor er

$$P(E) + P(\overline{E}) > P(E) + \left(1 - 2\left(\frac{1}{2}\right)^n\right) > \frac{1}{2},$$

hvor $P(E)$ er sandsynligheden for, at algoritmen giver en ikke-triviel faktor i trin 2, og $P(\overline{E})$ er sandsynligheden for, at algoritmen giver en ikke-triviel faktor i trin 4.

Igen er sandsynligheden for at få failure i vores output

$$P(F) = 1 - \big(P(E) + P(\overline{E})\big) < 1 - \left(P(E) + \left(1 - 2\left(\frac{1}{2}\right)^n\right)\right) < \frac{1}{2}.$$

Sandsynligheden for failure efter at have kaldt algoritmen t gange er dermed mindre end $\left(\frac{1}{2}\right)^t$, idet valgene af polynomier igen er uafhængige.

3.2.3 Bestemmelse af rødder

I de to foregående afsnit fandt vi ikke-trivielle faktorer til et polynomium bestående af et produkt af irreducible faktorer af grad 1. I dette afsnit ønsker vi at faktorisere disse ikke-trivielle faktorer til de irreducible faktorer.

Algoritme 25 (Equal-degree faktorisering)
Input: Et kvadratfrit monisk polynomium $f \in \mathbb{F}_q[x]$ af grad $n > 0$, sådan at alle irreducible faktorer af f har grad 1.
Output: De moniske irreducible faktorer af f tilhørende $\mathbb{F}_q[x]$.

1. **if** $n = 1$ **then return** f **else**
2. **if** *q har ulige karakteristik* **then call** *Algoritme 23 med f som input indtil der returneres en ikke-triviel faktor $g \in \mathbb{F}_q[x]$ af f*
3. **else call** *Algoritme 24 med f som input indtil der returneres en ikke-triviel faktor $g \in \mathbb{F}_q[x]$ af f*
4. **call** *algoritmen rekursivt med input g og input $\frac{f}{g}$*
   return *resultatet af de to rekursive kald*

Denne algoritme vil stoppe når graden af alle vores input er lig graden af de irreducible faktorer.

I efterfølgende algoritme kan inputtet være et hvilket som helst polynomium, som det derpå er muligt, at bestemme de irreducible lineære faktorer til.

Algoritme 26 (Bestemmelse af rødder over endelige legemer)
Input: Et ikke-konstant polynomium $f \in \mathbb{F}_q[x]$.
Output: De forskellige rødder til f i $\mathbb{F}_q$.

3. Bestemmelse af førstegradsfaktorer i $Q(x,y)$

1. **call** *Algoritme 17 i* $\tilde{R} = \mathbb{F}_q[x]/\langle f \rangle$ *til at bestemme* $h = x^q \operatorname{rem} f$
2. $g := \gcd(h - x, f)$, $r := \deg g$
   if $r = 0$ **then return** $\emptyset$ **else**
3. **call** *Algoritme 25 til at bestemme de irreducible faktorer* $x - u_1, \ldots, x - u_r$ *af* g
4. **return** $u_1, \ldots, u_r$

Trin 2 giver et kvadratfrit polynomium, hvorved det er tilladt at kalde Algoritme 25 i trin 3.
Gyldigheden af algoritmen følger da af Algoritme 17, Algoritme 25 og Lemma 22, samt af, at det at bestemme lineære faktorer, tilhørende $\mathbb{F}_q[x]$, i f svarer til at faktorisere $\gcd(x^q - x, f)$, idet $x^q - x = \prod_{u_i \in \mathbb{F}_q}(x - u_i)$.

For at bestemme de lineære faktorer til $Q(x,y)$ på formen $y - f(x)$, hvor $\deg(f(x)) < k$, bestemmes altså først rødderne i $\mathbf{E}$ til $\varphi(Q(x,y))$ ved hjælp af Algoritme 26, hvor inputtet er $\varphi(Q(x,y)) \in \mathbf{E}[y]$.
Herefter indsættes disse rødder i interpolationspolynomiet, $Q(x,y)$, for at afgøre om de også er rødder hertil.

Kapitel 4

Gröbner basis teori

Formålet med dette kapitel er at få defineret Gröbner baser og beskrive nogle af disses egenskaber, da dette ligger til grund for nogle af de resultater, vi senere får brug for. Først kræves dog nogle indledende definitioner og resultater, såsom Dicksons lemma og Hilberts basis sætning.

Vi vil gennem resten af rapporten lade $\mathbf{K}$ betegne et vilkårligt legeme, med mindre andet er antaget.

Kapitlet er baseret på [2, Kapitel 2].

4.1 Dicksons lemma

Dette afsnit vil belyse monomielle idealer, og i Dicksons lemma vil det blive vist, at et monomielt ideal er endeligt genereret.

Definition 27 (Monomielt ideal) *Et ideal $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$ er et monomielt ideal, hvis der er en delmængde $A \subseteq \mathbb{N}_0^n$, sådan at I består af alle polynomier, som er endelige summer på formen $\sum_{\alpha \in A} h_\alpha x^\alpha$, hvor $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\alpha_i \geq 0$, og $h_\alpha \in \mathbf{K}[x_1, \ldots, x_n]$. I dette tilfælde skrives $I = \langle x^\alpha : \alpha \in A \rangle$.*

Ved at benytte følgende lemma kan det afgøres, hvorvidt et monomium tilhører et monomielt ideal.

Lemma 28 *Lad $I = \langle x^\alpha : \alpha \in A \rangle$ være et monomielt ideal. Et monomium, x^β, ligger i I hvis og kun hvis x^β er divisibel med x^α for et $\alpha \in A$.*

Bevis: Hvis x^β er divisibel med x^α for et $\alpha \in A$, så gælder det, at $x^\beta = hx^\alpha$, hvor $h \in \mathbf{K}[x_1, \ldots, x_n]$. Så pr. definition af et ideal vil $x^\beta \in I$.

Hvis $x^\beta \in I$, så er $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, hvor $h_i \in \mathbf{K}[x_1, \ldots, x_n]$ og $\alpha(i) \in A$. Ved at skrive h_i som en linearkombination af monomier, ses det, at ethvert led på højresiden er divisibelt med et eller andet $x^{\alpha(i)}$. Da venstresiden kun består af ét monomium vil leddene på højresiden ophæve hinanden således, at kun et enkelt monomium er tilbage. Da der specielt gælder for dette monomium, at det er divisibelt med et $x^{\alpha(i)}$, vil x^β være divisibelt med dette $x^{\alpha(i)}$. □

Næste lemma viser, at man kan afgøre om et polynomium f tilhører I, ved at afgøre om de monomier, som f består af, tilhører I.

Lemma 29 *Lad I være et monomielt ideal, og $f \in \mathbf{K}[x_1, \ldots, x_n]$. Så er følgende ækvivalent:*

(*i*) *$f \in I$.*

(*ii*) *Ethvert led i f tilhører I.*

(*iii*) *f er en linearkombination af monomierne i I, hvor koefficienterne tilhører $\mathbf{K}$.*

Bevis: (*iii*) $\Rightarrow$ (*ii*): Da f er en linearkombination af monomierne i I med koefficienter i $\mathbf{K}$, vil ethvert led i f tilhøre I, da dette netop er et krav for at være et ideal.

(*ii*) $\Rightarrow$ (*i*): Ethvert led i f tilhører I, og pr. definition af et ideal, så tilhører summen også I.

$(i) \Rightarrow (iii)$: Idet f tilhører $I = \langle x^\alpha : \alpha \in A \subseteq \mathbb{N}_0^n \rangle$, så kan f skrives på formen $f = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, hvor $h_i \in \mathbf{K}[x_1, \ldots, x_n]$. Hvert led i $h_i x^{\alpha(i)}$ tilhører I, idet hvert led er divisibelt med $x^{\alpha(i)}$. Desuden har leddene koefficienter i $\mathbf{K}$, da h_i tilhører $\mathbf{K}[x_1, \ldots, x_n]$. Det vil sige, at f er en linearkombination af monomier i I med koefficienter i $\mathbf{K}$. □

Samspillet mellem punkt (i) og punkt (iii) giver, at et monomielt ideal er entydigt bestemt af dets monomier. Dette giver, at to monomielle idealer er ens, hvis og kun hvis de indeholder de samme monomier, hvilket benyttes i beviset for Dicksons lemma, som er følgende:

Sætning 30 (Dicksons lemma) *Et monomielt ideal $I = \langle x^\alpha : \alpha \in A \rangle \subseteq \mathbf{K}[x_1, \ldots, x_n]$ kan skrives på formen $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, hvor $\alpha(1), \ldots, \alpha(s) \in A$. Specielt har I en endelig basis.*

Bevis: Beviset føres ved induktion i antallet af variable.

Basistrin: Hvis $n = 1$, så er I genereret af monomierne x_1^α, hvor $\alpha \in A \subseteq \mathbb{N}_0$. Lad β være det mindste element i A. Så er $\beta \leq \alpha$ for alle $\alpha \in A$. Dermed vil x_1^β gå op i alle andre generatorer x_1^α. Heraf ses det, at $I = \langle x_1^\beta \rangle$.

Induktionshypotese: Antag, at $n > 1$ samt, at sætningen gælder for $n - 1$.

Induktionstrin: De variable skrives i det følgende som $x_1, \ldots, x_{n-1}, y$. Dermed skrives monomierne i $\mathbf{K}[x_1, \ldots, x_{n-1}, y]$ som $x^\alpha y^m$, hvor $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}_0^{n-1}$ og $m \in \mathbb{N}_0$.

Lad $I \subseteq \mathbf{K}[x_1, \ldots, x_{n-1}, y]$ være et monomielt ideal. For at finde generatorerne for I betragtes "projektionen", J, af I på $\mathbf{K}[x_1, \ldots, x_{n-1}]$. J er det ideal i $\mathbf{K}[x_1, \ldots, x_{n-1}]$, som er genereret af monomierne x^α, for hvilke det gælder, at $x^\alpha y^m \in I$ for mindst et $m \geq 0$.

Pr. induktionshypotese gælder det hermed, at J er genereret af endeligt mange af x^α'erne, $J = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. Udfra definitionen af J vil der for alle i mellem 1 og s eksistere $m_i \geq 0$, sådan at $x^{\alpha(i)} y^{m_i}$ tilhører I. Da J er genereret af endeligt mange monomier vil der findes en største værdi af m_i'erne. Betegn denne værdi m.

Betragt, for hvert k mellem 0 og $m-1$, idealet $J_k \subseteq \mathbf{K}[x_1, \ldots, x_{n-1}]$, som er genereret af monomierne x^β for hvilke det gælder, at $x^\beta y^k \in I$.

Ved endnu engang at benytte induktionshypotesen ses det, at J_k er genereret af endeligt mange monomier, $J_k = \langle x^{\alpha_k(1)}, \ldots, x^{\alpha_k(s_k)} \rangle$.

Lad I^* være genereret af monomierne:

$$\begin{aligned}
\textit{fra } J &: x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m \\
\textit{fra } J_0 &: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)} \\
\textit{fra } J_1 &: x^{\alpha_1(1)}y, \ldots, x^{\alpha_1(s_1)}y \\
&\vdots \\
\textit{fra } J_{m-1} &: x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}
\end{aligned}$$

Det skal nu vises, at $I = I^*$.

Udfra konstruktionen af J'erne er det klart, at monomierne i I^* er en delmængde af monomierne i I.

Hvis det kan vises, at alle monomierne i I er divisible med et i I^*, så gælder det ifølge Lemma 28, at monomierne i I er en delmængde af monomierne i I^*.

Antag $x^\alpha y^p \in I$. Hvis $p \geq m$, så er $x^\alpha y^p$ divisibelt med et $x^{\alpha(i)}y^m$, idet $x^{\alpha(i)}$ tilhører den genererende mængde for J. Hvis derimod $p \leq m-1$, så er $x^\alpha y^p$ divisibelt med et $x^{\alpha_p(j)}y^p$ ifølge konstruktionen af J_p.
Dermed er det vist, at monomierne i I er en delmængde af monomierne i I^*. Altså indeholder I og I^* de samme monomier, hvormed $I = I^*$.

Til sidst skal det vises, at en given mængde af generatorer for et ideal kan udtyndes til en endelig genererende mængde for idealet.

Lad $x_1, \ldots, x_n$ være de variable. Så er det monomielle ideal $I = \langle x^\alpha : \alpha \in A \rangle \subseteq \mathbf{K}[x_1, \ldots, x_n]$. Det skal vises, at I er genereret af endeligt mange af x^α'erne.

Fra tidligere i beviset ved vi, at der findes en endelig genererende mængde for $I = I^* = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$. Da $x^{\beta(i)} \in I = \langle x^\alpha : \alpha \in A \rangle$, så gælder det fra Lemma 28, at alle $x^{\beta(i)}$'erne er divisible med $x^{\alpha(i)}$, for et $\alpha(i) \in A$. Det vil sige, at $x^{\beta(i)} = x^{\gamma(i)}x^{\alpha(i)}$, hvor $\gamma(i) \in \mathbb{N}_0^n$.

Så ethvert element i I kan skrives på formen:

$$f = \sum_{i=0}^{s} h_i x^{\beta(i)} = \sum_{i=0}^{s} h_i x^{\gamma(i)} x^{\alpha(i)},$$

hvor $h_i \in \mathbf{K}[x_1, \ldots, x_n]$.

Altså er $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. □

Det vil sige, at ethvert monomielt ideal er endeligt genereret, og at det er muligt at udtynde en given genererende mængde for et ideal til en endelig genererende mængde. Dette benyttes i næste afsnit til at vise Hilberts basis sætning.

4.2 Hilberts basis sætning og Gröbner baser

I dette afsnit bevises Hilberts basis sætning, som siger, at alle idealer er endeligt genererede. Herefter kan Gröbner baser defineres.

Allerførst skal monomiel ordning defineres, da dette er nødvendigt for at holde styr på monomierne i et polynomium.

Definition 31 (Monomiel ordning) *En monomiel ordning på* $\mathbf{K}[x_1, \ldots, x_n]$ *er enhver relation* $\prec$ *på* $\mathbb{N}_0^n$*, eller ækvivalent, enhver relation* $\prec$ *på mængden af monomier,* x^α*,* $\alpha \in \mathbb{N}_0^n$*, som opfylder, at:*

(*i*) $\prec$ *er en total ordning på* $\mathbb{N}_0^n$*.*

(*ii*) *Hvis* $\alpha \prec \beta$ *og* $\gamma \in \mathbb{N}_0^n$*, så er* $\alpha + \gamma \prec \beta + \gamma$*.*

(*iii*) $\prec$ *er en velordning på* $\mathbb{N}_0^n$*.*

En total ordning, er en ordning, hvori præcis ét af følgende tre udsagn er opfyldt:

$$\alpha \prec \beta, \qquad \alpha = \beta, \qquad \alpha \succ \beta.$$

En velordning vil sige, at enhver ikke-tom delmængde af $\mathbb{N}_0^n$ har et mindste element under $\prec$.

Er der fastsat en monomiel ordning, kan følgende begreber defineres for et polynomium.

Definition 32 *Lad $f = \sum_\alpha a_\alpha x^\alpha \neq 0$ tilhøre $\mathbf{K}[x_1, \ldots, x_n]$, og lad $\prec$ være en monomiel ordning. Da benyttes følgende terminologi:*

(*i*) ***Multigrad** af f er*

$$mdeg(f) = \max\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\},$$

hvor maximum er taget med hensyn til $\prec$.

(*ii*) ***Ledende koefficient** for f er*

$$\mathtt{LC}(f) = a_{mdeg(f)} \in \mathbf{K}.$$

(*iii*) ***Ledende monomium** for f er*

$$\mathtt{LM}(f) = x^{mdeg(f)}.$$

(*iv*) ***Ledende term** for f er*

$$\mathtt{LT}(f) = \mathtt{LC}(f) \cdot \mathtt{LM}(f).$$

For multigraden af polynomier er følgende opfyldt.

Lemma 33 *Lad $f, g \in \mathbf{K}[x_1, \ldots, x_n]$ være forskellige fra nulpolynomiet. Så gælder det, at*

$$\textit{Hvis } f + g \neq 0, \textit{ så er } mdeg(f+g) \leq \max\{mdeg(f), mdeg(g)\}.$$

Bevis: Lad $f = \sum_\alpha a_\alpha x^\alpha$ og $g = \sum_\beta b_\beta x^\beta$. Antag, at $\mathtt{LT}(f) = -\mathtt{LT}(g)$, det vil sige, at $mdeg(f) = mdeg(g)$, så er

$$mdeg(f+g) < \max\{mdeg(f), mdeg(g)\}.$$

Hvis derimod $\mathtt{LT}(f) \neq -\mathtt{LT}(g)$, det vil sige, enten er $mdeg(f) \neq mdeg(g)$, eller også er $mdeg(f) = mdeg(g)$ og $\mathtt{LC}(f) \neq -\mathtt{LC}(g)$. I begge tilfælde gælder det, da den monomielle ordning er total, at

$$mdeg(f+g) = \max\{mdeg(f), mdeg(g)\}.$$

□

For en fastsat monomiel ordning kan det ledende term, $\mathtt{LT}(f)$, af et polynomium $f \in \mathbf{K}[x_1, \ldots, x_n]$ bestemmes. Dermed kan man for ethvert ideal definere idealet af ledende termer således.

Definition 34 *Lad $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$ være et ideal forskellig fra $\{0\}$, og lad $\mathtt{LT}(I)$ betegne mængden af ledende termer af elementerne i I. Det vil sige, at*

$$\mathtt{LT}(I) = \{cx^\alpha : \textit{der eksisterer } f \in I, \textit{hvor } \mathtt{LT}(f) = cx^\alpha\}.$$

Da er $\langle \mathtt{LT}(I) \rangle$ idealet genereret af elementerne i $\mathtt{LT}(I)$.

Det kan desuden vises, at $\langle \mathtt{LT}(I) \rangle$ er endeligt genereret.

Proposition 35 *Lad $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$ være et ideal.*

(*i*) *$\langle \mathtt{LT}(I) \rangle$ er et monomielt ideal.*

(*ii*) *Der findes $g_1, \ldots g_t \in I$ sådan, at $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$.*

Bevis: (*i*) De ledende monomier $\mathtt{LM}(g)$ af elementer $g \in I - \{0\}$ genererer det monomielle ideal $\langle \mathtt{LM}(g) : g \in I - \{0\} \rangle$.
Idet $\mathtt{LM}(g)$ og $\mathtt{LT}(g)$ kun afviger med en konstant forskellig fra nul, så genererer dette ideal det samme som $\langle \mathtt{LT}(g) : g \in I - \{0\} \rangle = \langle \mathtt{LT}(I) \rangle$. Dermed er $\langle \mathtt{LT}(I) \rangle$ et monomielt ideal.

(*ii*) Da $\langle \mathtt{LT}(I) \rangle$ er genereret af monomierne $\mathtt{LM}(g), g \in I - \{0\}$, så giver Dicksons lemma, at $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LM}(g_1), \ldots, \mathtt{LM}(g_t) \rangle$ for endeligt mange $g_1, \ldots, g_t \in I$. Da $\mathtt{LM}(g_i)$ udelukkende adskiller sig fra $\mathtt{LT}(g_i)$ med en konstant forskellig fra nul,

følger det, at $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. □

Hilberts basis sætning giver nu samme resultat for polynomielle idealer, som Dicksons lemma giver for monomielle idealer.

Sætning 36 (Hilberts Basis Sætning) *Ethvert ideal $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$ har en endelig genererende mængde, som er $I = \langle g_1, \ldots, g_t \rangle$ for nogle $g_1, \ldots, g_t \in I$.*

Bevis: Er $I = \{0\}$, kan den endelige genererende mængde vælges til at være $\{0\}$.

Hvis I indeholder polynomier forskellige fra nulpolynomiet, så kan en endelig genererende mængde $g_1, \ldots, g_t$ for I konstrueres som følgende.

Af Proposition 35 har vi, at der eksisterer $g_1, \ldots, g_t \in I$ sådan, at $\langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$.

Idet alle g_i'erne tilhører I, så gælder det, at $\langle g_1, \ldots, g_t \rangle \subseteq I$.
Lad nu $f \in I$ være et polynomium. Ved at benytte divisionsalgoritmen for polynomier i flere variable til division af f med $(g_1, \ldots, g_t)$ fås udtrykket

$$f = a_1 g_1 + \cdots + a_t g_t + r,$$

hvor intet led i r er divisibelt med $\mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t)$.
Det skal nu vises, at $r = 0$.
Først ses det, at

$$r = f - a_1 g_1 - \cdots - a_t g_t \in I.$$

Hvis $r \neq 0$, så vil $\mathtt{LT}(r) \in \langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$, og af Lemma 28 vides det, at $\mathtt{LT}(r)$ er divisibel med et eller andet $\mathtt{LT}(g_i)$. Dette er i modstrid med, at r er et restled, så derfor må det gælde, at $r = 0$. Det vil sige, at

$$f = a_1 g_1 + \cdots + a_t g_t \in \langle g_1, \ldots, g_t \rangle.$$

Da f er vilkårligt valgt, vil $I \subseteq \langle g_1, \ldots, g_t \rangle$, og så er $I = \langle g_1, \ldots, g_t \rangle$, og dermed endeligt genereret. □

Det er muligt at finde flere genererende mængder for samme ideal, men nogle viser sig mere anvendelige end andre, og disse kaldes Gröbner baser.

Definition 37 (Gröbner basis) *Fastsæt en monomiel ordning. En endelig delmængde $G = \{g_1, \ldots, g_t\}$, af et ideal I, er en Gröbner basis, hvis*

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

Af beviset for Hilberts basis sætning fremgår det, at en Gröbner basis, $\{g_1, \ldots, g_t\}$, udgør en basis for idealet I, og af Proposition 35 (ii) følger det desuden, at en sådan basis altid eksisterer.

Hilberts basis sætning har også betydning i beviset for næste sætning. Selvom denne ikke direkte har forbindelse til definitionen af en Gröbner basis er den relevant i forbindelse med konstruktionen af en sådan basis.

Sætning 38 (Opstigende kædes egenskab) *Lad $I_1 \subseteq I_2 \subseteq \cdots$ være en voksende kæde af idealer i $\mathbf{K}[x_1, \ldots, x_n]$. Så eksisterer der et $N \geq 1$ sådan, at*

$$I_N = I_{N+1} = \cdots .$$

Bevis: Givet den voksende kæde $I_1 \subseteq I_2 \subseteq \cdots$, betragt da mængden $I = \bigcup_{i=1}^{\infty} I_i$.

Først skal det vises, at I er et ideal.
Idet $0 \in I_i$ for alle i, så vil $0 \in I$.
Hvis $f, g \in I$, så følger det pr. definition af I, at $f \in I_i$ og $g \in I_j$ for nogle i'er og j'er. Antag, at $i \leq j$, så vil $f, g \in I_j$, da I_i'erne danner en voksende kæde, og da I_j er et ideal, vil $f + g$ tilhøre I_j og dermed også I.
Tilsvarende hvis $f \in I$ og $r \in \mathbf{K}[x_1, \ldots, x_n]$, så gælder det, at $r \cdot f \in I_i \subseteq I$.
Altså er I et ideal.

Af Hilberts basis sætning følger det, at I har en endelig genererende mængde sådan, at $I = \langle f_1, \ldots, f_t \rangle$. Enhver af disse generatorer er indeholdt i et I_j. Antag $f_i \in I_{j_i}$ for et j_i, $i = 1, \ldots, t$. Lad nu N være maximum af disse j_i'er. Da I_j'erne udgør en voksende kæde, gælder det, at $f_i \in I_N$ for alle i. Heraf følger det, at

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

Det vil sige, at kæden stabiliseres ved I_N, hvormed alle efterfølgende idealer er ens.

□

4.3 Egenskaber ved Gröbner baser

I dette afsnit vil vi beskrive en række af de anvendelige egenskaber, som Gröbner baser har, og afslutningsvis opstille en algoritme til konstruktion af en Gröbner basis.

Efterfølgende sætning viser, at man ved division af f med $G = (g_1, \ldots, g_t)$ får et entydigt bestemt restled, r, uafhængig af valg af rækkefølgen af $g_1, \ldots, g_t$, når G er en Gröbner basis.

Sætning 39 *Lad $G = \{g_1, \ldots, g_t\}$ være en Gröbner basis for et ideal $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$, og lad $f \in \mathbf{K}[x_1, \ldots, x_n]$. Da vil der findes et entydigt $r \in \mathbf{K}[x_1, \ldots, x_n]$ med følgende egenskaber:*

(*i*) *Ingen af monomierne i r er divisible med nogle af $\mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t)$.*

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

Bevis: Divisionsalgoritmen for polynomier i flere variable giver eksistens af r, og at både (*i*) og (*ii*) er opfyldt med $g = a_1 g_1 + \cdots + a_t g_t$.

For at bevise entydigheden antages det, at $f = g + r = g' + r'$ begge opfylder (*i*) og (*ii*), men at $r \neq r'$. Da vil $r - r' = g' - g \in I$, og dermed vil $\mathtt{LT}(r - r') \in \langle \mathtt{LT}(I) \rangle = \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. Dette betyder ifølge Lemma 28, at $\mathtt{LT}(r - r')$ er divisibel med et $\mathtt{LT}(g_i)$. Dette er umuligt, da intet monomium i hverken r eller r' er divisibelt med noget $\mathtt{LT}(g_i)$. Dermed må $r - r'$ være nulpolynomiet, hvilket medfører, at $r = r'$. □

Denne egenskab med hensyn til r benyttes i følgende korollar.

Korollar 40 *Lad $G = \{g_1, \dots g_t\}$ være en Gröbner basis for et ideal $I \subseteq \mathbf{K}[x_1, \dots x_n]$, og lad $f \in \mathbf{K}[x_1, \dots, x_n]$. Da vil $f \in I$, hvis og kun hvis restleddet, r, ved division af f med G er nul.*

Bevis: Hvis restleddet er nul, vil $f \in I$ på grund af divisionsalgoritmen for polynomier i flere variable. Hvis derimod $f \in I$, vil $f = f + 0$ opfylde de to betingelser i Sætning 39, og dermed er restleddet nul ved division af f med G. □

Indtil videre har vi beskæftiget os med eksistensen af Gröbner baser for ethvert ideal. Det ønskes desuden at kunne afgøre om en given basis er en Gröbner basis. I de situationer, hvor dette ikke er tilfældet, vil vi gerne kunne beskrive en algoritme, som kan finde en sådan Gröbner basis. Til dette benyttes S-polynomier.

Definition 41 (Fællesgradsmonomium og S-polynomium) *Lad $f, g \in \mathbf{K}[x_1, \dots, x_n]$ være ikke-nul polynomier.*

(i) Lad $mdeg(f) = \alpha$ og $mdeg(g) = \beta$. Da er fællesgradsmonomiet af $\mathtt{LM}(f)$ og $\mathtt{LM}(g)$ benævnt $\mathtt{LCM}(\mathtt{LM}(f), \mathtt{LM}(g)) = x^\gamma$, hvor $\gamma = (\gamma_1, \dots, \gamma_n)$ og $\gamma_i = \max(\alpha_i, \beta_i)$.

(ii) S-polynomiet for f og g defineres som

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

Det ses heraf, at S-polynomierne er konstrueret således, at de ledende termer elimineres og sådan, at koefficienterne til f og g tilhører $\mathbf{K}[x_1, \dots, x_n]$. Ved hjælp af følgende lemma benyttes S-polynomier i beviset for, om en basis er en Gröbner basis.

Lemma 42 *Antag, at det for summen $\sum_{i=1}^{s} c_i f_i$, hvor $c_i \in \mathbf{K}$ og $f_i \in \mathbf{K}[x_1, \dots, x_n]$, gælder, at $mdeg(f_i) = \delta \in \mathbb{N}_0^n$ for alle i.*

Hvis $mdeg(\sum_{i=1}^{s} c_i f_i) < \delta$*, da kan summen skrives, som*

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

hvor $c_{jk} \in \mathbf{K}$*, og* $1 \leq j, k \leq s$*. Desuden er multigraden af hvert* $S(f_j, f_k)$ *mindre end* δ*.*

Bevis: Lad $d_i = \mathtt{LC}(f_i)$. Derved bliver $\mathtt{LC}(c_i f_i) = c_i d_i$. Da hvert $c_i f_i$ har multigrad δ, og deres sum har multigrad skarpt mindre end δ, må det gælde, at $\sum_{i=1}^{s} c_i d_i = 0$.

Lad $p_i = \frac{f_i}{d_i}$. Dermed kan summen skrives som

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \\ &\quad (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s. \quad (4.1)\end{aligned}$$

Da $\sum_{i=1}^{s} c_i d_i = 0$ vil det sidste led i denne opskrivning forsvinde.
Da $\mathtt{LT}(f_i) = d_i x^{\delta}$ for alle i, vil $\mathtt{LCM}(\mathtt{LM}(f_j), \mathtt{LM}(f_k)) = x^{\delta}$ for alle par af $1 \leq j, k \leq s$. Dermed bliver

$$S(f_j, f_k) = \frac{x^{\delta}}{\mathtt{LT}(f_j)} f_j - \frac{x^{\delta}}{\mathtt{LT}(f_k)} f_k = \frac{x^{\delta}}{d_j x^{\delta}} f_j - \frac{x^{\delta}}{d_k x^{\delta}} f_k = p_j - p_k. \quad (4.2)$$

Derved får ligning (4.1) nu udseendet

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

hvilket netop er en sum på den ønskede form.

Både p_j og p_k har multigrad δ, og deres ledende koefficient er 1, hvorved multigraden af $p_j - p_k$ bliver skarpt mindre end δ, hvilket ifølge ligning (4.2) derfor også må gælde for $S(f_j, f_k)$. Dette fuldfører beviset. □

Det vises nu hvilke kriterier, der kræves for, at en delmængde af I er en Gröbner basis for I.

Sætning 43 (Buchbergers kriterie for Gröbner baser) *Lad $I = \langle g_1, \ldots, g_t \rangle$ være et polynomielt ideal. Da er $G = \{g_1, \ldots, g_t\}$ en Gröbner basis for I, hvis og kun hvis restleddet, ved division af $S(g_i, g_j)$ med G, er nul, for alle par af i, j.*

Bevis: $\Rightarrow$: $S(g_i, g_j) \in I$, da g_i og g_j tilhører I. Er G en Gröbner basis for I, giver Korollar 40, at restleddet, ved division af $S(g_i, g_j)$ med G, er nul, for alle par af i, j.

$\Leftarrow$: Lad $f \in I$ være forskellig fra nulpolynomiet. Det ønskes nu bevist, at når $S(g_i, g_j)$-polynomierne alle har rest nul ved division med G, så medfører det, at $\mathtt{LT}(f) \in \langle \mathtt{LT}(g_1), \ldots \mathtt{LT}(g_t) \rangle$. Dette vil, da f er vilkårligt valgt, give, at $\langle \mathtt{LT}(I) \rangle \subseteq \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$. Det indses let, at $\langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle \subseteq \langle \mathtt{LT}(I) \rangle$, da g_i tilhører I. Dermed er $\langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle = \langle \mathtt{LT}(I) \rangle$, og altså danner G en Gröbner basis for I.

Strategien er at tage udgangspunkt i, at når $f \in I = \langle g_1, \ldots, g_t \rangle$, så findes der polynomier $h_i \in \mathbf{K}[x_1, \ldots, x_n]$ sådan, at

$$f = \sum_{i=1}^{t} h_i g_i. \tag{4.3}$$

Lemma 33 giver da, at

$$mdeg(f) \leq \max(mdeg(h_i g_i)), \ \textit{for } i = 1, \ldots t. \tag{4.4}$$

Ved at antage, at restleddet, ved division af $S(g_i, g_j)$ med G, er nul for alle par af i, j bevises det, at $mdeg(f) = mdeg(h_i g_i)$ for et eller andet i. Dette betyder, at $\mathtt{LT}(f)$ er divisibel med $\mathtt{LT}(g_i)$, hvormed Lemma 28 giver, at $\mathtt{LT}(f) \in \langle \mathtt{LT}(g_1), \ldots, \mathtt{LT}(g_t) \rangle$, hvilket netop var det ønskede resultat.

Som sagt tages der udgangspunkt i udtrykket for f, som det står i ligning (4.3). Lad $m(i) = mdeg(h_i g_i)$, og definer $\delta = \max(m(1), \ldots, m(t))$. Det vil sige, at ligning (4.4) bliver

$$mdeg(f) \leq \delta.$$

Polynomiet f kan muligvis opskrives i forskellige variationer, dog vil alle disse være på formen som i (4.3), hvilket kan have indflydelse på størrelsen af δ.
Da der er valgt en monomiel ordning, som er velordnet, er det muligt at vælge netop den variation af ligning (4.3), som giver δ så lille som muligt. Det ønskes

nu bevist, at når dette minimale δ er valgt, vil $mdeg(f) = \delta = mdeg(h_i g_i)$ for et eller andet i, hvilket, som beskrevet ovenfor, vil fuldføre beviset.

At $mdeg(f) = \delta$ bevises ved et modstridsbevis, det vil sige, det antages, at $mdeg(f) < \delta$.

Der tages udgangspunkt i ligning (4.3). Denne kan også skrives, som

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathtt{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{4.5}$$

Leddene i de to sidste summer har alle multigrad mindre end δ, så disse to summer har begge multigrad mindre end δ. Da det er antaget, at multigraden af f er mindre end δ, må også den første sum have multigrad mindre end δ. Det vil sige, at

$$mdeg\left(\sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i\right) < \delta.$$

Lad nu $\mathtt{LT}(h_i) = c_i x^{\alpha(i)}$. Da vil summen,

$$\sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i,$$

netop have den form som er beskrevet i Lemma 42, hvor $f_i = x^{\alpha(i)} g_i$. Det er ovenfor blevet konkluderet, at $mdeg\left(\sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i\right) < \delta$, så betingelserne til Lemma 42 er opfyldt.
Dette giver, at summen kan skrives som en linearkombination af S-polynomier på formen $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$, hvor $x^\delta = \mathtt{LCM}(\mathtt{LM}(x^{\alpha(j)} g_j), \mathtt{LM}(x^{\alpha(k)} g_k))$. Det kan dog indses, at når $x^{\gamma_{jk}} = \mathtt{LCM}(\mathtt{LM}(g_j), \mathtt{LM}(g_k))$ er

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

Det vil sige, at der findes $c_{jk} \in \mathbf{K}$ sådan, at

$$\sum_{m(i)=\delta} \mathtt{LT}(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k), \tag{4.6}$$

hvor $mdeg(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta$.

Nu benyttes, betingelsen om, at $S(g_j, g_k)$ har restled nul ved division med G. Dette betyder, at ethvert S-polymonium kan skrives som

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{i,jk} g_i, \tag{4.7}$$

hvor $a_{i,jk} \in \mathbf{K}[x_1, \ldots x_n]$. Desuden vides det fra [2, Theorem 3, side 61], at

$$mdeg(a_{i,jk} g_i) \leq mdeg(S(g_j, g_k)) \text{ for alle } i, j, k. \tag{4.8}$$

Lad nu $b_{ijk} = x^{\delta-\gamma_{jk}} a_{i,jk}$, da er

$$x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i. \tag{4.9}$$

Dette giver sammen med ligning (4.8), og konklusionen fra Lemma 42, at

$$mdeg(b_{ijk} g_i) \leq mdeg(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta. \tag{4.10}$$

Ved nu at kombinere ligning (4.6) og (4.9), fås udtrykket

$$\sum_{m(i)=\delta} \mathtt{LT}(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \left(\sum_{i=1}^{t} b_{ijk} g_i \right) = \sum_{i=1}^{t} \tilde{h_i} g_i,$$

hvor $\tilde{h_i} = \sum_{j,k} c_{jk} b_{ijk}$.
Da $c_{jk} \in \mathbf{K}$, ændrer det ikke på multigraden, så det kan ses udfra ligning (4.10), at for alle i, er

$$mdeg(\tilde{h_i} g_i) < \delta$$

Ved nu at vende tilbage til ligning (4.5) ses det, at når det er antaget, at $mdeg(f) < \delta$, kan f skrives som

$$f = \sum_i \tilde{h_i} g_i + \sum_{m(i)=\delta} (h_i - \mathtt{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i.$$

Dette er en polynomiel kombination af g_i'erne, hvor alle leddene har multigrad mindre end δ. Men da vi netop havde valgt den opskrivning af f, hvor δ var mindst mulig, er det ikke muligt, at opskrive f uden at mindst ét led har multigrad lig δ. Dermed er der opnået en modstrid, hvormed det konkluderes, at under de valgte omstændigheder er $mdeg(f) = \delta$, hvilket fuldfører beviset. □

Ved hjælp af dette kriterie er det herefter muligt at opstille en algoritme til konstruktion af en Gröbner basis udfra en kendt genererende mængde.

Sætning 44 *Lad $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$ være et polynomielt ideal. Så kan en Gröbner basis for I konstrueres i et endeligt antal skridt udfra følgende algoritme.*

Input: $F = (f_1, \ldots, f_s)$
Output: En Gröbner basis $G = (g_1, \ldots, g_t)$ for I, hvor $F \subseteq G$

$G := F$
repeat
  $G' := G$
  for *hvert par* $\{p, q\}$, $p \neq q$ *i* G' **do**
    $S := \overline{S(p,q)}^{G'}$
    if $S \neq 0$ **then** $G := G \cup \{S\}$
until $G = G'$

Bevis: Hvis $G = \{g_1, \ldots, g_t\}$, så betegner $\langle G \rangle$ og $\langle \mathtt{LT}(G) \rangle$ idealerne:

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

Først skal det vises, at $G \subseteq I$ for alle trin i algoritmen. Dette er oplagt i første skridt, idet $G = F$.

Når G bliver udvidet sker dette ved at tilføje resten $S = \overline{S(p,q)}^{G'}$ for $p, q \in G$. Altså skal det vises, at $G \cup \{S\}$ er en delmængde af I. Da $G \subseteq I$, så er både p, q og herved også $S(p,q)$ i I. Det vil sige, at når $S(p,q)$ divideres med G', så kan resten, $\overline{S(p,q)}^{G'}$, skrives som summen $\overline{S(p,q)}^{G'} = r = S(p,q) - (a_1 g_1 + \cdots + a_t g_t)$, hvorved $\overline{S(p,q)}^{G'} \in I$. Hermed er $G \cup \{S\}$ en delmængde af I.

Mængden G er en basis for idealet I, da $F \subseteq G$, og F er en basis. Når algoritmen standser gælder det, at $G = G'$, hvilket betyder, at $\overline{S(p,q)}^{G'} = 0$ for alle $p, q \in G$, og udfra Sætning 43 er G en Gröbner basis for I.

Det mangler nu at blive vist, at algoritmen vil standse. For at vise dette betragtes algoritmen efter hvert skridt.

Mængden G består af G' (det foregående G) og $S \neq 0$. Da $G' \subseteq G$, så er

$$\langle \mathtt{LT}(G') \rangle \subseteq \langle \mathtt{LT}(G) \rangle. \tag{4.11}$$

Antag, at $G' \neq G$, og at $\overline{S(p,q)}^{G'} = r \neq 0$ er tilføjet G. Da r er restleddet ved division af et S-polynomium med G', så er $\mathtt{LT}(r)$ ikke divisibelt med nogle af de ledende termer i G', og hermed gælder det, at $\mathtt{LT}(r) \notin \langle \mathtt{LT}(G') \rangle$. Idet $\mathtt{LT}(r) \in \langle \mathtt{LT}(G) \rangle$, så er $\langle \mathtt{LT}(G') \rangle \subset \langle \mathtt{LT}(G) \rangle$.

Af ligning (4.11) ses det, at idealerne $\langle \mathtt{LT}(G') \rangle$ udgør en voksende kæde af idealer i $\mathbf{K}[x_1, \ldots, x_n]$. Dermed følger det af Sætning 38, at kæden stabiliseres efter et endeligt antal skridt sådan, at $\langle \mathtt{LT}(G') \rangle = \langle \mathtt{LT}(G) \rangle$ for et eller andet G'. Det vil sige, at inklusionen $\langle \mathtt{LT}(G') \rangle \subset \langle \mathtt{LT}(G) \rangle$ ikke gælder, og dermed kan det ikke gælde, at $G' \neq G$. Dette medfører, at $G = G'$, og altså standser algoritmen efter et endeligt antal skridt. □

Så for at udvide en given basis for et ideal til en Gröbner basis divideres alle S-polynomier af den genererende mængde på skift med den genererende mængde. Hvis resten ved division ikke er nul tilføjes denne til den genererende mængde, og denne undersøges på tilsvarende vis. Denne procedure fortsættes til resten ved division af alle S-polynomier er nul.

Kapitel 5

Koder udtrykt ved hjælp af norm- trace polynomier

Dette kapitel har til formål at nå frem til en beskrivelse af en type koder, som bygger på samme princip som Reed-Solomon koderne. Dog kan kodeordene i disse koder blive betydeligt længere end kodeordene i Reed-Solomon koderne.

Vi søger altså punkter og polynomier, sådan at vi, ved at evaluere polynomierne i de valgte punkter, får kodeordene i en kode, som vi vil kalde en NTP-kode. Vi vil betragte elementer fra legemet $\mathbb{F}_{q^m}$, hvor q er en primtalspotens, p^r, og $m \in \mathbb{N}\backslash\{1\}$. Er vi i det specialtilfælde, hvor $m = 2$, så kaldes koden en Hermite-kode.

5.1 Bestemmelse af punkter

Dette afsnit bygger hovedsageligt på [6, Afsnit 2.3].

Punkterne vælges til at være de $p_1 = (x_1, y_1), p_2 = (x_2, y_2), \ldots, p_n = (x_n, y_n) \in$

$\mathbb{F}_{q^m}^2$, som er nulpunkter i norm- trace polynomiet:

$$x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y. \tag{5.1}$$

Dette svarer til at bestemme varieteten $\mathbf{V}(I)$, hvor I er givet ved $\langle x^{\frac{q^m-1}{q-1}} - q^{m-1} - \cdots - y^q - y,\ x^{q^m} - x,\ y^{q^m} - y\rangle$, idet $x^{q^m} - x$ og $y^{q^m} - y$ netop har alle elementer i $\mathbb{F}_{q^m}$ som nulpunkter, se kommentaren til Lemma 79.

For at afgøre størrelsen af varieteten $\mathbf{V}(I)$, samt udseendet af de pågældende punkter introduceres trace- og norm afbildningerne.

Definition 45 (Trace afbildningen) *Lad $\alpha \in \mathbb{F}_{q^m}$, så er trace afbildningen $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ givet ved*

$$\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Leddene i $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ kaldes de konjugerede af α med hensyn til $\mathbb{F}_q$.
For at klargøre, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ altid er et element i $\mathbb{F}_q$, betragtes følgende redegørelse:

Lad $f \in \mathbb{F}_q[x]$ være minimalpolynomiet af α, af grad d, hvor $\alpha \in \mathbb{F}_{q^m}$. Da er d ifølge Sætning 76 en divisor for m. Desuden gælder det af Sætning 77, at røddderne til f i $\mathbb{F}_{q^d}$ er givet ved $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$.
Polynomiet givet ved $g(x) = f(x)^{\frac{m}{d}} \in \mathbb{F}_q[x]$, har ifølge Sætning 78 netop de konjugerede af α med hensyn til $\mathbb{F}_q$ som rødder. Så en opskrivning af dette polynomium giver

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ &= (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}). \end{aligned} \tag{5.2}$$

Ved at sammenligne koefficienter i de to ovenstående udtryk for $g(x)$, ses det, at

$$\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -a_{m-1}.$$

Heraf fremgår det, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ altid er et element i $\mathbb{F}_q$.

Dette kan også indses ved at betragte følgende:

$$(\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha))^q = (\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}})^q.$$

Ved herpå at benytte Lemma 80 gentagne gange fås:

$(\alpha+\alpha^q+\cdots+\alpha^{q^{m-1}})^q = \alpha^q+\alpha^{q^2}+\cdots+\alpha^{q^m} = \alpha^q+\cdots+\alpha^{q^{m-1}}+\alpha = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$.

Da $(\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha))^q = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ giver Lemma 79, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$.

Trace afbildningen er altså en afbildning fra $\mathbb{F}_{q^m}$ til $\mathbb{F}_q$.

Norm afbildningen defineres således:

Definition 46 (Norm afbildningen) *Lad $\alpha \in \mathbb{F}_{q^m}$. Da er norm afbildningen $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ givet ved*

$$\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}}.$$

Ved endnu engang, at sammenligne koefficienter i (5.2), ses det, at

$$\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = (-1)^m a_0.$$

Hvoraf det ses, at også norm afbildningen er en afbildning fra $\mathbb{F}_{q^m}$ over i $\mathbb{F}_q$.

Tilsvarende Traceafbildningen, kan dette også indses ved:

$$\begin{aligned}(\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha))^q &= (\alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}})^q \\ &= \alpha^q \cdot \alpha^{q^2} \cdots \alpha^{q^m} \\ &= \alpha^q \cdot \alpha^{q^2} \cdots \alpha = \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha),\end{aligned}$$

og endnu engang benyttes Lemma 79 til at konkludere, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$.

Af disse to definitioner ses det, at norm- trace polynomiet netop er givet ved $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) - \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(y)$.

Vi søger derfor de punkter (δ, β) i $\mathbb{F}_{q^m}^2$, som opfylder, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$.

Til dette formål introduceres følgende resultater vedrørende trace og norm.

Sætning 47 *Traceafbildningen $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ opfylder følgende:*

(*i*) $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha+\beta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) + \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$ *for alle $\alpha, \beta \in \mathbb{F}_{q^m}$.*

(*ii*) $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c\alpha) = c\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ *for alle* $c \in \mathbb{F}_q, \alpha \in \mathbb{F}_{q^m}$.

(*iii*) $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *er en lineær transformation fra* $\mathbb{F}_{q^m}$ *på* $\mathbb{F}_q$*, hvor både* $\mathbb{F}_{q^m}$ *og* $\mathbb{F}_q$ *betragtes som vektorrum over* $\mathbb{F}_q$.

(*iv*) $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = ma$ *for alle* $a \in \mathbb{F}_q$.

(*v*) $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ *for alle* $\alpha \in \mathbb{F}_{q^m}$.

Bevis:

(*i*) For $\alpha, \beta \in \mathbb{F}_{q^m}$ fås, ved at benytte Lemma 80, at

$$\begin{aligned}\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha+\beta) &= \alpha+\beta+(\alpha+\beta)^q+\cdots+(\alpha+\beta)^{q^{m-1}} \\ &= \alpha+\beta+\alpha^q+\beta^q+\cdots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \\ &= \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)+\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta).\end{aligned}$$

(*ii*) Hvis $c \in \mathbb{F}_q$, så gælder det som følge af Lemma 79, at $c^{q^j} = c$ for alle $j \geq 0$. Dermed fås

$$\begin{aligned}\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c\alpha) &= c\alpha+c^q\alpha^q+\cdots+c^{q^{m-1}}\alpha^{q^{m-1}} \\ &= c\alpha+c\alpha^q+\cdots+c\alpha^{q^{m-1}} \\ &= c\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha).\end{aligned}$$

(*iii*) At $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ er en lineær transformation fra $\mathbb{F}_{q^m}$ til $\mathbb{F}_q$ følger dels af punkt (*i*) og (*ii*), og dels af, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ for alle $\alpha \in \mathbb{F}_{q^m}$.
For at vise, at trace afbildningen er surjektiv, skal det vises, at der eksisterer et $\alpha \in \mathbb{F}_{q^m}$, så $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \neq 0$.
Dette er tilstrækkeligt, idet punkt (*ii*) er opfyldt, og idet alle elementer i $\mathbb{F}_q$ kan skrives på formen β^j, $0 \leq j \leq q-2$, hvor β er et primitivt element i $\mathbb{F}_q$. Ved da at lade c gennemløbe $\mathbb{F}_q$ fås samtlige elementer i $\mathbb{F}_q$.

Det gælder, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$ hvis og kun hvis α er rod i polynomiet $x^{q^{m-1}}+\cdots+x^q+x \in \mathbb{F}_q[x]$. Dette polynomium har højst q^{m-1} nulpunkter i $\mathbb{F}_{q^m}$, og da $\mathbb{F}_{q^m}$ har q^m elementer, må der eksistere $\alpha \in \mathbb{F}_{q^m}$, så $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \neq 0$.

(*iv*) Dette følger direkte fra definitionen af trace afbildningen samt Lemma 79.

(*v*) Af Lemma 79 følger det, at $\alpha^{q^m} = \alpha$ for $\alpha \in \mathbb{F}_{q^m}$. Det vil sige, at

$$\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^m} = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha).$$

□

Det fremgår af punkt (*i*) og (*ii*), at trace afbildningen er en vekorrumshomomorfi mellem de to endelige legemer $\mathbb{F}_{q^m}$ og $\mathbb{F}_q$, her begge set som vektorrum over $\mathbb{F}_q$. Dermed fremgår det af kommentaren efter beviset for Sætning 93, at ækvivalensklasserne i $\mathbb{F}_{q^m}$ alle har samme størrelse. Da det af punkt (*iii*) desuden fremgår, at trace afbildningen er surjektiv, så må størrelsen af disse ækvivalensklasser netop være $\frac{q^m}{q}$.
Det vil altså sige, at hver af de q elementer i $\mathbb{F}_q$ bliver ramt af præcis $\frac{q^m}{q}$ elementer fra $\mathbb{F}_{q^m}$.

Sætning 48 *Normafbildningen* $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *opfylder følgende:*

(*i*) $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha\beta) = \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$ *for alle* $\alpha, \beta \in \mathbb{F}_{q^m}$.

(*ii*) $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *afbilder* $\mathbb{F}_{q^m}$ *på* $\mathbb{F}_q$ *og* $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m}\backslash\{0\}$ *på* $\mathbb{F}_q^* = \mathbb{F}_q\backslash\{0\}$.

(*iii*) $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = a^m$ *for alle* $a \in \mathbb{F}_q$.

(*iv*) $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ *for alle* $\alpha \in \mathbb{F}_{q^m}$.

Bevis:

(*i*) Dette følger direkte af definitionen for norm afbildningen.

(*ii*) Fra tidligere ved vi, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ afbilder $\mathbb{F}_{q^m}$ over i $\mathbb{F}_q$. Desuden gælder det, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = 0$ hvis og kun hvis $\alpha = 0$, hvorved $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ afbilder $\mathbb{F}_{q^m}^*$ over i $\mathbb{F}_q^*$.
Punkt (*i*) viser, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ er en gruppe homomorfi mellem de to multiplikative grupper $\mathbb{F}_{q^m}^*$ og $\mathbb{F}_q^*$. Dermed er kernen af $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, pr. definition af norm, netop rødderne til polynomiet $x^{\frac{q^m-1}{q-1}} - 1$ i $\mathbb{F}_{q^m}$, og antallet af elementer, d, i kernen opfylder, at $d \leq \frac{q^m-1}{q-1}$.

Desuden giver Sætning 93, idet $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ er en gruppe homomorfi, at alle ækvivalensklasser i $\mathbb{F}_{q^m}^*$ indeholder d elementer. Det vil sige, at billedet af $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ vil indeholde $\frac{q^m-1}{d}$ elementer, og da dette er større end eller lig $q-1$, så er afbildningen $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ fra $\mathbb{F}_{q^m}^*$ til $\mathbb{F}_q^*$ surjektiv, hvormed også $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\colon \mathbb{F}_{q^m} \to \mathbb{F}_q$ er surjektiv.

(*iii*) Dette følger af definitionen på norm afbildningen samt Lemma 79.

(*iv*) Af punkt (*i*) gælder det, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^q) = \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)^q$, og af Lemma 79 gælder det, da $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)^q = \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$, hvorved sætningen er vist.

□

Det er nu muligt at bestemme de punkter, (δ, β), tilhørende $\mathbb{F}_{q^m}^2$, som opfylder $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$, samt antallet af dem.

Sætning 49 *Lad* $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle \in \mathbb{F}_{q^m}[x,y]$. *Da er størrelsen, n, af varieteten* $\mathbf{V}(I) \in \mathbb{F}_{q^m}^2$ *lig* q^{2m-1}, *og punkterne tilhørende* $\mathbf{V}(I)$ *er enten på formen:*

(*i*) $(0, \beta)$, *hvor* $\beta \in \mathbb{F}_{q^m}$ *og* $\beta^{q^{m-1}} + \cdots + \beta^q + \beta = 0$

eller

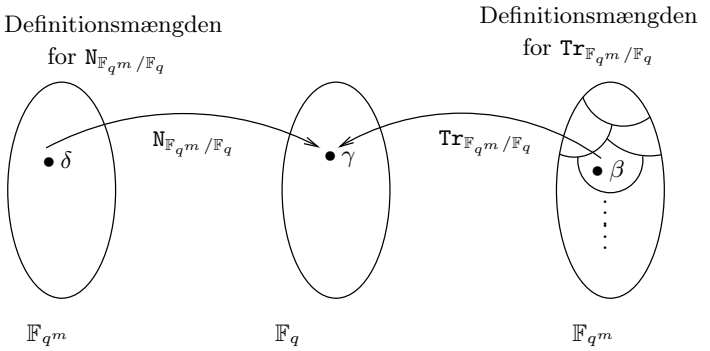
(*ii*) *hvis* δ *er et primitivt element i* $\mathbb{F}_{q^m}$, $(\delta^{i+j(q-1)}, \beta_{i,k})$, *hvor* $i = 0, \ldots, q-2$, $j = 0, \ldots, \frac{q^m-1}{q-1} - 1$, $k = 0, \ldots, q^{m-1} - 1$, *og* $\beta_{i,k}^{q^{m-1}} + \cdots + \beta_{i,k}^q + \beta_{i,k} = \delta^{i\frac{q^m-1}{q-1}}$.

Punkterne beskrevet i (*i*) *udgør* q^{m-1} *punkter, mens punkterne beskrevet i* (*ii*) *udgør de resterende* $q^{2m-1} - q^{m-1}$ *punkter.*

Sætning 49 og beviset herfor er en generalisering af [5, Lemma 14.1.1].

Bevis: Først bestemmes det samlede antal punkter $(\delta, \beta) \in \mathbb{F}_{q^m}^2$, som opfylder, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \gamma = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$.

For ethvert $\delta \in \mathbb{F}_{q^m}$ eksisterer der et $\gamma \in \mathbb{F}_q$, sådan at $\gamma = \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta)$.
Fra kommentaren til Sætning 47 ved vi, at da trace afbildningen er en surjektiv vektorrumshomomorfi, så er antallet af elementer i hver ækvivalensklasse tilhørende $\mathbb{F}_{q^m}$ lig $\frac{q^m}{q}$.
Det vil sige, at for ethvert $\gamma \in \mathbb{F}_q$ eksisterer der q^{m-1} β'er i $\mathbb{F}_{q^m}$, således at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = \gamma$.
Ovenstående er illustreret i Figur 5.1, hvor $\mathbb{F}_{q^m}$ er vist to gange for overblikkets skyld.



Figur 5.1: *Illustration af norm- og trace afbildningerne. Definitionsmængden for* $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *er inddelt i* q *ækvivalensklasser hver indeholdende* q^{m-1} *elementer.*

Antallet af kombinationer af δ og β, hvor $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$ er dermed lig $q^m \cdot q^{m-1} = q^{2m-1}$, hvilket netop er antallet af punkter i $\mathbf{V}(I)$.

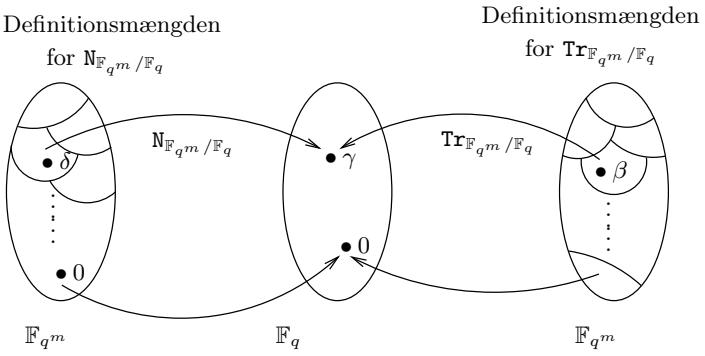
Dernæst betragtes udseendet af punkterne. Det skal stadig gælde, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$.
Punkterne bliver opdelt i de, hvor $\delta = 0$ og de, hvor $\delta \neq 0$.
Lad først δ være lig nul. Hermed er $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(0) = 0$. Altså søges de $\beta \in \mathbb{F}_{q^m}$, som opfylder, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = 0$, det vil sige, hvor

$$\beta^{q^{m-1}} + \cdots + \beta^q + \beta = 0.$$

Det vil sige, vi får punkterne $(0, \beta)$, hvor $\beta^{q^{m-1}} + \cdots + \beta^q + \beta = 0$ er opfyldt, og antallet af disse udgør q^{m-1} af de ialt q^{2m-1} punkter, se Figur 5.2.

Lad nu δ være et primitivt element i $\mathbb{F}_{q^m}$.
Idet $\mathbb{F}_{q^m}^*$ og $\mathbb{F}_q^*$ er multiplikative grupper, er $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ en surjektiv gruppe ho-

momorfi ifølge Sætning 48. Hvormed $\mathbb{F}_{q^m}^*$ ifølge Sætning 93 er inddelt i $q-1$ ækvivalensklasser med $\frac{q^m-1}{q-1}$ elementer i hver, se Figur 5.2.



Figur 5.2: *Illustration af norm- og trace afbildningerne. Definitionsmængderne for* $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *og* $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ *er inddelt i henholdsvis* $q-1$ *ækvivalensklasser med* $\frac{q^m-1}{q-1}$ *elementer i hver, og i* q *ækvivalensklasser med* q^{m-1} *elementer i hver.*

Udseendet af δ vælges til $\delta^{i+j(q-1)}$, hvor $i = 0, \ldots, q-2$, og $j = 0, \ldots, \frac{q^m-1}{q-1} - 1$. Derved gennemløber i de $q-1$ forskellige ækvivalensklasser, mens j gennemløber de $\frac{q^m-1}{q-1}$ forskellige elementer i hver ækvivalensklasse, fordi δ er et primitivt element i $\mathbb{F}_{q^m}$.
Med dette udseende af δ bliver

$$\begin{aligned}\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta^{i+j(q-1)}) &= \delta^{i+j(q-1)} \cdot \delta^{(i+j(q-1))q} \cdots \delta^{(i+j(q-1))q^{m-1}} \\ &= \delta^{i\frac{q^m-1}{q-1}} \cdot \delta^{j(q^m-1)} \\ &= \delta^{i\frac{q^m-1}{q-1}} = \gamma_i \in \mathbb{F}_q^*.\end{aligned}$$

Der søges herefter de elementer $\beta \in \mathbb{F}_{q^m}$, som opfylder, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = \gamma_i = \delta^{i\frac{q^m-1}{q-1}}$, $i = 0, \ldots, q-2$. Disse γ_i'er vil ved trace afbildningen hver blive ramt af q^{m-1} elementer i $\mathbb{F}_{q^m}$. Dermed vælges udseendet af β til $\beta_{i,k}$, hvor $k = 0, \ldots, q^{m-1}-1$ gennemløber de forskellige elementer i den i'te ækvivalensklasse. Det vil sige, at vi får punkterne på formen $(\delta^{i+j(q-1)}, \beta_{i,k})$, hvor det skal være opfyldt, at

$$\delta^{i\frac{q^m-1}{q-1}} = \beta_{i,k}^{q^{m-1}} + \cdots + \beta_{i,k} + \beta_{i,k}.$$

og antallet af disse punkter bliver hermed

$$\#j \cdot \#i \cdot \#k = \frac{q^m - 1}{q - 1} \cdot (q - 1) \cdot (q^{m-1}) = q^{2m-1} - q^{m-1}.$$

□

Hermed har vi fået fastsat punkternes udseende og antal, og vi vil i næste afsnit beskæftige os med konstruktion af koderne.

5.2 Definition af NTP-koder

I dette afsnit vil vi ved at betragte idealet $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y \rangle \in \mathbb{F}_{q^m}[x, y]$ finde frem til en metode til at udvælge polynomierne, som skal benyttes til definitionen af NTP-koderne. Hertil kræves først følgende.

5.2.1 Fodaftryk af et ideal

Dette underafsnit bygger primært på [2, Afsnit 5.3].

Når der er valgt en monomiel ordning af polynomierne tilhørende $\mathbf{K}[x_1, \ldots, x_n]$, som defineret i Definition 31, er det muligt at bestemme $\mathtt{LT}(f)$, og dermed også det ledende term ideal, $\langle \mathtt{LT}(I) \rangle$, som benyttes til bestemmelse af fodaftrykket af et ideal, som er defineret således:

Definition 50 (Fodaftryk af et ideal) *Fastsæt en monomiel ordning, $\prec$. Lad I være et ideal i $\mathbf{K}[x_1, \ldots, x_n]$. Da er fodaftrykket af I givet ved*

$$\Delta_\prec(I) = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : x_1^{\alpha_1} \cdots x_n^{\alpha_n} \notin \langle \mathtt{LT}(I) \rangle\}.$$

Det vil sige, at der til bestemmelse af et fodaftryk kræves kendskab til et $\langle \mathtt{LT}(I) \rangle$. Dette kan findes ved at bestemme en Gröbner basis for idealet I, for da er $\langle \mathtt{LT}(I) \rangle$ netop idealet frembragt af de ledende termer i Gröbner basen.

Antallet af monomier i fodaftrykket er uafhængig af valg af monomiel ordning. For at vise dette benyttes Proposition 51.

Proposition 51 *Fastsæt en monomiel ordning på* $\mathbf{K}[x_1, \ldots, x_n]$*, og lad* $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$ *være et ideal. Da gælder følgende:*

(*i*) *Ethvert* $f \in \mathbf{K}[x_1, \ldots, x_n]$ *er kongruent modulo* I *til et entydigt bestemt polynomium* r*, som er en linearkombination af monomierne tilhørende fodaftrykket af* I*, med koefficienter i* $\mathbf{K}$*.*

(*ii*) *Elementerne i* $\{x^\alpha : x^\alpha \notin \langle \mathtt{LT}(I)\rangle\}$*, hvor* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}, 0 \leq \alpha_i$*, er lineært uafhængige modulo* I*. Det vil sige, hvis*

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

hvor x^α *tilhører fodaftrykket af* I*, så er* $c_\alpha = 0$ *for alle* α*.*

Bevis: (*i*) : Lad $G = \{g_1, \ldots, g_t\}$ være en Gröbner basis for I, og lad $f \in \mathbf{K}[x_1, \ldots, x_n]$. Ifølge divisionsalgoritmen for polynomier i flere variable opfylder restleddet $r = \overline{f}^G$, hvor $\overline{f}^G$ er resten af f ved division med G, at $f = q + r$, hvor $q \in I$.
Dermed vil $f - r = q \in I$, hvilket netop er definitionen på, at f og r er kongruente modulo I.
Divisionsalgoritmen for polynomier i flere variable giver desuden, at r er en linearkombination af monomierne $x^\alpha \notin \langle \mathtt{LT}(I)\rangle$, med koefficienter i k. Entydigheden af r følger af Sætning 39.

(*ii*) : Antag, at elementerne i $\{x^\alpha : x^\alpha \notin \langle \mathtt{LT}(I)\rangle\}$ ikke er lineært uafhængige. Det vil sige, at der eksisterer mindst et $c_{\alpha(i)} \neq 0$.
Da $\sum_\alpha c_\alpha x^\alpha \equiv 0 \mod I$, så vil $\sum_\alpha c_\alpha x^\alpha$ tilhøre I, og dermed vil den ledende term af dette polynomium tilhøre $\langle \mathtt{LT}(I)\rangle$.
Idet dette er i modstrid med antagelsen, er elementerne i $\{x^\alpha : x^\alpha \notin \langle \mathtt{LT}(I)\rangle\}$ lineært uafhængige. □

Man kan betragte $\mathbf{K}[x_1, \ldots, x_n]$ som et uendeligt dimensionalt vektorrum, hvor basisvektorerne er alle monomier i $x_1, \ldots, x_n$.

Ved at udtage et antal monomier som basisvektorer, fås et underrum af vektorrummet $\mathbf{K}[x_1, \ldots, x_n]$.
Af Proposition 51 ses det, at monomierne i fodaftrykket udspænder et sådant underrum af $\mathbf{K}[x_1, \ldots, x_n]$. Det vil sige at alle restled $r = \overline{f}^G$, hvor G er en Gröbner basis for idealet I, ligger i det pågældende underrum.

Ifølge næste sætning, vil fodaftrykket af et ideal I, uanset monomiel ordning, udgøre en basis for kvotientringen $\mathbf{K}[x_1, \ldots, x_n]/I$. Det vil sige, at størrelsen af fodaftrykket for I altid er den samme uafhængig af monomiel ordning.

Sætning 52 *Lad $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$ være et ideal. Så er $\mathbf{K}[x_1, \ldots, x_n]/I$, set som et vektorrum over $\mathbf{K}$, isomorf med $S = \mathrm{Span}(x^\alpha : x^\alpha \notin \langle \mathtt{LT}(I) \rangle)$.*

Bevis: Udfra Proposition 51 definerer afbildningen ϕ: $\mathbf{K}[x_1, \ldots, x_n]/I \to S$, givet ved $\phi([f]) = \overline{f}^G$, en bijektiv afbildning mellem ækvivalensklasserne i $\mathbf{K}[x_1, \ldots, x_n]/I$ og elementerne i S.
Det skal nu vises, at denne afbildning er lukket under addition og multiplikation med skalar, idet ϕ da vil opfylde betingelserne for at være en vektorrumsisomorfi.

Hvis $[f]$ og $[g]$ er elementer i $\mathbf{K}[x_1, \ldots, x_n]/I$, så skal det vises, at $\phi([f] + [g]) = \phi([f]) + \phi([g])$.
Idet man lægger ækvivalensklasser sammen ved at addere deres repræsentanter, gælder det, at $\phi([f] + [g]) = \phi([f + g])$, og dermed er $\phi([f] + [g]) = \overline{f + g}^G$, og det skal derfor vises, at

$$\overline{f + g}^G = \overline{f}^G + \overline{g}^G. \tag{5.3}$$

For at vise dette skal det først vises, at

$$\overline{f}^G = \overline{g}^G \Leftrightarrow f - g \in I. \tag{5.4}$$

$\Rightarrow$: Lad $f = q_1 + \overline{f}^G$ og $g = q_2 + \overline{g}^G$, hvor $q_1, q_2 \in I$. Så vil $f - g = q_1 - q_2 \in I$.

$\Leftarrow$: Lad f og g være givet som ovenfor. Så er $f - g = q_1 + \overline{f}^G - q_2 - \overline{g}^G$. Dermed vil $\overline{f}^G - \overline{g}^G = f - g - q_1 + q_2$ tilhøre I. Men da ingen af leddene i $\overline{f}^G$ og $\overline{g}^G$ er divisible med elementerne i G, så er $\overline{f}^G - \overline{g}^G = 0$. Altså er $\overline{f}^G = \overline{g}^G$, hvormed (5.4) er vist.

Betragt $\overline{f+g}^G = f+g-q$, hvor $q \in I$. Hvis det antages, at f og g er givet som tidligere, så vil $\overline{f+g}^G - (\overline{f}^G + \overline{g}^G) = (q_1+q_2)-q \in I$. Så (5.4) giver, at $\overline{\overline{f+g}^G} = \overline{\overline{f}^G + \overline{g}^G}^G$, og da ingen af monomierne i $\overline{f+g}^G$, $\overline{f}^G$ eller $\overline{g}^G$ er divisible med polynomierne i G får vi, at $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$. Altså er ϕ lukket under addition.

Det skal ligeledes vises, at ϕ er lukket under multiplikation med skalar. Det vil sige, at $\phi(c[f]) = c \cdot \phi([f])$, hvor $c \in \mathbf{K}$. Da $\phi(c[f]) = \phi([cf])$, så gælder det pr. definition af ϕ, at $\phi(c[f]) = \overline{cf}^G$. Det skal dermed vises, at

$$\overline{cf}^G = c\overline{f}^G. \tag{5.5}$$

Lad følgende ligheder være opfyldt

$$\begin{aligned} f &= q_1 + \overline{f}^G, \\ cf &= q_2 + \overline{cf}^G. \end{aligned}$$

Heraf følger det, da $q_1, q_2 \in I$, at

$$\overline{cf}^G - c\overline{f}^G = cq_1 - q_2 \in I.$$

Dette medfører ifølge (5.4), at $\overline{\overline{cf}^G}^G = \overline{c\overline{f}^G}^G$. Idet der ikke findes monomier i hverken $\overline{cf}^G$ eller $c\overline{f}^G$, som er divisible med polynomierne i G, så er $\overline{cf}^G = c\overline{f}^G$.

Vi konkluderer hermed, at ved at benytte repræsentanter for ækvivalensklasserne, så svarer operationerne i $\mathbf{K}[x_1, \ldots, x_n]/I$ til operationerne i vektorrummet S over $\mathbf{K}$.
Altså er ϕ en vektorrumsisomorfi. □

Idet kvotientringen $\mathbf{K}[x_1, \ldots, x_n]/I$ og vektorrummet udspændt af fodaftrykket af I er isomorfe, så giver efterfølgende sætning, at størrelsen af fodaftrykket er en øvre grænse for antallet af punkter i varieteten $\mathbf{V}(I)$.

Sætning 53 *Lad $I \subseteq \mathbf{K}[x_1, \ldots, x_n]$, være et ideal, sådan at $V = \mathbf{V}(I)$ er en endelig mængde, så gælder det, at antallet af punkter i V er højst* $\dim(\mathbf{K}[x_1, \ldots, x_n]/I)$.

Bevis: For at vise sætningen, skal det først vises at, hvis vi har givet forskellige punkter $p_1, \ldots, p_m \in \mathbf{K}^n$, så findes der et polynomium $f_1 \in \mathbf{K}[x_1, \ldots, x_n]$, så $f_1(p_1) = 1$ og $f_1(p_2) = \cdots = f_1(p_m) = 0$.
For hvert par af punkter p_1 og p_i, $i \geq 2$, gælder det, at $p_1 \neq p_i$. Antag, at p_1 og p_i er forskellige på den j'te position. Der kan nu dannes polynomier $g_i = (x_j - p_{i_j})/(p_{1_j} - p_{i_j})$. Disse opfylder, at $g_i(p_1) = 1$ og $g_i(p_i) = 0$. Dermed opfylder $f_1 = g_2 g_3 \cdots g_m$ de ønskede betingelser.
Hvis vi erstatter p_1 med hver af $p_2, \ldots, p_m$, fås, udover f_1, polynomierne $f_2, \ldots f_m$ sådan, at $f_i(p_i) = 1$ og $f_i(p_j) = 0$, for $i \neq j$.

Antag, at $V = \{p_1, \ldots, p_m\}$, så har vi $f_1, \ldots, f_m$ som givet ovenfor. Kan det vises, at $[f_1], \ldots, [f_m] \in \mathbf{K}[x_1, \ldots, x_n]/I$ er lineært uafhængige, så er

$$m \leq \dim(\mathbf{K}[x_1, \ldots, x_n]/I), \tag{5.6}$$

hvilket netop er, hvad der ønskes vist.
For at vise, at $[f_1], \ldots, [f_m]$ er lineært uafhængige, antages det, at $\sum_{i=1}^m a_i[f_i] = [0]$ i $\mathbf{K}[x_1, \ldots, x_n]/I$, hvor $a_i \in \mathbf{K}$.
I $\mathbf{K}[x_1, \ldots, x_n]$ svarer dette til, at $h = \sum_{i=1}^m a_i f_i \in I$. Det vil sige, at h giver nul for alle punkter i $V = \{p_1, \ldots, p_m\}$, så for et vilkårligt j, $1 \leq j \leq m$, er

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

Da dette gælder for alle a_j'erne, så er $[f_1], \ldots, [f_m]$ lineært uafhængige.

□

Denne sætning kan desuden betragtes udfra det synspunkt, at afbildningen

$$\begin{array}{ccc} \varphi\colon \mathbf{K}[x_1, \ldots, x_n]/I & \longrightarrow & \mathbf{K}^m \\ \varphi(f + I) & \longmapsto & (f(p_1), \ldots, f(p_m)), \end{array} \tag{5.7}$$

hvor m er antallet af punkter i varieteten $V = \{p_1, \ldots p_m\}$, er en surjektiv vektorrumshomomorfi.

Hvis φ er en surjektiv afbildning, så er billedrummet af $\mathbf{K}[x_1, \ldots, x_n]/I$ præcis $\mathbf{K}^m$. Det vil sige, at $\dim(\varphi(\mathbf{K}[x_1, \ldots, x_n]/I)) = \dim(\mathbf{K}^m) = m$. Hvis det desuden gælder, at φ er en vektorumshomomorfi, så stammer en basis for $\mathbf{K}^m$ fra m

lineært uafhængige elementer i $\mathbf{K}[x_1, \ldots, x_n]/I$.
Så alt i alt gælder det, at

$$\text{antal punkter i } V = m = \dim(\mathbf{K}^m) \leq \dim(\mathbf{K}[x_1, \ldots, x_n]/I),$$

hvilket netop er resultatet i Sætning 53.

Det skal derfor vises, at φ er en surjektiv vektorrumshomomorfi.
Hvis φ er en vektorrumshomomorfi, skal den være lukket under addition og multiplikation med skalar.
Lad derfor $[f], [g] \in \mathbf{K}[x_1, \ldots, x_n]/I$ være ækvivalensklasserne repræsenteret ved f og g. Så gælder det, at

$$\varphi([f] + [g]) = \varphi([f + g]).$$

Herudfra fås:

$$\begin{aligned} \varphi([f] + [g]) &= ((f+g)(p_1), \ldots, (f+g)(p_m)) \\ &= (f(p_1), \ldots, f(p_m)) + (g(p_1), \ldots, g(p_m)) \\ &= \varphi([f]) + \varphi([g]). \end{aligned}$$

Altså er φ lukket under addition.
Ligeledes ses det, at φ er lukket under multiplikation med skalar, idet

$$\begin{aligned} \varphi(c[f]) &= \varphi([cf]) = (cf(p_1), \ldots, cf(p_m)) \\ &= c(f(p_1), \ldots, f(p_m)) \\ &= c\varphi([f]), \end{aligned}$$

hvor $c \in \mathbf{K}$. Dermed er φ en vektorrumshomomorfi.

I første del af beviset for Sætning 53 defineres polynomierne $f_1, \ldots, f_m$ sådan, at $f_i(p_i) = 1$ og $f_i(p_j) = 0$ for $i \neq j$. Ved dermed at benytte φ på ækvivalensklasserne repræsenteret ved f_i, for $i = 1, \ldots, m$, vil disse blive afbildet over i den ortonormale basis for $\mathbf{K}^m$. Da φ er en vektorrumshomomorfi, vil alt i $\mathbf{K}^m$ derfor blive ramt, og alt i alt er φ en surjektiv vektorrumshomomorfi.

5.2.2 Udvælgelse af polynomier

Foregående afsnits teori anvendes i dette afsnit på monomier i to variable.
Før kode-polynomierne udvælges skal der fastsættes en monomiel ordning, og til dette formål defineres først (u, v)-vægten af et monomium i $\mathbb{F}_{q^m}[x, y]$.

Definition 54 (Vægt af et monomium) *Lad $x^i y^j \in \mathbb{F}_{q^m}[x,y]$. Da er (u,v)-vægten af dette monomium givet ved:*

$$W(x^i y^j) = iu + jv.$$

Ligeledes kan vægten af et polynomium, $W(f)$, $f \in \mathbb{F}_{q^m}[x,y]$, bestemmes. Dette er defineret som $W(f) = \max\{W(x^i y^j) : x^i y^j \in f\}$.
Der vil gennem rapporten desuden blive refereret til vægten af et monomium som den vægtede grad af det pågældende monomium.
Vægten af et monomium kan herefter benyttes i definitionen på vægtet lex-orden.
Definitionen stammer fra [4, Definition 1, side 353].

Definition 55 (Vægtet lex-orden, $\prec_W$) *Lad $x^{i_1} y^{j_1}$, $x^{i_2} y^{j_2} \in \mathbb{F}_{q^m}[x,y]$, og lad $\prec_{lex}$ være lex-ordningen, hvor $x \prec_{lex} y$.*

Så er

$$x^{i_1} y^{j_1} \prec_W x^{i_2} y^{j_2}$$

hvis enten

a) $W(x^{i_1} y^{j_1}) < W(x^{i_2} y^{j_2})$

eller

b) $W(x^{i_1} y^{j_1}) = W(x^{i_2} y^{j_2})$ *og*
$x^{i_1} y^{j_1} \prec_{lex} x^{i_2} y^{j_2}$, *hvilket her vil sige, at* $j_1 < j_2$.

Det kan vises, at den vægtede lex-orden, $\prec_W$, opfylder betingelserne i Definition 31 for at være en monomiel ordning.

Vi vil gennem rapporten benytte $\prec_w$ om den vægtede lex-orden, hvor $x \prec_{lex} y$, og hvor $u = q^{m-1}$ og $v = \frac{q^m-1}{q-1}$. Det vil sige $w(x^i y^j) = i(q^{m-1}) + j(\frac{q^m-1}{q-1})$.

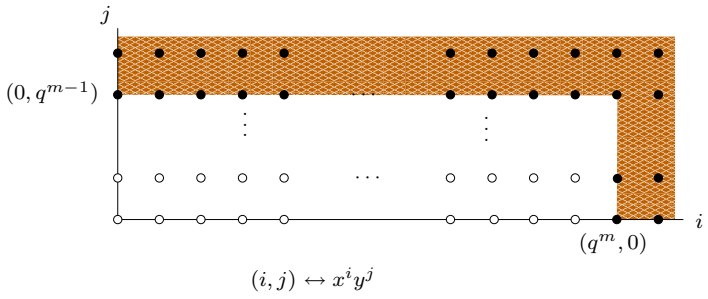
Det kan nu vises, at $\{x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\}$ er en Gröbner basis for idealet $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$.

Proposition 56 *Mængden* $G = \{x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\}$ *er en Gröbner basis med hensyn til* $\prec_w$ *for idealet* $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$.

Bevis: Betragt mængden af de monomier tilhørende $\mathbb{F}_{q^m}[x, y]$, som ligger i komplementet til $\langle y^{q^{m-1}}, x^{q^m}, y^{q^m}\rangle$,

$$D = \{x^i y^j : 0 \leq i < q^m, 0 \leq j < q^{m-1}\},$$

se Figur 5.3.
Antallet af monomier i D er dermed $q^{m-1} \cdot q^m = q^{2m-1}$.



Figur 5.3: *Mængden D.*

Antag nu, at G ikke er en Gröbner basis for I. Det vil sige, at

$$\langle y^{q^{m-1}}, x^{q^m}, y^{q^m}\rangle \subset \langle \mathtt{LT}(I)\rangle.$$

Så hvis vi ønsker en Gröbner basis for I, skal der tilføjes polynomier g til G således, at $\mathtt{LT}(g) = x^l y^k$, hvor $l < q^m$ eller $k < q^{m-1}$.

Antag, at der er blevet tilføjet tilstrækkeligt med polynomier til G, så vi nu har en Gröbner basis for I. Det er herudfra muligt, at bestemme fodaftrykket af I, og det ses, at størrelsen af dette fodaftryk er mindre end størrelsen af D, hvilken er lig q^{2m-1}.

Fra Sætning 49 har vi, at antallet af punkter i varieteten $\mathbf{V}(I)$ er q^{2m-1}, og ifølge Sætning 53 er antallet af monomier i fodaftrykket af I en øvre grænse for

antallet af punkter i varieteten $\mathbf{V}(I)$. Dermed har vi alt i alt, at

$$q^{2m-1} = \#\mathbf{V}(I) \leq \#\Delta_{\prec_w}(I) < q^{2m-1}.$$

Da dette er en modstrid, er $G = \{x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\}$ en Gröbner basis for I. □

Udfra denne proposition ses det, at fodaftrykket af idealet I med hensyn til $\prec_w$ kan skrives som følgende mængde:

$$\Delta_{\prec_w}(I) = \{x^i y^j : 0 \leq i < q^m, 0 \leq j < q^{m-1}\}.$$

Det er linearkombinationer af monomier fra en delmængde af $\Delta_{\prec_w}(I)$, der udgør de polynomier, som benyttes i definitionen af NTP-koderne. Før koden defineres betragtes nogle egenskaber ved fodaftrykket af I, samt konsekvenser af disse. Antallet af punkter i fodaftrykket af I er, som en konsekvens af ovenstående proposition, lig q^{2m-1}, hvilket også er antallet af punkter, n, i $\mathbf{V}(I)$, se Sætning 49.

Lad nu I være givet som i Proposition 56, så giver kommentaren efter Sætning 53, at følgende afbildning, ψ, er en surjektiv vektorrumshomomorfi,

$$\begin{array}{rccc} \psi\colon & \mathbb{F}_{q^m}[x,y]/I & \longrightarrow & \mathbb{F}_{q^m}^n \\ & \psi(f+I) & \longmapsto & (f(p_1), \ldots, f(p_n)), \end{array} \tag{5.8}$$

hvor $\{p_1, \ldots, p_n\} = \mathbf{V}(I)$.
Da Sætning 52 giver, at $\mathbb{F}_{q^m}[x,y]/I$ er isomorf med vektorrummmet udspændt af monomierne i $\Delta_{\prec_w}(I)$, er

$$\dim\left(\mathbb{F}_{q^m}[x,y]/I\right) = \dim\left(\operatorname{Span}\Delta_{\prec_w}(I)\right) = q^{2m-1} = n.$$

Da dimensionen af $\mathbb{F}_{q^m}^n$ også er n, er ψ en surjektiv vektorrumshomomorfi, som er defineret mellem to lige store mængder, hvorved ψ også er en injektiv vektorrumshomomorfi. Dette giver tilsammen, at ψ er en vektorrumsisomorfi. Udfra denne afbildning, kan vi nu definere NTP-koderne.

Definition 57 (NTP-kode) *Vælg et $s \geq 0$ og lad $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle \subseteq \mathbb{F}_{q^m}[x,y]$. Da er koden $NTP(s)$ over $\mathbb{F}_{q^m}$ defineret til at være*

$$NTP(s) = \operatorname{Span}_{\mathbb{F}_{q^m}}\{\psi(M+I) : M \in \Delta_{\prec_w}(I), w(M) \leq s\}.$$

For at dette er veldefineret ønsker vi, at der til ethvert kodeord i $NTP(s)$ svarer netop ét polynomium, som er en linearkombination af monomierne i fodaftrykket af idealet I med vægtet grad mindre end eller lig s, og omvendt, at der til ethvert polynomium på denne form, svarer præcis ét kodeord i $NTP(s)$.

Idet $\mathbb{F}_{q^m}[x,y]/I$ er isomorf med vektorrummet udspændt af monomierne i $\Delta_{\prec_w}(I)$, og da ψ er en isomorf afbildning mellem $\mathbb{F}_{q^m}[x,y]/I$ og $\mathbb{F}_{q^m}^n$, så afbilder en basis for ethvert underrum af Span$\Delta_{\prec_w}(I)$ over i en basis for et underrum i $\mathbb{F}_{q^m}^n$.
Det vil sige, at enhver linearkombination af monomier i $\Delta_{\prec_w}(I)$ med vægtet grad mindre end eller lig s giver et entydigt bestemt kodeord i $NTP(s)$, og ligeledes svarer der til ethvert kodeord i $NTP(s)$ præcis et polynomium, som er en linearkombination af monomier i $\Delta_{\prec_w}(I)$ med vægtet grad mindre end eller lig s. Hermed er NTP-koder veldefinerede.

Lad $f, g \in \text{Span}\,(\Delta_{\prec_w}(I))$, hvor alle monomier, som indgår i f og g, har vægt mindre end eller lig s. Dermed er $\psi(f+I)$ og $\psi(g+I)$ kodeord i $NTP(s)$-koden. Hvis $c, d \in \mathbb{F}_{q^m}$, så vil $cf + dg$ også opfylde, at det er en linearkombination af monomier fra $\text{Span}\,(\Delta_{\prec_w}(I))$, som har vægt mindre end eller lig s. Dermed er $c \cdot \psi(f+I) + d \cdot \psi(g+I) = \psi((cf+dg)+I)$ også et kodeord i $NTP(s)$, hvormed det kan konkluderes, at NTP-koden er en lineær kode.

Kapitel 6

Egenskaber ved NTP- koden

Dette kapitel behandler forskellige egenskaber for NTP-koden. Først bestemmes minimumsafstanden, og dernæst en formel for kodens dimension, hvilket til slut benyttes til at bestemme dualkoden til NTP-koden.

6.1 Minimumsafstand af NTP-koden

For at bestemme en nedre grænse for minimumsafstanden for en NTP-kode kan det benyttes, at en sådan kode er lineær, hvormed man i stedet kan bestemme en nedre grænse for minimumsvægten.

Lad $n = q^{2m-1}$. Hvis $\overline{c}$ er et kodeord i en NTP-kode, så er $\overline{c}$ på formen $\overline{c} = (f(p_1), \ldots, f(p_n))$, hvor $f \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{M \in \Delta_{\prec_w}(I) : w(M) \leq s\}$.
Hamming vægten, ω_H, af kodeordet $\overline{c}$ afhænger af antallet af fælles nulpunkter, tilhørende $\mathbb{F}_{q^m}^2$, mellem f og norm- trace polynomiet. Dette antal fås udfra følgende proposition.

Proposition 58 *Lad* $\mathbf{K}$ *være et vilkårligt legeme, og lad der være givet en vægtet lexikografisk ordning* $\prec_W$*, hvor* $x \prec_{lex} y$*,* $W(x^i) = bi$ *og* $W(y^j) = aj$*.*

Betragt

$$\begin{aligned} F(x,y) &= x^a + \alpha y^b + F'(x,y) \in \mathbf{K}[x,y] \\ G(x,y) &= x^i y^j + G'(x,y) \in \mathbf{K}[x,y], \end{aligned}$$

hvor $\alpha \neq 0$, $a, b > 0$, $W(F') < ab$ *og* $W(G') < bi + aj$.
Så har $F(x,y) = G(x,y) = 0$ *højst* $bi + aj$ *løsninger i* $\mathbf{K}^2$.

Denne proposition samt bevis stammer fra [8, Proposition 4, side 637].

Bevis: Pr. definition af den vægtede lexikografiske ordning er $\mathtt{LM}(F) = y^b$ og $\mathtt{LM}(G) = x^i y^j$.
Hvis $j \geq b$ dannes polynomiet,

$$\begin{aligned} \tilde{G}_1(x,y) &= G(x,y) + (-1)^1 \alpha^{-1} x^i y^{j-b} F(x,y) \\ &= G'(x,y) + (-1)^1 \alpha^{-1} x^i y^{j-b}(x^a + F'(x,y)). \end{aligned}$$

Heraf ses, at det ledende monomium er $x^{i+a}y^{j-b}$.
Hvis $j - b \geq b$, så fortsættes processen indtil vi får:

$$\tilde{G}_t(x,y) = \tilde{G}_{t-1}(x,y) + (-1)^t \alpha^{-t} x^{i+(t-1)a} y^{j-tb} F(x,y),$$

med $\mathtt{LM}(\tilde{G}_t) = x^{i+ta}y^{j-tb} = x^{\tilde{i}}y^{\tilde{j}}$, hvor $\tilde{j} < b$.
Det ses udfra konstruktionen af $\tilde{G}_t$, at denne tilhører idealet $\tilde{I} = \langle F(x,y), G(x,y) \rangle$.
Endvidere ses det, at:

$$W(x^{\tilde{i}}y^{\tilde{j}}) = W(x^{i+ta}y^{j-tb}) = b(i+ta) + a(j-tb) = bi + aj = W(x^i y^j).$$

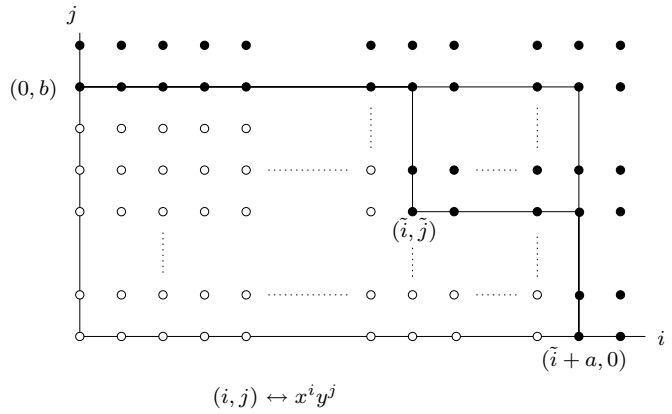
For at begrænse fodaftrykket af $\tilde{I}$ betragtes desuden S-polynomiet, $S(F, \tilde{G}_t)$, som er endnu et polynomium i idealet $\tilde{I}$.

$$\begin{aligned} S(F,\tilde{G}_t) &= \frac{x^{\tilde{i}}y^b}{\alpha y^b} F(x,y) - \frac{x^{\tilde{i}}y^b}{(-1)^t \alpha^{-t} x^{\tilde{i}} y^{\tilde{j}}} \tilde{G}_t(x,y) \\ &= \alpha^{-1} x^{\tilde{i}} F(x,y) - (-1)^{-t} \alpha^t y^{b-\tilde{j}} \tilde{G}_t(x,y). \end{aligned}$$

Det ses, at S-polynomiet eliminerer monomiet $x^{\tilde{i}}y^b$, og det ledende monomium i $S(F, \tilde{G}_t)$ er dermed $x^{\tilde{i}+a}$, idet de øvrige led har vægtet grad højst $ab + \tilde{i}b - 1$.

Vi har nu følgende begrænsning for fodaftrykket af $\tilde{I}$:

$$\Delta_{\prec_W}(\tilde{I}) \subseteq \{x^\alpha y^\beta : \alpha < a + \tilde{i}, \beta < b, \text{ hvor ikke både } \alpha \geq \tilde{i} \text{ og } \beta \geq \tilde{j}\}.$$



Figur 6.1: *Mængden, som $\tilde{I}$'s fodaftryk vil ligge i.*

Denne begrænsning er illustreret på Figur 6.1.
Størrelsen af denne mængde er:

$$(a+\tilde{i})b-(a+\tilde{i}-\tilde{i})(b-\tilde{j})=W(x^{\tilde{i}}y^{\tilde{j}})=W(x^iy^j)=bi+aj.$$

Det vil sige, idet fodaftrykket er en øvre grænse for antallet af nulpunkter i $\mathbf{V}(\tilde{I})$, så har $F(x,y)$ og $G(x,y)$ højst $bi+aj$ fælles nulpunkter. □

Korollar 59 *Lad $J=\langle x^{\frac{q^m-1}{q-1}}-y^{q^{m-1}}-\cdots-y^q-y\rangle\in\mathbb{F}_{q^m}[x,y]$. Da vil enhver mulig vægt være repræsenteret i fodaftrykket for J.*

Bevis: Udfra beviset for Proposition 58 ses det, at vægten for det ledende monomium i $G(x,y)$ vil optræde som vægt af et monomium $x^{\tilde{i}}y^{\tilde{j}}$, hvor $\tilde{j}<b$.
Det vil sige, at enhver vægt er repræsenteret ved et monomium tilhørende fodaftrykket af idealet givet ved $\langle F(x,y)\rangle$.
Dermed gælder det, i det tilfælde hvor $a=\frac{q^m-1}{q-1}$, $b=q^{m-1}$ og $\alpha=-1$, at enhver vægt er repræsenteret ved et monomium i fodaftrykket af idealet $J=\langle x^{\frac{q^m-1}{q-1}}-y^{q^{m-1}}-\cdots-y^q-y\rangle$, som netop var det søgte resultat. □

Følgende lemma giver desuden, at monomierne i fodaftrykket af J alle har forskellig vægt.

Lemma 60 *Lad* $J = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y \rangle \in \mathbb{F}_{q^m}[x,y]$. *Da vil fodaftrykket af* J, $\Delta_{\prec_w}(J)$, *ikke indeholde to monomier af samme vægtet grad.*

Bevis: Det skal først vises, at $\gcd(\frac{q^m-1}{q-1}, q^{m-1}) = 1$, når q er en primtalspotens, p^r, hvor $r \in \mathbb{N}$. Dermed er $q^{m-1} = p^{r(m-1)}$, og de mulige kandidater til $\gcd(\frac{q^m-1}{q-1}, q^{m-1})$ vil være mængden $\{1, p, p^2, \ldots, p^{r(m-1)}\}$.
Da $\frac{q^m-1}{q-1} = 1 + q + q^2 + \cdots + q^{m-1}$, ses det, at den eneste kandidat, som går op i alle disse led er tallet 1. Dermed er $\gcd(\frac{q^m-1}{q-1}, q^{m-1}) = 1$.

Det antages nu, at monomierne $x^i y^j, x^k y^l \in \Delta_{\prec_w}(J) = \{x^\alpha y^\beta : 0 \leq \beta < q^{m-1}, 0 \leq \alpha\}$ har samme vægtede grad. Hermed er

$$\begin{aligned} i(q^{m-1}) + j(\tfrac{q^m-1}{q-1}) &= k(q^{m-1}) + l(\tfrac{q^m-1}{q-1}) \\ \Updownarrow & \\ q^{m-1}(i-k) &= \tfrac{q^m-1}{q-1}(l-j). \end{aligned}$$

Altså må q^{m-1} gå op i $(l-j)$, da q^{m-1} og $\frac{q^m-1}{q-1}$ er indbyrdes primiske. Men da $(l-j)$ er nummerisk mindre end q^{m-1}, vil dette kun kunne lade sig gøre, hvis $(l-j)$ er lig nul. Dette betyder, at $l = j$ og dermed er $i = k$, hvorved to forskellige monomier i fodaftrykket $\Delta_{\prec_w}(J)$ ikke kan have samme vægtede grad.

□

Proposition 58 kan nu anvendes til at bestemme en nedre grænse for minimumsafstanden for NTP-koden.

Sætning 61 *Lad* $NTP(s)$ *være en* NTP*-kode. Da vil det gælde, at minimumsafstanden,* d, *for* $NTP(s)$ *er mindst* n - s.

Bevis: Som tidligere nævnt, kan det udnyttes, at $NTP(s)$ er en lineær kode, hvormed minimumsafstanden er lig minimumsvægten.

Vælger vi nu at betragte den vægtede lexikografiske ordning, $\prec_w$, hvor $w(x^i) = i(q^{m-1})$ og $w(y^j) = j(\frac{q^m-1}{q-1})$, så ser vi fra Proposition 58 at antallet af fælles nulpunkter i $\mathbb{F}_{q^m}^2$ mellem norm- trace polynomiet, repræsenteret ved $F(x,y)$, og et polynomium $f \in \mathrm{Span}_{\mathbb{F}_{q^m}}\{M \in \Delta_{\prec_w}(I) : w(M) \leq s\}$, repræsenteret ved $G(x,y)$, højst er lig:

$$(q^{m-1})i + (\frac{q^m-1}{q-1})j.$$

Det vil sige, at Hamming vægten, ω_H for et kodeord $\overline{c}$ tilhørende $NTP(s)$-koden mindst er $n - ((q^{m-1})i + (\frac{q^m-1}{q-1})j)$, og da dette gælder for alle $\overline{c} \neq 0$, så er minimumsvægten og dermed minimumsafstanden $d \geq n - s$, da s er den største vægtede grad af monomierne, som anvendes til konstruktion af $NTP(s)$-koden. □

For et begrænset interval af s er minimiumsafstanden for $NTP(s)$ præcis lig $n - s$.

Sætning 62 *Lad $NTP(s)$ være en NTP-kode, og lad $i(q^{m-1}) + j\left(\frac{q^m-1}{q-1}\right) = s$. Da er minimumsafstanden*

$$d = n - s,$$

hvis funktionen givet ved

$$B(i,j) = \begin{cases} \lceil \frac{j}{q^{m-1}} \rceil & \text{for} \quad i = 0 \\ 1 + \lceil \frac{i-1}{(q^m-1)/(q-1)} \rceil + \lceil \frac{j}{q^{m-1}} \rceil & \text{for} \quad i \geq 1 \end{cases}$$

er mindre end eller lig q.

Bevis: For at bestemme den eksakte minimiumsafstand skal der kunne findes et kodeord i $NTP(s)$, som netop har Hammingvægt $n - s$. Dette svarer til at finde et polynomium, som har præcis s nulpunkter til fælles med norm-trace polynomiet.

Definer mængderne

$$\begin{aligned} N_\gamma &= \{\alpha \in \mathbb{F}_{q^m} : \mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \gamma \in \mathbb{F}_q\}, \\ Tr_\gamma &= \{\alpha \in \mathbb{F}_{q^m} : \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \gamma \in \mathbb{F}_q\}. \end{aligned}$$

Opskriv desuden $\mathbb{F}_q$ og $\mathbb{F}_{q^m}$ på følgende måder:

$$\begin{aligned}
\mathbb{F}_q &= \{0, \gamma_1, \ldots, \gamma_{q-1}\}, \\
\mathbb{F}_{q^m{}_{(\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q})}} &= \{\underbrace{\delta_1(=0)}_{N_0}, \underbrace{\delta_2, \ldots,}_{N_{\gamma_1}} \ldots, \ldots, \underbrace{\delta_{q^m}}_{N_{\gamma_{q-1}}}\}, \\
\mathbb{F}_{q^m{}_{(\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})}} &= \{\underbrace{\beta_1, \ldots,}_{Tr_{\gamma_{q-1}}} \ldots, \ldots, \underbrace{\beta_{q^m}}_{Tr_0}\}.
\end{aligned}$$

Her er $\mathbb{F}_{q^m{}_{(\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q})}}$ inddelt i q delmængder ordnet således, at elementerne i første delmængde tilhører N_0, elementerne i anden delmængde tilhører N_{γ_1} og så videre.
Tilsvarende er $\mathbb{F}_{q^m{}_{(\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q})}}$ inddelt i q delmængder ordnet således, at elementerne i første delmængde tilhører $Tr_{\gamma_{q-1}}$, elementerne i anden delmængde tilhører $Tr_{\gamma_{q-2}}$ og så videre.
Vælg nu et polynomium

$$f(x,y) = \prod_{r=1}^{i}(x-\delta_r)\prod_{t=1}^{j}(y-\beta_t),$$

som er en linearkombination af monomierne i fodaftrykket af $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$, hvis vægtede grader er mindre end eller lig s, og hvor det ledende monomium x^iy^j har vægtet grad s.
Ifølge Lemma 60 har monomierne i fodaftrykket af I alle forskellige vægtede grader, hvormed x^iy^j er det eneste monomium med vægtet grad s. Dermed vides det fra Proposition 58, at antallet af fælles nulpunkter mellem $f(x,y)$ og norm-trace polynomiet er mindre end eller lig s.

Det ses, at nulpunkterne til $f(x,y)$ er de (x,y), hvor enten $x = \delta_r$ for $r = 1, \ldots, i$ eller $y = \beta_t$ for $t = 1, \ldots, j$. Nulpunkterne til norm-trace polynomiet er de (δ, β), hvorom det gælder, at $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$. Dermed er det muligt at bestemme de fælles nulpunkter mellem $f(x,y)$ og norm-trace polynomiet.

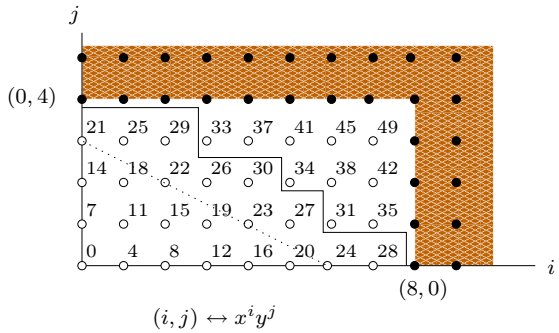
For hvert valgt δ_r, som er rod i $f(x,y)$, eksisterer der q^{m-1} β_t'er, så (δ_r, β_t) er rod i norm-trace polynomiet. Antallet af δ_r'er er i, så dette giver anledning til $i(q^{m-1})$ fælles nulpunkter.
Idet $j < q^{m-1}$, vælges der kun β_t'er fra $Tr_{\gamma_{q-1}}$.
For hvert valgt β_t vil der dermed være $\frac{q^m-1}{q-1}$ δ_r'er, så (δ_r, β_t) er rod i norm-trace

polynomiet. Antallet af β_t'er er j, så dette giver anledning til $j\left(\frac{q^m-1}{q-1}\right)$ fælles nulpunkter. Det vil sige, at der er $i(q^{m-1}) + j\left(\frac{q^m-1}{q-1}\right) = s$ fælles nulpunkter mellem $f(x,y)$ og norm-trace polynomiet med undtagelse af eventuelle overlap. Et overlap forekommer, når et valgt (δ_r, β_t) er sammenfaldende med et tidligere valgt (δ_r, β_t).
Da der højst vælges β_t'er indeholdt i $Tr_{\gamma_{q-1}}$, kan et overlap finde sted i de tilfælde, hvor i er så stor, at der skal vælges et δ_r fra $N_{\gamma_{q-1}}$, da denne skal kombineres med alle β_t tilhørende $Tr_{\gamma_{q-1}}$.
Altså forekommer der ingen overlap, hvis antallet af N_γ'er plus antallet af Tr_γ'er, hvorfra der vælges henholdsvis δ_r'er og β_t'er, er mindre end eller lig q.
Antallet af Tr_γ'er, hvorfra der vælges β_t'er, er $\lceil \frac{j}{q^{m-1}} \rceil$, og antallet af N_γ'er, hvorfra der vælges δ_r'er, er $1 + \lceil \frac{i-1}{(q^m-1)/(q-1)} \rceil$, for $i \geq 1$. Hvis enten i eller j er lig nul, er $f(x,y)$ kun et polynomium i én variabel, hvorved der kun skal vælges enten β_t'er eller δ_r'er for at få fastsat nulpunkterne for $f(x,y)$, så da vil enten antallet af N_γ'er eller antallet af Tr_γ'er være lig nul.

Dermed har $f(x,y)$ og norm-trace polynomiet præcis s fælles nulpunkter, hvis funktionen $B(i,j)$ er mindre end eller lig q. □

6.2 Dimension af NTP - koden

I dette afsnit vil vi afdække, hvorledes dimensionen, k, af en NTP-kode bestemmes. Dimensionen af en kode er antallet af elementer, som danner en basis for koden. Da monomierne i $\Delta_{\prec_w}(I)$ er lineært uafhængige ifølge Propsition 51, vil også en delmængde af dem være lineært uafhængige. Afbildes monomierne i denne delmængde med ψ givet som i ligning (5.8), vil dette danne en basis for en NTP-kode, da ψ er en vektorrumsisomorfi.
Ønskes dimensionen af $NTP(s)$-koden bestemt, svarer dette derfor til at bestemme antallet af monomier i $\Delta_{\prec_w}(I)$, som har vægt mindre end eller lig s. På Figur 6.2 er fodaftrykket af I illustreret, hvor m er valgt til 3 og q til 2. Tallene ved hvert punkt, som illustrerer et monomium, er vægten af det pågældende



Figur 6.2: *Fodaftryk af I, når $m = 3$ og $q = 2$.*

monomium.
Idet der altid er fastsat en vægt på x og y, og idet disses eksponenter vokser ud ad akserne, så vil de vægtede grader altid optræde i en ordnet rækkefølge. Dette er illustreret ved hjælp af den stiplede linie på Figur 6.2.
Da monomierne optræder i en ordnet rækkefølge er det muligt at afgrænse et område, hvori alle monomier har vægtet grad mindre end eller lig s.
Den fuldt optrukne streg, som går gennem figuren, viser hvilke monomier, der repræsenterer en basis for $NTP(30)$. Det ses, at $k(NTP(30)) = 22$.

Vi søger herefter at finde en formel til bestemmelse af dimensionen for en NTP-kode, og til dette formål introduceres følgende teori vedrørende nummeriske semigrupper.

6.2.1 Nummeriske semigrupper -genus og konduktor

Dette underafsnit omhandlende nummeriske semigrupper har til formål at præsentere begreberne genus og konduktor, som senere skal benyttes til udledningen af dimensionen for NTP-koden.

Dette underafsnit bygger på [9, Afsnit 10.5].

Definition 63 (Nummerisk semigruppe) *En delmængde $\Gamma \in \mathbb{N}_0$ kaldes en nummerisk semigruppe, hvis følgende er opfyldt:*

(*i*) $0 \in \Gamma$, *og*

(*ii*) *hvis* $r, t \in \Gamma$, *så vil* $r + t \in \Gamma$.

Elementerne i $\mathbb{N}_0 \backslash \Gamma$ kaldes *gaps* og elementerne i Γ kaldes *nongaps*.
Antallet af gaps kaldes *genus* og benævnes g. Herudfra defineres *konduktor*.

Definition 64 (Konduktor) *For* $g < \infty$, *så eksisterer der* $n \in \Gamma$ *sådan, at når* $t \in \mathbb{N}_0$ *og* $t \geq n$, *så vil* $t \in \Gamma$.
Konduktoren for Γ, $c(\Gamma)$, *er da det mindste* $n \in \Gamma$ *sådan, at* $\{t \in \mathbb{N}_0 : t \geq n\}$ *er indeholdt i* Γ.

Af definitionen på konduktor ses det, at den største gap er lig $c(\Gamma) - 1$, hvis $0 < g < \infty$.

Der gælder følgende sammenhæng mellem konduktor og genus:

Proposition 65 *Antag* $g < \infty$. *Så er* $c(\Gamma) \leq 2g$. *Specielt er* $c(\Gamma) = 2g$, *hvis og kun hvis der for ethvert* $t \in \mathbb{N}_0$ *gælder, at hvis* t *er en gap, så er* $c(\Gamma) - 1 - t$ *en nongap.*

Bevis: Betragt et ordnet par af ikke negative heltal (r, t), hvor $r + t = c(\Gamma) - 1$. Idet summen af to nongaps pr. definition er en nongap, er enten r eller t en gap. Der er ialt $c(\Gamma)$ ordnede par, som opfylder ligheden, og da der optræder mindst en gap i hvert par, så er $c(\Gamma) \leq 2g$.

Det ses heraf at der gælder lighed præcis når det ene af de to tal er en gap og det andet er en nongap for alle de ordnede par. □

Hvis $c(\Gamma) = 2g$, så siges den nummeriske semigruppe Γ at være symmetrisk.

Definition 66 (Generator for en nummerisk semigruppe) *Lad* $A = \{a_1, \ldots, a_k\}$ *være en delmængde af en nummerisk semigruppe* Γ. *Hvis der, for ethvert element* $t \in \Gamma$, *eksisterer* $\alpha_1, \ldots, \alpha_k \in \mathbb{N}_0$ *sådan, at* $t = \sum_{i=1}^{k} \alpha_i a_i$, *så siges* Γ *at være genereret af A, hvilket skrives* $\Gamma = \langle A \rangle$.

Ovenstående definition samt Proposition 65 benyttes i efterfølgende proposition.

Proposition 67 *Lad $a, b \in \mathbb{N}$ således, at $\gcd(a,b) = 1$.*
Den nummeriske semigruppe genereret af a og b er symmetrisk, og har $ab-a-b$ som største gap, $(a-1)(b-1)$ som konduktor og genus lig $\frac{(a-1)(b-1)}{2}$.

Bevis: Idet $\gcd(a,b) = 1$, så har ethvert heltal m en entydig repræsentation, givet ved $m = \alpha_1 b + \alpha_2 a$, hvis $0 \leq \alpha_2 < b$.
Heraf samt af Definition 66 gælder det, at enhver gap, m har en entydig repræsentation $m = \alpha_1 b + \alpha_2 a$, hvor $0 \leq \alpha_2 < b$ og $\alpha_1 < 0$, og enhver nongap, m har en entydig repræsentation $m = \alpha_1 b + \alpha_2 a$, hvor $0 \leq \alpha_2 < b$ og $\alpha_1 \geq 0$.

Lad $c(\Gamma)$ være konduktoren for den nummeriske semigruppe $\Gamma = \langle a, b \rangle$. Vi ønsker først at bestemme den største gap for Γ.
Inddeles $\mathbb{Z}$ i ækvivalensklasser modulo b, kan disse repræsenteres af $\alpha_2 a \in \Gamma$, hvor $\alpha_2 = 0, 1, \ldots, b-1$.
For en vilkårlig ækvivalensklasse er det største element, $\alpha_2 a + \alpha_1 b$, hvor koefficienten til b er negativ, lig $\alpha_2 a - b$.
Dermed er den største gap $(b-1)a - b$, hvilken pr. definition af konduktor er lig $c(\Gamma) - 1$. Hvormed $c(\Gamma) = (a-1)(b-1)$.

Det skal nu vises, at $\langle a, b \rangle$ er symmetrisk. Det antages, at r og t er gaps, og at $r + t = c(\Gamma) - 1$.
Der gælder da for r og t, at

$$r = \alpha_1 b + \alpha_2 a, \qquad t = \tilde{\alpha}_1 b + \tilde{\alpha}_2 a, \qquad 0 \leq \alpha_2, \tilde{\alpha}_2 < b \text{ og } \alpha_1, \tilde{\alpha}_1 < 0.$$

Vi har dermed, at $c(\Gamma) - 1 = ab - a - b = (\alpha_1 + \tilde{\alpha}_1)b + (\alpha_2 + \tilde{\alpha}_2)a$, så

$$(-\alpha_1 - \tilde{\alpha}_1 - 1)b = (\alpha_2 + \tilde{\alpha}_2 - b + 1)a,$$

hvor $0 \leq \alpha_2 + \tilde{\alpha}_2 \leq 2b - 2$ og $\alpha_1 + \tilde{\alpha}_1 \leq -2$. Idet parentesen på højresiden er strengt mindre end b og $\gcd(a,b) = 1$, så kan b kun gå op, hvis højresiden er lig nul. Dette er umuligt, da venstresiden er strengt større end nul.
Dermed er der opnået en modstrid, hvormed r og t ikke begge er gaps. Altså følger det af Proposition 65, at $c(\Gamma) = 2g$, hvor g er antallet af gaps, og Γ er dermed symmetrisk. Det vil sige, at $g = \frac{(a-1)(b-1)}{2}$. □

6.2.2 Bestemmelse af dimension af NTP-koden

For at bestemme dimensionen af NTP-koden, skal det først vises, at mængden, $\Gamma(\Delta_{\prec_w}(J))$, bestående af de vægtede grader repræsenteret af monomierne i fodaftrykket af J, udgør en nummerisk semigruppe. Herefter kan vi benytte Proposition 67 til at bestemme genus og konduktor.

Sætning 68 *Mængden $\Gamma(\Delta_{\prec_w}(J))$, udgør en nummerisk semigruppe.*

Bevis: Det er klart, at $0 \in \Gamma(\Delta_{\prec_w}(J))$, så det skal nu vises, at hvis r og t tilhører $\Gamma(\Delta_{\prec_w}(J))$, så vil $r+t \in \Gamma(\Delta_{\prec_w}(J))$.
Lad $r = i_1 q^{m-1} + j_1 \frac{q^m-1}{q-1}$ og $t = i_2 q^{m-1} + j_2 \frac{q^m-1}{q-1}$, så er $r+t = (i_1+i_2)q^{m-1} + (j_1+j_2)\frac{q^m-1}{q-1}$. Da dette er vægten af et monomium, så ved vi fra Korollar 59, at denne vægt er repræsenteret af et monomium tilhørende fodaftrykket af J. Det vil sige, at $r+t \in \Gamma(\Delta_{\prec_w}(J))$. Altså er $\Gamma(\Delta_{\prec_w}(J))$ en nummerisk semigruppe.

□

Da alle vægte i $\Gamma(\Delta_{\prec_w}(J))$ er linearkombinationer af q^{m-1} og $\frac{q^m-1}{q-1}$, er $\Gamma(\Delta_{\prec_w}(J))$ genereret af q^{m-1} og $\frac{q^m-1}{q-1}$ ifølge Definition 66.

Det blev i beviset for Lemma 60 vist, at $\gcd(q^{m-1}, \frac{q^m-1}{q-1}) = 1$. Dermed følger det af Proposition 67, at konduktoren, $c(\Gamma)$, for den nummeriske semigruppe $\Gamma(\Delta_{\prec_w}(J))$, er lig $(\frac{q^m-1}{q-1}-1)(q^{m-1}-1)$, og at genus er lig

$$\frac{(\frac{q^m-1}{q-1}-1)(q^{m-1}-1)}{2}.$$

Det er nu muligt, at opskrive formlen til bestemmelse af dimensionen for koden $NTP(s)$ indenfor et begrænset interval af s.

Sætning 69 (Dimension af NTP-koden) *Lad $NTP(s)$ være en NTP-kode. Da er dimensionen $k(NTP(s))$ givet ved:*

$$k(NTP(s)) = s + 1 - g \qquad for \qquad c(\Gamma) - 1 \leq s < q^{2m-1},$$

hvor $g = \frac{(\frac{q^m-1}{q-1}-1)(q^{m-1}-1)}{2}$ *og* $c(\Gamma) = (\frac{q^m-1}{q-1}-1)(q^{m-1}-1)$.

Bevis: Antag, at s er større end eller lig $c(\Gamma) - 1$. Så gælder det, idet monomierne i $\Delta_{\prec_w}(J)$ ifølge Lemma 60 alle har forskellig vægt, at antallet af monomier i $\Delta_{\prec_w}(J)$ med vægt mindre end eller lig s er, s plus monomiet med vægt nul minus antallet af elementer, som ikke repræsenterer noget monomium. Sidstnævnte svarer netop til antallet af gaps.

Da koderne $NTP(s)$ kun består af linearkombinationer af monomier med vægt mindre end eller lig s, som tilhører $\Delta_{\prec_w}(I)$, så er det nødvendigt at fastsætte en øvre grænse for s for at kunne bestemme dimensionen af koden, som beskrevet ovenfor.
Denne øvre grænse for s er $q^{2m-1} - 1$, idet q^{2m-1} er vægten af det første monomium som ligger udenfor $\Delta_{\prec_w}(I)$.
Dermed er sætningen bevist. □

Sætningen giver altså kun en formel til bestemmelse af dimensionen for NTP-koden på et afgrænset interval for s. Vælges et s udenfor dette interval er fremgangsmåden at tælle monomier med vægtet grad mindre end eller lig s, som beskrevet i indledningen til Afsnit 6.2.

Efter dimensionen for en NTP-kode er bestemt kan generatormatricen for NTP-koden beskrives. Rækkerne består af monomierne i fodaftrykket af I, hvis vægtede grad er mindre end eller lig s, evalueret i de $q^{2m-1} = n$ punkter. Det vil sige, at generatormatricen er en $(\dim(NTP(s)) \times n)$-matrix.

6.3 Dualkode

I dette afsnit bestemmes NTP-kodens dualkode.
En dualkode, $C^\perp$, til en kode C, er udspændt af rækkerne i paritetstjeksmatricen for C. Det vil sige, at

$$C^\perp = \{\overline{x} \in \mathbb{F}_{q^m}^n : \overline{x} \cdot \overline{c} = 0 \quad \forall \overline{c} \in C\}.$$

Dermed kan vi ved at bestemme dualkoden til NTP-koden også finde dennes paritetstjeksmatrix.

I beviset for Sætning 71 får vi brug for følgende lemma:

Lemma 70 *Betragt $\mathbb{F}_{q^m}$, hvor q er en primtalspotens, p^r. Hvis det gælder, at $i \in \{1, \ldots, q^m - 2\}$, så er*

$$\sum_{\gamma \in \mathbb{F}_{q^m}} \gamma^i = 0.$$

Bevis: Lad α være et primitivt element i $\mathbb{F}_{q^m}$, så er

$$\begin{aligned}
\sum_{\gamma \in \mathbb{F}_{q^m}} \gamma^i &= \left(\sum_{j=0}^{q^m-2} (\alpha^j)^i \right) + 0^i \\
&= \sum_{j=0}^{q^m-2} (\alpha^i)^j \\
&= \frac{(\alpha^i)^{q^m-1} - 1}{\alpha^i - 1} \\
&= \frac{(\alpha^{q^m-1})^i - 1}{\alpha^i - 1} = 0.
\end{aligned}$$

□

Det er nu muligt at vise, hvordan dualkoden til en NTP-kode findes.
Efterfølgende sætning er en generalisering af [5, Theorem 14.1.4].

Sætning 71 *Lad s tilhøre intervallet $c(\Gamma) - 2 < s < q^{2m-1}$, hvor q er en primtalspotens p^r. Dualkoden til $NTP(s)$ er da givet ved koden $NTP(n + c(\Gamma) - 2 - s)$, hvor $n = q^{2m-1}$ og $c(\Gamma) = (q^{m-1} - 1)\left(\frac{q^m-1}{q-1} - 1\right)$.*

Bevis: For at $NTP(n+c(\Gamma)-2-s)$ er dualkoden til $NTP(s)$, skal den opfylde, at dens dimension er $n-k(NTP(s))$, samt at alle kodeord i $NTP(n+c(\Gamma)-2-s)$ er ortognale med alle kodeord i $NTP(s)$.

For at bestemme dimensionen af $NTP(n + c(\Gamma) - 2 - s)$ ønskes det at benytte Sætning 69. Dermed skal følgende dobbeltulighed være opfyldt

$$c(\Gamma) - 2 < q^{2m-1} + c(\Gamma) - 2 - s < q^{2m-1}.$$

Da $s < q^{2m-1}$ er den første ulighed opfyldt, og da $s > c(\Gamma)-2$ er også den anden ulighed opfyldt. Dermed kan Sætning 69 benyttes til at bestemme dimensionen af $NTP(n + c(\Gamma) - 2 - s)$ til

$$\begin{aligned} & n + c(\Gamma) - 2 - s + 1 - \frac{c(\Gamma)}{2} \\ &= n - s - 1 + \frac{c(\Gamma)}{2}, \end{aligned}$$

hvilket netop er $n - k(NTP(s))$.

Dernæst skal det vises, at kodeordene i $NTP(n+c(\Gamma)-2-s)$ alle er ortogonale med alle kodeordene i $NTP(s)$.
Betragt fodaftrykket $\Delta_{\prec_w}(I) = \{x^i y^j : 0 \leq i < q^m, 0 \leq j < q^{m-1}\}$. For et vilkårligt kodeord, $\overline{c}_1$, i $NTP(s)$ vil der eksistere et polynomium, $F \in \mathbb{F}_{q^m}[x, y]$, i $\text{Span}\{M \in \Delta_{\prec_w}(I) : w(M) \leq s\}$, sådan at $\overline{c}_1 = (F(p_1), \ldots, F(p_n))$.
Ligeledes vil der for et vilkårligt kodeord, $\overline{c}_2$ i $NTP(n+c(\Gamma)-2-s)$ eksistere et polynomium, $G \in \mathbb{F}_{q^m}[x, y]$, i $\text{Span}\{M \in \Delta_{\prec_w}(I) : w(M) \leq (n + c(\Gamma) - 2 - s)\}$, sådan at $\overline{c}_2 = (G(p_1), \ldots, G(p_n))$. For at vise at kodeordene er ortogonale skal deres prikprodukt være lig nul. Altså skal

$$\begin{aligned} \overline{c}_1 \cdot \overline{c}_2 &= (F(p_1)G(p_1) + \cdots + F(p_n)G(p_n)) \\ &= \sum_{i=1}^{n} (FG)(p_i) = 0. \end{aligned}$$

Da NTP-koden er en lineær kode, er det nok at tjekke de kodeord, som danner baser for koderne, hvilket her betyder, at F og G blot skal være monomier fra fodaftrykket af I. Det vil sige, at $F = x^{i_1} y^{j_1}$ og $G = x^{i_2} y^{j_2}$, hvor det er opfyldt, at $i_1, i_2 < q^m$ og $j_1, j_2 < q^{m-1}$. Dermed er $FG = x^{i_1+i_2} y^{j_1+j_2}$.
Fra Sætning 49 kender vi udseendet af punkterne, hvilket her kan benyttes til udregning af prikproduktet $\overline{c}_1 \cdot \overline{c}_2$. Det vil nu gælde, at prikproduktet får følgende udseende

$$\sum_{\beta^{q^{m-1}} + \cdots + \beta^q + \beta = 0} 0^{i_1+i_2} \beta^{j_1+j_2} + \sum_{k=0}^{q-2} \sum_{\substack{\beta^{q^{m-1}} + \cdots + \beta^q + \beta = \\ \delta^k \frac{q^m-1}{q-1}}} \beta^{j_1+j_2} \sum_{l=0}^{\frac{q^m-1}{q-1}-1} \left(\delta^{k+l(q-1)}\right)^{i_1+i_2}, \tag{6.1}$$

hvor δ er et primitivt element i $\mathbb{F}_{q^m}$.
Er $i_1 + i_2 = 0$ vil den første sum i (6.1) overleve og den sidste sum vil give $\frac{q^m-1}{q-1} =$

$1+q+\cdots+q^{m-1}$, hvilket er lig 1, idet vi regner over $\mathbb{F}_{q^m}$ med karakteristik p. Dette giver alt i alt, at ligning (6.1) kan omskrives til:

$$\sum_{\beta \in \mathbb{F}_{q^m}} \beta^{j_1+j_2}. \tag{6.2}$$

For $j_1+j_2=0$ er (6.2) lig q^m, hvilket er nul, da vi regner med karakteristik p. Det gælder desuden, at $j_1+j_2 \leq \frac{q^m}{q}-1+\frac{q^m}{q}-1 = 2\frac{q^m}{q}-2$. Da $q \geq 2$, vil det derfor være opfyldt, at $j_1+j_2 < q^m-1$. Dermed bliver ligning (6.2) ifølge Lemma 70 lig nul, hvormed kodeordene i de to koder er ortogonale, når $i_1+i_2=0$.

Hvis $i_1+i_2 \neq 0$ vil den første sum i ligning (6.1) blive nul, og det resterende kan skrives op som følgende

$$\sum_{k=0}^{q-2} \delta^{k(i_1+i_2)} \sum_{\substack{\beta_k^{q^{m-1}}+\cdots+\beta_k^q+\beta_k= \\ \delta^k\frac{q^m-1}{q-1}}} \beta^{j_1+j_2} \sum_{l=0}^{\frac{q^m-1}{q-1}-1} \delta^{l(q-1)(i_1+i_2)}. \tag{6.3}$$

Hvis $\delta^{(q-1)(i_1+i_2)} \neq 1$, vil følgende omskrivning af sidste sum kunne foretages, idet δ er et primitivt element for $\mathbb{F}_{q^m}$.

$$\sum_{l=0}^{\frac{q^m-1}{q-1}-1} \delta^{l(q-1)(i_1+i_2)} = \frac{\left(\delta^{(q-1)(i_1+i_2)}\right)^{\left(\frac{q^m-1}{q-1}\right)}-1}{\delta^{(q-1)(i_1+i_2)}-1} = \frac{\left(\delta^{(q^m-1)}\right)^{(i_1+i_2)}-1}{\delta^{(q-1)(i_1+i_2)}-1} = 0,$$

hvormed hele summen i ligning (6.3) er lig nul.

Tilbage er nu at betragte tilfældet, hvor $\delta^{(q-1)(i_1+i_2)}=1$.
Dette medfører, idet δ er et primitivt element for $\mathbb{F}_{q^m}$, at $(q^m-1)|((q-1)(i_1+i_2))$.
Hermed gælder det, at $i_1+i_2 = h\left(\frac{q^m-1}{q-1}\right)$, hvor $h \geq 1$.
Desuden ved vi, da $x^{i_1}y^{j_1} \in NTP(s)$ og $x^{i_2}y^{j_2} \in NTP(n+c(\Gamma)-2-s)$, at $w(x^{i_1}y^{j_1}) \leq s$ og $w(x^{i_2}y^{j_2}) \leq n+c(\Gamma)-2-s$, og endelig har vi, at $j_1+j_2 \leq 2(q^{m-1}-1)$.

Det skal altså vises, at (6.3) er lig nul under følgende tre omstændigheder:

1. Lad w være vægtfunktionen hvor $w(x^iy^j) = i(q^{m-1}) + j(\frac{q^m-1}{q-1})$, så er

$$\begin{aligned} w(x^{i_1+i_2}y^{j_1+j_2}) &\leq s+n+c(\Gamma)-2-s \\ &= q^{2m-1}+\frac{q^m-1}{q-1}\cdot q^{m-1}-q^{m-1}-\frac{q^m-1}{q-1}-1 \\ &= q^{2m-1}+\frac{q^{m-1}-1}{q-1}\cdot q^m-\frac{q^m-1}{q-1}-1. \end{aligned}$$

2. $i_1 + i_2 = h \cdot \frac{q^m-1}{q-1}$, hvor $h \geq 1$.
3. $j_1 + j_2 \leq 2(q^{m-1} - 1)$.

Først vises det, at $h \in \{1, \ldots, q-1\}$.
Antag, at $h \geq q$, så er

$$\begin{aligned} w(x^{i_1+i_2}y^{j_1+j_2}) &\geq w(x^{i_1+i_2}) \\ &= h \cdot \frac{q^m-1}{q-1} \cdot q^{m-1} \\ &\geq q \cdot \frac{q^m-1}{q-1} \cdot q^{m-1} \\ &= q^m(1 + q + \cdots + q^{m-1}) \\ &= q^{2m-1} + \frac{q^{m-1}-1}{q-1} \cdot q^m. \end{aligned}$$

Da dette er i modstrid med betingelse 1 vil $h \in \{1, \ldots, q-1\}$.

Det er nu muligt at vende tilbage til (6.3), som nu får udseendet

$$\sum_{k=0}^{q-2} \delta^{kh(\frac{q^m-1}{q-1})} \sum_{\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)=\delta^{k(\frac{q^m-1}{q-1})}} \beta^{j_1+j_2} \sum_{l=0}^{\frac{q^m-1}{q-1}-1} (\delta^{q^m-1})^{lh}. \tag{6.4}$$

For overskuelighedens skyld er $\beta^{q^{m-1}} + \cdots + \beta^q + \beta$ erstattet med $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$ i den midterste sum.
Idet der regnes i $\mathbb{F}_{q^m}$, med karakteristik p , er $\frac{q^m-1}{q-1} = 1+q+\cdots+q^{m-1} = 1$, hvormed (6.4) kan skrives som:

$$\sum_{k=0}^{q-2} \delta^{kh(\frac{q^m-1}{q-1})} \sum_{\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)=\delta^{k(\frac{q^m-1}{q-1})}} \beta^{j_1+j_2}. \tag{6.5}$$

For hvert k eksisterer der q^{m-1} β'er, så $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = \delta^{k(\frac{q^m-1}{q-1})}$. Det vil sige, at den samlede sum består af $(q-1)(q^{m-1}) = q^m - q^{m-1}$ led.
Dette svarer netop til det antal β'er, hvor $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) \neq 0$.

Desuden er δ et primitivt element for $\mathbb{F}_{q^m}$, og dermed gennemløber $\delta^{k(\frac{q^m-1}{q-1})}$ $\mathbb{F}_q^*$, for $k = 0, \ldots, q-2$, og idet der præcis er q^{m-1} β'er, som giver det samme $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) \in \mathbb{F}_q^*$, kan (6.5) omskrives til

$$\sum_{\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)\neq 0} (\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta))^h \cdot \beta^{j_1+j_2}. \tag{6.6}$$

Da $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = 0$ ikke vil bidrage med noget yderligere til summen, så er (6.6) det samme som

$$\sum_{\beta \in \mathbb{F}_{q^m}} (\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta))^h \cdot \beta^{j_1+j_2}. \tag{6.7}$$

Det skal alså vises, at denne sum er lig nul, og fra Lemma 70 ved vi, at en sum på formen $\sum_{\beta \in \mathbb{F}_{q^m}} \beta^t = 0$, når $t \in \{1, \ldots, q^m - 2\}$.
Den mindst forekommende potens i (6.7) er $h+j_1+j_2$. Det er klart, at denne er strengt større end nul, idet $j_1 + j_2 \geq 0$ og $h \geq 1$.
Det skal herefter vises at den højest forekommende potens i (6.7) er strengt mindre end $q^m - 1$.

Fra tidligere i beviset ved vi, at $h \in \{1, \ldots, q-1\}$.
Antag først, at $h \leq q-2$, så har vi fra betingelse 3, at

$$\begin{aligned} h \cdot \deg(\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}) + j_1 + j_2 &\leq (q-2)(q^{m-1}) + 2(q^{m-1}-1) \\ &= q^m - 2 \\ &< q^m - 1. \end{aligned}$$

Dermed er der kun det tilfælde tilbage, hvor $h = q-1$.
Af betingelse 2 har vi, at

$$i_1 + i_2 = (q-1)(\frac{q^m-1}{q-1}) = q^m - 1,$$

og af betingelse 1 fås da

$$\begin{aligned} w(y^{j_1+j_2}) &\leq q^{2m-1} + \frac{q^m-1}{q-1} \cdot q^{m-1} - q^{m-1} - \frac{q^m-1}{q-1} - 1 - w(x^{i_1+i_2}) \\ &= q^{2m-1} + \frac{q^m-1}{q-1} \cdot q^{m-1} - q^{m-1} - \frac{q^m-1}{q-1} - 1 - q^{m-1}(q^m-1) \\ &= \frac{q^m-1}{q-1} \cdot q^{m-1} - \frac{q^m-1}{q-1} - 1 \\ &= \frac{q^m-1}{q-1}(q^{m-1}-1) - 1. \end{aligned}$$

Det vil sige, at $j_1 + j_2 \leq q^{m-1} - 1 - \frac{q-1}{q^m-1} < q^{m-1} - 1$.

Den højeste potens i (6.7) bliver da:

$$\begin{aligned} h(q^{m-1}) + j_1 + j_2 &< (q-1)(q^{m-1}) + q^{m-1} - 1 \\ &= q^m - 1. \end{aligned}$$

Hermed er det vist, at (6.3) er lig nul under betingelse 1, 2 og 3.

Altså er $NTP(n + c(\Gamma) - 2 - s)$ dualkoden til $NTP(s)$, når $c(\Gamma) - 2 < s < q^{2m-1}$. □

Paritetstjeksmatricen til $NTP(s)$ er hermed lig generatormatricen for $NTP(n + c(\Gamma) - 2 - s)$.
Rækkerne i paritetstjeksmatricen for $NTP(s)$-koden består altså af monomierne i fodaftrykket af I, hvis vægtede grad er mindre end eller lig $(n + c(\Gamma) - 2 - s)$, evalueret i de $q^{2m-1} = n$ punkter.

Kapitel 7

Dekodning af NTP-koder

I dette kapitel, som er baseret på [5, Afsnit 14.2], vil vi se nærmere på dekodning af NTP-koder.

Betragt koden $NTP(s)$, givet som i Definition 57, samt et modtaget ord, $\overline{r} = (r_1, \ldots, r_n)$, som er en sum af et kodeord $\overline{c} = (f(p_1), \ldots, f(p_n))$ og en fejlvektor, $\overline{e}$, med vægt τ. For at kunne finde frem til det afsendte kodeord ønsker vi at bestemme interpolationspolynomiet:

$$Q(x, y, z) = Q_0(x, y) + zQ_1(x, y) \in \mathbb{F}_{q^m}[x, y, z] \setminus \{0\},$$

hvor

1. $Q(x_i, y_i, r_i) = 0, i = 1, \ldots, n.$
2. $w(Q_0) \leq s + \tau + g.$
3. $w(Q_1) \leq \tau + g.$

Først vises det, at der altid vil eksistere et sådant polynomium.

Sætning 72 *Lad der være sket τ fejl i det modtagne ord $\overline{r}$, så eksisterer der mindst et polynomium $Q(x, y, z)$ forskellig fra nulpolynomiet, som opfylder de tre betingelser.*

Bevis: Lad $\phi_0, \ldots, \phi_n$ være ordningen af monomierne i fodaftrykket af idealet I udfra vægtfunktionen w.
Lad fejlpositionerne i $\overline{r}$ være $j_1, \ldots, j_\tau$, og

$$Q_1(x, y) = \sum_{i=0}^{\tau} \lambda_i \phi_i(p_{j_s}) = 0, \, \forall s = 1, \ldots \tau,$$

hvor $\lambda_i \in \mathbb{F}_q$ for $i = 0, \ldots, \tau$.
Idet der er τ homogene ligninger med $\tau + 1$ ubekendte vil et sådant polynomium altid eksistere.
Dette benyttes nu til at konstruere et polynomium $Q(x, y, z)$, som opfylder alle tre betingelser.
Lad $f(x, y)$ være det polynomium, der svarer til det afsendte kodeord, og $r(x, y)$ det, som svarer til det modtagne ord. Så gælder det, at $f(p_j)Q_1(p_j) = r(p_j)Q_1(p_j)$ for $j = 1, \ldots, n$, da $f(p_j) = r(p_j)$, når p_j ikke er en fejlposition, og $Q_1(p_j) = 0$ når p_j er en fejlposition. Hermed vil polynomiet givet ved

$$Q(x, y, z) = f(x, y)Q_1(x, y) - zQ_1(x, y)$$

opfylde betingelse 1.
Da $Q_1(x, y) = \sum_{i=0}^{\tau} \lambda_i \phi_i$, så er de vægtede grader hørende til monomierne i $Q_1(x, y)$ mindre end eller lig $\tau + g$. Det vil sige, at $w(Q_1(x, y)) \leq \tau + g$.
Da $Q_0 = f(x, y)Q_1(x, y)$, hvor $w(f(x, y)) \leq s$ og $w(Q_1(x, y)) \leq \tau + g$, er $w(Q_0(x, y)) \leq s + \tau + g$. Hermed opfylder $Q(x, y, z)$ alle tre betingelser, og sætningen er vist. □

Efter at have vist, at interpolationspolynomiet altid eksisterer, bevises i næste sætning en egenskab ved interpolationspolynomiet, som kan udnyttes i dekodningen.

Sætning 73 *Hvis antallet af fejlpositioner i $\overline{r}$ er mindre end $\frac{n-s-g}{2}$, så er fejlpositionerne i $\overline{r}$ nulpunkter i $Q_1(x, y)$.*

Bevis: Lad der være sket τ fejl i et modtaget ord $\overline{r}$, således at $\tau < \frac{n-s-g}{2}$, hvormed $s + \tau + g < n - \tau$.
I beviset benyttes notationen

$$\begin{aligned} NT(x,y) &= x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, \\ J &= \langle NT(x,y) \rangle. \end{aligned}$$

Ideen i beviset er at tage udgangspunkt i interpolationspolynomiet $Q(x, y, f(x, y))$, hvor det afsendte ord, $\overline{c}$, er genereret af polynomiet $f(x, y)$.

Det ønskes at kunne benytte Propostition 58, og for at dette er muligt, skal vi sikre os, at det polynomium, som svarer til $G(x, y)$ i propositionen, kun indeholder ét monomium med den højeste vægt.
Ifølge Proposition 51 kunne et sådant polynomium være den simple repræsentant for den ækvivalensklasse i $\mathbb{F}_{q^m}[x, y]/J$, som indeholder $Q(x, y, f(x, y))$. Denne simple repræsentant er nemlig restleddet frembragt ved division af $Q(x, y, f(x, y))$ med polynomierne i J. Det vil sige, den er en linearkombination af monomierne i fodaftrykket af J, hvilke ifølge Lemma 60 alle har forskellig vægt.

Den simple repræsentant har dermed udseendet

$$\tilde{Q}(x, y, f(x, y)) = Q(x, y, f(x, y)) - g(x, y)NT(x, y), \tag{7.1}$$

hvor $g(x, y) \in \mathbb{F}_{q^m}[x, y]$. Dette polynomium, $\tilde{Q}$, undersøges nu nærmere.

Det ønskes først vist, at $w(Q(x, y, f(x, y))) \geq w(\tilde{Q}(x, y, f(x, y)))$.
Hvis $\tilde{Q}(x, y, f(x, y))$ er forskellig fra $Q(x, y, f(x, y))$, så betyder det, at $\mathtt{LT}(NT(x, y))$ går op i $\mathtt{LT}(Q(x, y, f(x, y)))$, og da $\mathtt{LT}(NT(x, y)) = y^{q^{m-1}}$ vil Q være på formen

$$Q(x, y, f(x, y)) = x^i y^{(nq^{m-1}+k)} + Q'(x, y, f(x, y)),$$

hvor $k < q^{m-1}$ og $w(Q'(x, y, f(x, y))) \leq w(x^i y^{(nq^{m-1}+k)})$.
Det ønskes nu bekræftet, at den største vægt i $Q(x, y, f(x, y))$ ikke vokser ved division af $Q(x, y, f(x, y))$ med $NT(x, y)$.

Vægten af $Q(x, y, f(x, y))$ før division er

$$w(Q(x, y, f(x, y))) = i(q^{m-1}) + (nq^{m-1} + k)\left(\frac{q^m - 1}{q - 1}\right).$$

Idet $-y^{q^{m-1}}(-x^i y^{((n-1)q^{m-1}+k)}) = x^i y^{(nq^{m-1}+k)}$, ganges $NT(x,y)$ i første divisionsskridt med $-x^i y^{((n-1)q^{m-1}+k)}$, hvilket efterfølgende trækkes fra $Q(x,y,f(x,y))$.
Hermed elimineres $x^i y^{(nq^{m-1}+k)}$, og den største vægt stammer nu enten fra monomiet $x^{\frac{q^m-1}{q-1}} x^i y^{((n-1)q^{m-1}+k)}$ eller et monimium i $Q'(x,y,f(x,y))$. Vægten af monomiet $x^{\frac{q^m-1}{q-1}} x^i y^{((n-1)q^{m-1}+k)}$ er

$$\begin{aligned}(i + \frac{q^m-1}{q-1})(q^{m-1}) + ((n-1)q^{m-1}+k)\left(\frac{q^m-1}{q-1}\right) \\ = i(q^{m-1}) + (nq^{m-1}+k)\left(\frac{q^m-1}{q-1}\right),\end{aligned}$$

og idet, $w(Q'(x,y,f(x,y))) \leq w(Q(x,y,f(x,y)))$ ses det, at vægten ikke bliver større ved udførsel af et divisionsskridt, men derimod kan blive mindre, hvis der i Q' findes led, som netop ophæver monomiet $x^{\frac{q^m-1}{q-1}} x^i y^{((n-1)q^{m-1}+k)}$. Dermed er

$$w(Q(x,y,f(x,y))) \geq w(\tilde{Q}(x,y,f(x,y))).$$

Da $Q(x,y,f(x,y))$ opfylder betingelse 2 og 3 for interpolationspolynomiet, vil vægten af $Q(x,y,f(x,y))$ være højst $s+\tau+g$, da vægten af $f(x,y)$ højst er s. Udfra antagelsen om antal skete fejl, kan det konkluderes, at

$$n - \tau > s + \tau + g \geq w(Q(x,y,f(x,y))) \geq w(\tilde{Q}(x,y,f(x,y))). \tag{7.2}$$

Dermed er alle detaljerne på plads til at anvende Proposition 58. Propositionen giver, at $NT(x,y)$ og $\tilde{Q}(x,y,f(x,y))$ højst har $w(\tilde{Q}(x,y,f(x,y)))$ fælles nulpunkter. Det vil sammen med ligning (7.2) give, at

$$\#\mathbf{V}(\langle \tilde{Q}(x,y,f(x,y)), NT(x,y)\rangle) \leq s+\tau+g < n-\tau. \tag{7.3}$$

Ved at betragte $Q(x,y,f(x,y))$ og $\tilde{Q}(x,y,f(x,y))$, i ligning (7.1) ses det, at de fælles nulpunkter mellem $Q(x,y,f(x,y))$ og $NT(x,y)$ er de samme punkter, som er fælles nulpunkter mellem $\tilde{Q}(x,y,f(x,y))$ og $NT(x,y)$.
Da $Q(x,y,f(x,y))$ desuden opfylder betingelse 1 for interpolationspolynomiet, betyder dette, at $Q(x,y,f(x,y))$ har mindst $n-\tau$ nulpunkter blandt punkterne $p_1,\ldots,p_n$, som er løsningerne til $NT(x,y)$. Dette svarer til, at antal punkter i varieteten $\mathbf{V}(\langle Q(x,y,f(x,y)), NT(x,y)\rangle)$ er mindst $n-\tau$. Dermed kan det også udfra ovenstående konkluderes, at

$$\#\mathbf{V}(\langle \tilde{Q}(x,y,f(x,y)), NT(x,y)\rangle) \geq n-\tau.$$

Dette er i modstrid med ligning (7.3), så hermed må det konkluderes, at $\tilde{Q}$ er nulpolynomiet. Dermed er $Q(x, y, f(x, y))$ et multiplum af norm- trace polynomiet.
Det vil sige, at $Q_0(p_j) + f(p_j)Q_1(p_j) = 0$, for $j = 1, \ldots, n$. Desuden opfylder $Q(x, y, z)$ betingelse 1, og derfor er $Q_0(p_j) + r(p_j)Q_1(p_j) = 0$, for $j = 1, \ldots, n$. Ved at trække de to udtryk fra hinanden fås:

$$(r(p_j) - f(p_j))Q_1(p_j) = 0, \text{ for } j = 1, \ldots, n.$$

Da $r(p_j) - f(p_j)$ ikke er nul for de p_j, hvor der er sket fejl, må det være Q_1 der er nul i disse positioner. Altså er nulpunkterne, blandt $p_1, \ldots, p_n$, til Q_1 fejlpositionerne i $\overline{r}$. □

Denne sætning giver os altså en metode til at bestemme fejlpositionerne i det modtagne ord. For at kunne bestemme fejlvektoren, introduceres *syndrom.*

Definition 74 (Syndrom) *Lad H være en paritetstjeksmatrix for en NTP-kode, og lad $\overline{r} = \overline{c} + \overline{e} \in \mathbb{F}_{q^m}^n$, så er syndromet $S = Syn(\overline{r})$ givet ved:*

$$S = H\overline{r}^T = H(\overline{c} + \overline{e})^T = H\overline{e}^T.$$

Indgangene i S kaldes desuden syndromer.

Det er nu muligt, at opstille en dekodningsalgoritme for NTP-koder. Til dette formål defineres $l_0 = s + \lfloor \frac{n-s-g}{2} \rfloor$ og $l_1 = \lfloor \frac{n-s-g}{2} \rfloor$. Dermed beskriver $l_0 + 1$ og $l_1 + 1$ en øvre grænse for antallet af monomier, som optræder i henholdsvis Q_0 og Q_1. Algoritmen er som følgende:

Algoritme 75
Input: Et modtaget ord $\overline{r} = (r_1, \ldots, r_n)$.
Output: Fejlvektoren $\overline{e}$.

1. *Løs følgende lineære ligningssystem:*

$$\begin{bmatrix} \phi_0(p_1) & \phi_1(p_1) & \cdots & \phi_{l_0}(p_1) & r_1\phi_0(p_1) & r_1\phi_1(p_1) & \cdots & r_1\phi_{l_1}(p_1) \\ \phi_0(p_2) & \phi_1(p_2) & \cdots & \phi_{l_0}(p_2) & r_2\phi_0(p_2) & r_2\phi_1(p_2) & \cdots & r_2\phi_{l_1}(p_2) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \phi_0(p_n) & \phi_1(p_n) & \cdots & \phi_{l_0}(p_n) & r_n\phi_0(p_n) & r_n\phi_1(p_n) & \cdots & r_n\phi_{l_1}(p_n) \end{bmatrix} \begin{bmatrix} Q_{0,0} \\ Q_{0,1} \\ Q_{0,2} \\ \vdots \\ Q_{0,l_0} \\ Q_{1,0} \\ Q_{1,1} \\ \vdots \\ Q_{1,l_1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

2. *Sæt* $Q_1(x,y) = \sum_{j=0}^{l_1} Q_{1,j}\phi_j$.
3. *Find nulpunkterne til* $Q_1(x,y)$ *blandt punkterne* $p_1, \ldots, p_n$.
4. *Bestem syndromerne ved hjælp af paritetstjeksmatricen og det modtagne ord.*
5. *Løs det lineære ligningssystem* $H\overline{e} = S$*, ved hjælp af paritetstjeksmatricen, de udregnede syndromer samt fejlpositionerne, for at bestemme fejlvektoren.*

Denne algoritme virker, da Sætning 72 giver, at der altid vil eksistere en løsning til det opskrevne ligningssystem, hvorefter Sætning 73 sikrer, at det er muligt at finde fejlpositionerne herudfra, hvis der er sket færre end $\frac{n-s-g}{2}$ fejl. Tilsidst giver definitionen af syndrom, at det er muligt også at bestemme fejlværdierne. Når det er opfyldt, at $\tau < \frac{n-s-g}{2} \leq \frac{d-g}{2} < \frac{d}{2}$, er koden τ-fejlkorrigerende ifølge Proposition 5. Dermed bliver løsningerne til ligningssystemet i punkt 5, entydige da der ellers ville eksistere $\overline{e}_1$ og $\overline{e}_2$ begge med Hammingvægt mindre end eller lig τ, sådan at $\overline{r} = \overline{c}_1 + \overline{e}_1 = \overline{c}_2 + \overline{e}_2$, hvilket er i modstrid med, at koden er τ-fejlkorrigerende.

Kapitel 8

Vurdering af NTP-koder i forhold til RS-koder

I dette kapitel gives en kort vurdering af, hvor gode NTP-koderne er i forhold til Reed-Solomon koderne.
Med gode koder menes der her, at koden kan rette mange fejl, det vil sige, at koden har en stor relativ minimumsafstand, samtidig med at den har en forholdsvis høj hastighed.
Dermed ønsker vi at plotte punkterne $\left(\frac{d}{n}, \frac{k}{n}\right)$, for både NTP- og RS-koderne over et fastsat endeligt legeme $\mathbb{F}_{q^m}$.
Det vil sige, at man for en bestemt hastighed kan afgøre, hvor mange fejl den pågældende NTP- og RS-kode kan rette i forhold til længden af kodeordene, og modsat kan man, for et fastsat $\frac{d}{n}$, afgøre, hvor stor hastigheden er for henholdsvis NTP- og RS-koden.

Idet minimumsafstanden for RS-koder er givet ved $d = n-k+1$, så har punktet $\left(\frac{d}{n}, \frac{k}{n}\right)$ udseendet:

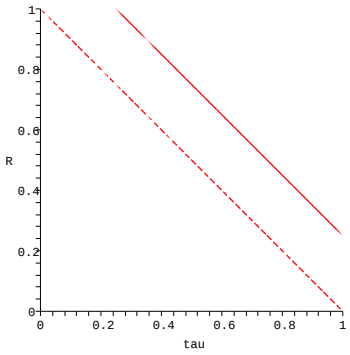
$$\begin{aligned}\left(\frac{d}{q^m}, \frac{k}{q^m}\right) &= \left(\tau, \frac{q^m - d + 1}{q^m}\right) \\ &= \left(\tau, 1 - \tau + \frac{1}{q^m}\right).\end{aligned}$$

Da vi ønsker at sammenligne disse med NTP-koderne, betragter vi punktet $\left(\frac{d}{n}, \frac{k}{n}\right)$, for disse, hvor vi lader $d = n - s$ og $k = s + 1 - g$.

$$\begin{aligned}\left(\frac{d}{q^{2m-1}}, \frac{k}{q^{2m-1}}\right) &= \left(\tau, \frac{q^{2m-1} - d + 1 - g}{q^{2m-1}}\right) \\ &= \left(\tau, 1 - \tau + \frac{1}{q^{2m-1}} - \frac{\left(\frac{q^m - 1}{q-1} - 1\right)\left(q^{m-1} - 1\right)}{2 \cdot q^{2m-1}}\right).\end{aligned}$$

Som det herudfra ses, er andenkoordinaten, $\frac{k}{q^{2m-1}}$, for NTP-koden mindre end andenkoordinaten, $\frac{k}{q^m}$, for RS-koden for et fastsat $\frac{d}{n}$. Så tilsvarende vil der for en fast hastighed gælde, idet punkterne beskriver rette linier i $\frac{d}{n}$ med hældning -1, at det er muligt for RS-koden at rette flere fejl i forhold til længden af kodeord, end det er for NTP-koden.

Vi vil nu betragte et eksempel, som illustrerer dette.



Figur 8.1: *Sammenligning af NTP-koderne og Reed-Solomon koderne for $q = 2$ og $m = 2$.*

Lad $q = 2$ og $m = 2$. Hermed er linien, som repræsenterer RS-koderne, givet ved $\frac{k}{n} = R = 1 - \tau + \frac{1}{4}$, og linien, som repræsenterer NTP-koderne, er givet ved $R = 1 - \tau$.
Heraf fremgår det, at linien, som repræsenterer RS-koderne, ligger øverst på

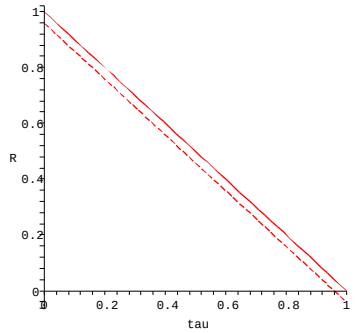
Figur 8.1, hvormed det for en given hastighed er muligt at rette flere fejl i forhold til længden af kodeordene i RS-koden, sammenlignet med NTP-koden, se Figur 8.1.
Som det ses på figuren, skærer linien, som repræsenterer RS-koden, ingen af akserne, hvilket skyldes, at $\frac{k}{n} \leq 1$ og $\frac{d}{n} \leq 1$ for alle koder.

Det kan desuden vises, at de to linier nærmer sig hinanden når q^m vokser.
Betragt for et fast τ udtrykket

$$\begin{aligned} 1-\tau+\frac{1}{q^m} &- \left(1-\tau+\frac{1}{q^{2m-1}}-\frac{\left(\frac{q^m-1}{q-1}-1\right)\left(q^{m-1}-1\right)}{2\cdot q^{2m-1}}\right) \\ &= \frac{1}{q^m}-\frac{1}{q^{2m-1}}+\frac{1}{2(q-1)}-\frac{1}{q^m-q^{m-1}}+\frac{1}{2(q^{2m-1}-q^{2m-2})}. \end{aligned}$$

Som det ses vil dette udtryk gå mod nul, for $q \to \infty$ og $m \to \infty$, hvormed det for en fastsat hastighed vil gælde, at NTP-koden og RS-koden kan rette næsten lige mange fejl i forhold til længden af de pågældende koder, når både q og m går mod uendelig.

Dette er illustreret ved at sammenligne Figur 8.1 med Figur 8.2. I dette tilfælde



Figur 8.2: *Sammenligning af NTP-koderne og Reed-Solomon koderne for $q = 13$ og $m = 5$.*

er $q = 13$ og $m = 5$, og det ses, at de to linier har nærmet sig hinanden i forhold til på Figur 8.1.

Det vil aldrig kunne finde sted, at linien, som repræsenterer NTP-koderne, vil lægge sig over linien, som repræsenterer RS-koden, da RS-koderne antager maksimum for Singleton grænsen, se Sætning 2.

Altså vil NTP-koderne for meget store alfabeter kunne rette stort set lige så mange fejl i forhold til længden af kodeordene, som RS-koderne kan. Derudover har NTP-koderne den fordel, at kodeordene er betydeligt længere end kodeordene i RS-koderne. Eksempelvis er længden af kodeordene i en NTP-kode over $\mathbb{F}_{q^m}$ lig q^{2m-1}, mens de for en RS-kode over samme legeme kun har længden q^m. Dette medfører, at NTP-koderne, i langt højere grad end RS-koderne, vil være i stand til at rette "byger" af fejl.

Kapitel 9

Afrunding

Vi har i dette speciale beskæftiget os med Reed-Solomon koder, og en generalisering af disse, kaldet NTP-koder.

Efter at have bestemt minimumsafstanden og dimensionen af Reed-Solomon koderne blev der opstillet en dekodningsalgoritme, som kan rette op til $\frac{d}{2}$ fejl.
Denne dekodningsalgoritme blev derefter forbedret ved hjælp af Sudans listedekodningsalgoritme således, at det er muligt at rette mere end $\frac{d}{2}$ fejl, forudsat, at hastigheden af koden opfylder, at

$$\frac{k}{n} < \frac{1}{2l-1} + \frac{1}{n}.$$

Da dette betyder, at der kun er sket forbedringer, med hensyn til hvor mange fejl det er muligt at rette, for meget små hastigheder for koden blev Guruswami-Sudans listedekodningsalgoritme introduceret.
Her så vi, at det for hastigheder for koden, som opfylder, at

$$\frac{k}{n} < \frac{s}{2l-s} + \frac{1}{n},$$

er muligt at rette mere end $\frac{d}{2}$ fejl.
Desuden er der sket en forbedring med hensyn til størrelsen af hastigheden, da det her er muligt at regulere på parameteren s.

Disse to listedekodningsalgoritmer benyttede sig begge af, at det er muligt at bestemme faktorer på formen $(y - f(x))$, hvor $\deg(f(x)) < k$, til interpolationspolynomiet $Q(x, y)$, hvilket der derpå blev gjort rede for i Kapitel 3.
Her blev problemet først reduceret til at bestemme lineære faktorer til polynomiet i én variabel $\varphi(Q(x, y))$. Dette blev gjort ved at finde

$$\gcd(y^{q^k} - y, \varphi(Q(x, y))).$$

Vi fandt frem til, at det for alle $(y - f(x))|Q(x, y)$ gælder, at $(y - [f(x)]_{\mathbf{E}})$ er en irreducibel faktor i $\varphi(Q(x, y))$.
Dermed kan de fundne rødder til $\varphi(Q(x, y))$, på formen $[f(x)]_{\mathbf{E}}$, indsættes i $Q(x, y)$ for at afgøre, om nogle af disse også er rødder her til. Hvis dette er tilfældet, har vi faktorer til $Q(x, y)$ på formen $(y - f(x))$, hvor $\deg(f(x)) < k$, idet $\deg([f(x)]_{\mathbf{E}}) < k$.

Den resterende del af specialet omhandlede NTP-koderne.
Kodeordene heri blev bestemt til at være polynomier, som er linearkombinationer af monomierne i fodaftrykket af $\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$, evalueret i de q^{2m-1} punkter tilhørende $\mathbf{V}(\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle)$.
Vi fandt frem til, at minimumsafstanden for en $NTP(s)$-kode altid er mindre end eller lig $n - s$. Specielt gælder der lighed, hvis funktionen

$$B(i, j) = \begin{cases} \lceil \frac{j}{q^{m-1}} \rceil & \textit{for} \quad i = 0 \\ 1 + \lceil \frac{i-1}{(q^m-1)/(q-1)} \rceil + \lceil \frac{j}{q^{m-1}} \rceil & \textit{for} \quad i \geq 1 \end{cases}$$

er mindre end eller lig q.
For at bestemme dimensionen af koden blev der introduceret teori om semigrupper, herunder genus og konduktor, og dimensionen blev bestemt til at være

$$k(NTP(s)) = s + 1 - g,$$

for $c(\Gamma) - 1 \leq s < q^{2m-1}$, hvor $c(\Gamma) = (\frac{q^m-1}{q-1} - 1)(q^{m-1} - 1)$ er konduktoren, og $g = \frac{c(\Gamma)}{2}$ er genus.
Dimensionen af NTP-koden blev derefter benyttet til bestemmelse af dualkoden til $NTP(s)$, hvilken er givet ved

$$NTP(n + c(\Gamma) - 2 - s),$$

hvor $c(\Gamma) - 1 \leq s < q^{2m-1}$.

Endelig blev der givet en dekodningsalgoritme for NTP-koden, som gjorde det muligt at rette op til $\frac{d-g}{2}$ fejl.

Til slut vurderede vi de to koder i forhold til hinanden udfra det synspunkt, at en kode er god, hvis hastigheden er høj samtidig med, at den relative minimumsafstand er stor. Vi fandt frem til, at for en given hastighed vil Reed-Solomon koderne kunne rette flere fejl i forhold til deres længde end NTP-koderne kan. Dog udlignes dette, hvis alfabetet vokser, og koderne vil dermed blive omtrent lige gode.

English Summary

During this report we have worked with Reed-Solomon codes and a generalization of these called NTP-codes.

After having determined the minimumdistance and the dimension of the Reed-Solomon codes, a decoding algorithm which is able to correct less than $\frac{d}{2}$ errors was presented.
The decoding algorithm was later improved by Sudans list decoding algorithm which is able to correct more than $\frac{d}{2}$ errors provided that the rate of the code satisfies

$$\frac{k}{n} < \frac{1}{2l-1} + \frac{1}{n}.$$

This implied that there were only made improvements for very low rates of the code. So we introduced the Guruswami-Sudan list decoding algorithm thus making it possible to correct more than $\frac{d}{2}$ errors for rates of the code which satisfies

$$\frac{k}{n} < \frac{s}{2l-s} + \frac{1}{n}.$$

In addition there had been an improvement of the rate owing to the fact that you could now adjust the s-parameter.
Both list decoding algorithms depended on the fact that you can identify linear factors of the interpolation polynomial $Q(x,y)$ of the form $(y - f(x))$ with $\deg(f(x)) < k$.
The problem was reduced to identifying linear factors of the polynomial in one variable $\varphi(Q(x,y))$ which is done by calculating

$$\gcd(y^{q^m} - y, \varphi(Q(x,y))).$$

For all factors $(y - f(x))$ of $Q(x, y)$ we saw that $(y - [f(x)]_{\mathbf{E}})$ was an irreducible factor of $\varphi(Q(x, y))$.
So the procedure to identify the roots of $Q(x, y)$ of degree less than k would be first to find the linear factors $(y-[f(x)]_{\mathbf{E}})$ of $\varphi(Q(x, y))$ and then, by substitution of these roots $[f(x)]_{\mathbf{E}}$ into $Q(x, y)$, to see which ones also are a root of $Q(x, y)$.

The remaining part of this report concerned NTP-codes. The codewords in this type of code were determined to be the polynomials which are linear combinations of the monomials in the footprint of the ideal $\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$ evaluated in the q^{2m-1} points from the variety $\mathbf{V}(\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle)$.
The minimum distance of an $NTP(s)$-code is always less than or equal to $n - s$. Especially the minimum distance is equal to $n - s$ if the function

$$B(i, j) = \begin{cases} \lceil \frac{j}{q^{m-1}} \rceil & for \quad i = 0 \\ 1 + \lceil \frac{i-1}{(q^m-1)/(q-1)} \rceil + \lceil \frac{j}{q^{m-1}} \rceil & for \quad i \geq 1 \end{cases}$$

is less than or equal to q.
To identify the dimension of the code we introduced some theory concerning numerical semigroups, genus and conductor and the dimension is

$$k(NTP(s)) = s + 1 - g,$$

for $c(\Gamma) - 1 \leq s < q^{2m-1}$, where $c(\Gamma) = (\frac{q^m-1}{q-1} - 1)(q^{m-1} - 1)$ is the conductor and $g = \frac{c(\Gamma)}{2}$ is genus.
The dimension of the NTP-code was used to identify the dualcode which is given by

$$NTP(n + c(\Gamma) - 2 - s),$$

where $c(\Gamma) - 1 \leq s < q^{2m-1}$.
Then a decoding algorithm for the NTP-codes was given which is able to correct less than $\frac{d-g}{2}$ errors.

Finally we compared the two codes to see which is the best. By best we mean which code has high rate and can correct many errors. We concluded that for a given rate the Reed-Solomon codes can correct more errors compared to their lenght than the NTP-codes. But if the alphabet grows then the NTP-codes will be nearly as good as the RS-codes.

Appendiks A

Dette appendiks knytter sig primært til Kapitel 5, og er opbygget med henblik på at vise, at $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$, $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$, $\alpha \in \mathbb{F}_{q^m}$, tilhører $\mathbb{F}_q$. Til dette formål skal der vises tre hovedresultater.

Hele Appendiks A bygger på udvalgte dele af [6].

Det første hovedresultat i Appendiks A er følgende:

Sætning 76 *Lad f være minimalpolynomiet af α over $\mathbb{F}_q$, hvor $\alpha \in \mathbb{F}_{q^m}$. Da vil* $\deg(f)|m$.

Det andet hovedresultat er:

Sætning 77 *Hvis f er et irreducibelt polynomium i $\mathbb{F}_q[x]$ med grad d, så har f en rod $\alpha \in \mathbb{F}_{q^d}$. Desuden er alle rødder i f simple, og givet ved de d forskellige elementer $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}} \in \mathbb{F}_{q^d}$.*

Endelig er det tredje hovedresultat i dette appendiks:

Sætning 78 *Lad $\alpha \in \mathbb{F}_{q^m}$ og lad $f \in \mathbb{F}_q[x]$ være minimalpolynomiet for α over $\mathbb{F}_q$. Da er de konjugerede af α med hensyn til $\mathbb{F}_q$, som er givet ved $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$, forskellige, hvis og kun hvis $deg(f) = m$.*
Hvis derimod $deg(f) = d < m$, så vil det gælde, at $d|m$, og de konjugerede af

α med hensyn til $\mathbb{F}_q$ er de forskellige elementer $\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}$, som hver er gentaget $\frac{m}{d}$ gange.

Disse tre sætninger vises udfra en række andre resultater, som vil blive introduceret i det efterfølgende.

A.1

I dette afsnit vil der blive vist to vigtige egenskaber ved endelige legemer, som ofte vil blive benyttet.

Lemma 79 *Hvis $\mathbb{F}_q$ er et endeligt legeme med q elementer så opfylder ethvert element $a \in \mathbb{F}_q$ ligningen $a^q = a$.*

Bevis: For $a = 0$ ses det umiddelbart, at $a^q = a$.
Lad α være et primitivt element i $\mathbb{F}_q$, hvilket vil sige, at $\alpha^{q-1} = 1$, og α^i for $i = 0, \ldots, q-2$ er alle de forskellige elementer i $\mathbb{F}_q^*$. Altså eksisterer der et $i \in \mathbb{N}_0$, sådan at $a = \alpha^i$.
Heraf fås, at

$$a^{q-1} = (\alpha^i)^{q-1} = (\alpha^{q-1})^i = 1.$$

Altså gælder det, at $a^q = a$ for alle $a \in \mathbb{F}_q$. □

Det ses udfra dette lemma, at elementerne i $\mathbb{F}_q$ netop er rødderne til polynomiet $x^q - x$. En udvidelse af dette betyder ligeledes, at rødderne til $x^{q^m} - x$ præcis er elementerne i $\mathbb{F}_{q^m}$.

Lemma 80 *Lad $\mathbb{F}_p$ være et endeligt legeme med p elementer, hvor p er et primtal, og lad $m \in \mathbb{N}$. Så er $(a+b)^{p^m} = a^{p^m} + b^{p^m}$.*

Bevis: Beviset føres ved induktion i m.
Basistrin: $m = 1$.
Udfra binomialformlen fås:

$$(a+b)^p = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1}b + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} ab^{p-1} + b^p. \qquad \text{(A.1)}$$

For $0 < i < p$ er binomialkoefficienten:

$$\begin{pmatrix} p \\ i \end{pmatrix} = \frac{p!}{(p-i)!\,i!} = \frac{p(p-1)\cdots(p-i+1)}{i!},$$

og idet p er et primtal vil dette ikke kunne forkortes væk i tælleren, hvorved $\begin{pmatrix} p \\ i \end{pmatrix} = 0 \mod p$, for $0 < i < p$. Hermed kan ligning (A.1) skrives som:

$$(a+b)^p = a^p + b^p,$$

i $\mathbb{F}_p$, da de resterende led forsvinder.
Induktionstrin:
Antag, at sætningen gælder for $m-1$, det vil sige, at $(a+b)^{p^{m-1}} = a^{p^{m-1}} + b^{p^{m-1}}$.
Det skal nu vises, at det også gælder for p^m.
Dette ses ved følgende udregning:

$$(a+b)^{p^m} = ((a+b)^p)^{p^{m-1}} = (a^p + b^p)^{p^m - 1} = (a^p)^{p^{m-1}} + (b^p)^{p^{m-1}} = a^{p^m} + b^{p^m},$$

og herved er sætningen bevist. □

A.2

I dette afsnit vil følgende hjælperesultat blive vist:

Lemma 81 *Lad $f \in \mathbb{F}_q[x]$ være et irreducibelt polynomium, hvor $\mathbb{F}_q$ er et endeligt legeme. Lad endvidere α være en rod i f tilhørende et udvidelseslegeme $\mathbb{F}_q(\alpha)$ af $\mathbb{F}_q$. Så gælder det for et polynomium $h \in \mathbb{F}_q[x]$, at $h(\alpha) = 0$ hvis og kun hvis f går op i h.*

Før beviset for dette lemma skal vi have introduceret nogle nyttige begreber. Der lægges ud med definitionen af et udvidelseslegeme.

Definition 82 (Udvidelseslegeme) *Lad* $\mathbf{K}$ *være et dellegeme af legemet* $\mathbf{F}$*, og* M *en hvilken som helst delmængde af* $\mathbf{F}$*. Så er udvidelseslegemet* $\mathbf{K}(M)$ *af* $\mathbf{K}$ *defineret som fællesmængden af alle dellegemer af* $\mathbf{F}$*, som alle indeholder både* $\mathbf{K}$ *og* M*.*

Det ses, at $\mathbf{K}(M)$ er det mindste legeme, som indeholder $\mathbf{K}$ og M, da det er en fællesmængde af legemer, der indeholder dem begge.
Der kan nu defineres en speciel form for udvidelseslegeme.

Definition 83 (Algebraisk udvidelse) *Lad* $\mathbf{K}$ *være et dellegeme af* $\mathbf{F}$ *og* $\alpha \in \mathbf{F}$*. Hvis* α *er rod i et polynomium* f*, forskellig fra nulpolynomiet, tilhørende* $\mathbf{K}[x]$*, da siges* α *at være algebraisk over* $\mathbf{K}$*. Et udvidelseslegeme* $\mathbf{L}$ *af* $\mathbf{K}$ *kaldes en algebraisk udvidelse af* $\mathbf{K}$ *hvis ethvert element i* $\mathbf{L}$ *er algebraisk over* $\mathbf{K}$*.*

Det vil sige, at alle elementer i $\mathbf{L}$ er rod i et eller andet polynomium i $\mathbf{K}[x]$. Hvis alle rødder til et polynomium f med koefficienter i $\mathbf{K}$ ligger i et udvidelseslegeme $\mathbf{E}$, og dette er det mindste legeme med denne egenskab, så kaldes $\mathbf{E}$ for spaltningslegemet for f. Dette defineres mere formelt som følgende.

Definition 84 (Spaltningslegeme) *Lad* $f \in \mathbf{K}[x]$ *være et polynomium med positiv grad, og* $\mathbf{E}$ *et udvidelseslegeme for* $\mathbf{K}$*. Da siges* f *at spalte i* $\mathbf{E}$*, hvis polynomiet kan skrives som produkt af lineære faktorer i* $\mathbf{E}[x]$*. Det vil sige der eksisterer elementer* $\alpha_1, \ldots, \alpha_n \in \mathbf{E}$ *sådan, at*

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n),$$

hvor a *er den ledende koefficient i* f*.*
Legemet $\mathbf{E}$ *kaldes spaltningslegemet for* f *over* $\mathbf{K}$*, hvis* $\mathbf{E}$ *er det mindst mulige udvidelseslegeme for* $\mathbf{K}$ *med ovenstående egenskab.*

Lad $\alpha \in \mathbf{F}$ være algebraisk over $\mathbf{K}$, og betragt idealet $I(\alpha) = \{f \in \mathbf{K}[x] : f(\alpha) = 0\} \subseteq \mathbf{K}[x]$. Dette ideal er ikke nul-idealet, idet α er algebraisk, og vi ved derved, at der eksisterer et polynomium i $\mathbf{K}[x]$, hvori α er rod. Da $\mathbf{K}[x]$ er et hovedidealområde, se [1, side 113], eksisterer der et entydigt monisk polynomium

$g \in \mathbf{K}[x]$, som genererer idealet $I(\alpha)$.
Det ses, at det genererende polynomium g er irreducibelt idet, hvis det antages, at det ikke er, så vil det kunne skrives som et produkt af irreducible polynomier. Det vil sige $g(x) = p(x)h(x)$, hvor $p, h \in \mathbf{K}[x]$ er irreducible. Altså er $g(\alpha) = p(\alpha)h(\alpha) = 0$, hvorved enten $p(\alpha) = 0$ eller $h(\alpha) = 0$. Antag, at $p(\alpha) = 0$, da er $p(x) = g(x)\frac{1}{h(x)}$, men $\frac{1}{h(x)} \notin \mathbf{K}[x]$ og g genererer derfor ikke p, som vi ved tilhører idealet, og vi har opnået en modstrid.
Det er nu muligt at definere minimalpolynomiet for et element i $\mathbf{F}$.

Definition 85 (Minimalpolynomium) *Hvis $\alpha \in \mathbf{F}$ er algebraisk over $\mathbf{K}$, så kaldes det entydige moniske polynomium g, som genererer idealet $I(\alpha) = \{f \in \mathbf{K}[x] : f(\alpha) = 0\} \subseteq \mathbf{K}[x]$, for minimalpolynomiet med hensyn til α over $\mathbf{K}$.*

Så minimal polynomiet for α er det moniske polynomium af mindst grad, som har α som rod. Af kommentaren før definitionen ses, at minimalpolynomiet er et irreducibelt polynomium.

Lemma 86 *Lad $\alpha \in \mathbf{F}$ være algebraisk over $\mathbf{K}$. Så har minimalpolynomiet $g \in \mathbf{K}[x]$ med hensyn til α følgende egenskab.*

For $f \in \mathbf{K}[x]$ er $f(\alpha) = 0$ hvis og kun hvis g går op i f.

Bevis: Hvis $f(\alpha) = 0$ vil det sige, at $f \in \langle g \rangle$ hvilket lige præcis betyder, at $f(x) = g(x)h(x)$, hvor $h(x) \in \mathbf{K}[x]$.
Omvendt hvis $f(x) = g(x)h(x)$, så er $f(\alpha) = 0$, da g er minimalpolynomiet for α. □

Heraf kan det ses, at er f et irreducibelt polynomium med α som rod, vil f højst afvige fra minimalpolynomiet med multiplikation med en skalar.
Dette skyldes, at minimalpolynomiet, g, med hensyn til α over $\mathbf{K}$, ifølge Lemma 86, går op i f, det vil sige $f = hg$, men da f jo netop var irreducibel, kan polynomiet h kun være en skalar.

Det er nu muligt at vise Lemma 81.

Bevis: Bevis for Lemma 81.
Lad a være den ledende koefficient i f, og lad $g(x) = a^{-1}f(x)$. Så er $g(x)$ et monisk irreducibelt polynomium i $\mathbb{F}_q[x]$, og $g(\alpha) = 0$. Derved ses det udfra Definition 85, at g er minimalpolynomiet for α over $\mathbb{F}_q$.
Hvis $h(\alpha) = 0$ medfører dette udfra Lemma 86, at $h(x) = g(x)p(x)$, hvor $p(x) \in \mathbb{F}_q[x]$. Det vil sige, at $h(x) = a^{-1}f(x)p(x)$, hvormed det ses, at $f(x)$ går op i $h(x)$.
Antag, at $f(x)$ går op i $h(x)$. Hermed går $g(x)$ også op i $h(x)$, og Lemma 86 benyttes endnu engang til at konkludere, at $h(\alpha) = 0$, hvilket fuldfører beviset. □

A.3

Gennem dette afsnit introduceres de sidste hjælperesultater til at bevise Appendiks A's tre hovedsætninger.
Følgende lemma benyttes direkte i beviset for Sætning 77.

Lemma 87 *Lad $f \in \mathbb{F}_q[x]$ være et irreducibelt polynomium over $\mathbb{F}_q$ af grad m. Så går $f(x)$ op i $x^{q^n} - x$ hvis og kun hvis m går op i n.*

For at bevise dette introduceres yderligere et par resultater.

Definition 88 *Lad $\mathbf{L}$ være et udvidelseslegeme for $\mathbf{K}$. Hvis $\mathbf{L}$ betragtes som et endeligt dimensionalt vektorrum over $\mathbf{K}$, så kaldes $\mathbf{L}$ en endelig udvidelse af $\mathbf{K}$. Desuden kaldes dimensionen af vektorrummet $\mathbf{L}$ over $\mathbf{K}$ for graden af $\mathbf{L}$ over $\mathbf{K}$, og skrives som $[\mathbf{L} : \mathbf{K}]$.*

Der gælder følgende sammenhæng mellem graderne på endelige udvidelser.

Lemma 89 *Hvis $\mathbf{L}$ er en endelig udvidelse af $\mathbf{K}$, og $\mathbf{M}$ er en endelig udvidelse af $\mathbf{L}$, så er $\mathbf{M}$ en endelig udvidelse af $\mathbf{K}$, hvorom det gælder, at*

$$[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}].$$

Bevis: Antag, at $[\mathbf{M} : \mathbf{L}] = m$ og $[\mathbf{L} : \mathbf{K}] = n$, og lad desuden $\{\alpha_1, \ldots, \alpha_m\}$ være en basis for $\mathbf{M}$ over $\mathbf{L}$, og $\{\beta_1, \ldots, \beta_n\}$ en basis for $\mathbf{L}$ over $\mathbf{K}$.
Dermed kan ethvert $\alpha \in \mathbf{M}$ skrives som en linearkombination

$$\alpha = \gamma_1\alpha_1 + \cdots + \gamma_m\alpha_m,$$

hvor $\gamma_i \in \mathbf{L}$ for $1 \leq i \leq m$. Dernæst kan hvert af disse $\gamma_i \in \mathbf{L}$ skrives som en linearkombination af basis elementerne β_j med koefficienter $r_{ij} \in \mathbf{K}$.
Hermed får vi

$$\alpha = \sum_{i=1}^{m} \gamma_i\alpha_i = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} r_{ij}\beta_j \right) \alpha_i = \sum_{i=1}^{m}\sum_{j=1}^{n} r_{ij}\beta_j\alpha_i.$$

Dette viser, at alle $\alpha \in \mathbf{M}$ kan skrives som en linearkombination af elementerne $\beta_j\alpha_i$, hvor $1 \leq i \leq m, 1 \leq j \leq n$, hvormed disse kan betragtes som en basis for $\mathbf{M}$. Hvis det kan vises, at de mn elementer $\beta_j\alpha_i$ er lineært uafhængige over $\mathbf{K}$, så er graden af $\mathbf{M}$ over $\mathbf{K}$, $[\mathbf{M} : \mathbf{K}]$, netop lig $[\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}]$.
Vi antager derfor, at

$$\sum_{i=1}^{m}\sum_{j=1}^{n} s_{ij}\beta_j\alpha_i = 0,$$

hvor koefficienterne $s_{ij} \in \mathbf{K}$. Dermed har vi, at

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} s_{ij}\beta_j \right) \alpha_i = 0.$$

Da α_i'erne er lineært uafhængige over $\mathbf{L}$, så gælder det, at

$$\sum_{j=1}^{n} s_{ij}\beta_j = 0, \text{ for } 1 \leq i \leq m.$$

Men idet β_j'erne er lineært uafhængige over $\mathbf{K}$. så er $s_{ij} = 0$ for $1 \leq i \leq m, 1 \leq j \leq n$. Altså er $\beta_j\alpha_i$'erne lineært uafhængige. hvormed

$$[\mathbf{M} : \mathbf{K}] = mn = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}].$$

□

Yderligere gælder der følgende, som vedrører graden af en specifik endelig udvidelse.

Lemma 90 *Lad $\alpha \in \mathbf{F}$ være algebraisk over $\mathbf{K}$, og lad g være minimalpolynomiet af α over $\mathbf{K}$, hvor $deg(g) = n$. Da gælder følgende to punkter:*

(*i*) *Udvidelseslegemet for $\mathbf{K}$ med hensyn til α, $\mathbf{K}(\alpha)$, er isomorf til legemet $\mathbf{K}[x]/\langle g(x)\rangle$.*

(*ii*) *$[\mathbf{K}(\alpha) : \mathbf{K}] = n$ og mængden $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ er basis for $\mathbf{K}(\alpha)$ over $\mathbf{K}$.*

Bevis: (*i*): Betragt afbildningen $\varphi\colon \mathbf{K}[x] \to \mathbf{K}(\alpha)$ givet ved $\varphi(f) = f(\alpha)$ for $f \in \mathbf{K}[x]$. Dette vil være en ring homomorfi, da det blot bliver polynomielle opskrivninger af α ganget eller lagt sammen. Kernen af φ er givet ved $\ker\varphi = \{f \in \mathbf{K}[x] : f(\alpha) = 0\} = \langle g(x)\rangle$.

Lad S være billedet af φ. Dermed er S en mængde af polynomier udtrykt ved α med koefficienter i $\mathbf{K}$, hvilket kan vises at være en ring. Hermed kan homomorfisætningen for ringe, [6, Theorem 1.40, side 14], benyttes til at konkludere, at S er isomorf til legemet $\mathbf{K}[x]/\langle g(x)\rangle$. Dermed er S også et legeme, og det kan af definitionen af S ses, at $S \subseteq \mathbf{K}(\alpha)$, og at $\alpha \in S$, og pr. definitionen af $\mathbf{K}(\alpha)$ er dette det mindste legeme, som indeholder både $\mathbf{K}$ og α, og det kan hermed konkluderes, at $S = \mathbf{K}(\alpha)$, hvorved punkt (*i*) er bevist.

(*ii*): Da det i forrige punkt blev vist, at $S = \mathbf{K}(\alpha)$, betyder dette, at alle $\beta \in \mathbf{K}(\alpha)$ kan skrives som $f(\alpha)$, for et eller andet $f \in \mathbf{K}[x]$. Ethvert $f \in \mathbf{K}[x]$ kan udfra divisionsalgoritmen skrives som $f = qg + r$, hvor $q, r \in \mathbf{K}[x]$ og $deg(r) < deg(g) = n$.
Hermed er $\beta = f(\alpha) = q(\alpha)g(\alpha) + r(\alpha) = r(\alpha)$. Altså kan ethvert $\beta \in \mathbf{K}(\alpha)$ skrives som en linear kombination af monomierne $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.
Disse monomier vil da udspænde den endelige udvidelse af $\mathbf{K}(\alpha)$ over $\mathbf{K}$. For at undersøge om de desuden er lineært uafhængige, og dermed en basis, betragtes polynomiet $h(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \in \mathbf{K}[x]$.
Antag, at $h(\alpha) = 0$, da giver Lemma 86, at g går op i h. Men da $deg(h) < n = deg(g)$ er dette kun muligt, hvis $h = 0$. Dette betyder, at en linear kombination af monomierne $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ kun giver nul, hvis alle koefficienterne er nul, og altså er de linært uafhængige, hvormed også punkt (*ii*) er vist. □

I beviset for Lemma 87 anvendes endnu en sætning, som dog ikke bevises her, men beviset kan findes i [6, Theorem 2.6, side 46].

Lemma 91 (Kriterie for dellegemer) *Lad $\mathbb{F}_q$ være det endelige legeme med $q = p^n$ elementer, hvor p er et primelement.*
Da har ethvert dellegeme af $\mathbb{F}_q$ orden p^m, hvor m er en positiv divisor for n.
Gælder det modsat, at m er en positiv divisor for n, så eksisterer der præcis et dellegeme af $\mathbb{F}_q$ med p^m elementer.

Det er nu muligt at vise Lemma 87.

Bevis: Bevis for Lemma 87.

Det antages først, at $f(x)|x^{q^n} - x$. Det vil sige, at $x^{q^n} - x = h(x)f(x)$, $h(x) \in \mathbb{F}_q[x]$. Lad α være rod i f i spaltningslegemet for f over $\mathbb{F}_q$, så er $\alpha^{q^n} = \alpha$, hvormed $\alpha \in \mathbb{F}_{q^n}$, ifølge Lemma 79.
Heraf følger det, da udvidelseslegemet for $\mathbb{F}_q$ med hensyn til α, $\mathbb{F}_q(\alpha)$, er det mindste udvidelseslegeme, som indeholder $\mathbb{F}_q$ og α, at $\mathbb{F}_q(\alpha)$ er en delmængde af $\mathbb{F}_{q^n}$.
Af Lemma 89 følger det så, at

$$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q].$$

Idet ethvert polynomium med koefficienter i et legeme kan gøres monisk, så antages det, at det irreducible polynomium f er et minimalpolynomium. Dermed kan vi benytte Lemma 90 punkt (ii) til at fastslå, at $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Desuden er $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, og af Lemma 89 følger det da, at $m|n$.

Antag modsat, at $m|n$, så følger det af Lemma 91, at $\mathbb{F}_{q^m}$ er et dellegeme af $\mathbb{F}_{q^n}$. Hvis α er en rod i f i spaltningslegemet for f over $\mathbb{F}_q$, så er $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ ifølge Lemma 90 punkt (ii). Hermed gælder det, at $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$.
Det vil sige, at $\alpha \in \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$, og dermed er $\alpha^{q^n} = \alpha$, hvorved α er rod i polynomiet $x^{q^n} - x \in \mathbb{F}_q[x]$. Der gælder da ifølge Lemma 81, at $f(x)$ går op i $x^{q^n} - x$. □

A.4

Det er nu muligt ved hjælp af de foregående hjælperesultater, at vise de tre hovedresultater i dette appendiks.

Det første hovedresultat lød som følger:

Sætning 76 *Lad $f \in \mathbb{F}_q[x]$ være minimalpolynomiet af α over $\mathbb{F}_q$, hvor $\alpha \in \mathbb{F}_{q^m}$. Da vil* $\deg(f)|m$.

Bevis: Betragt polynomiet $x^{q^m} - x$, som er det polynomium, der har alle elementer i $\mathbb{F}_{q^m}$ som rødder. Det vil sige det har specielt α som rod.
Da gælder det ifølge Lemma 86, da f er minimalpolynomiet med hensyn til α, at

$$f(x)|(x^{q^m} - x).$$

Idet f er minimal polynomiet er det også et irreducibelt polynomium, og det er nu muligt at benytte Lemma 87 til at konkludere, at

$$\deg(f)|m.$$

□

Herefter kan det andet hovedresultat bevises, hvilket lød således:

Sætning 77 *Hvis f er et irreducibelt polynomium i $\mathbb{F}_q[x]$ med grad d, så har f en rod $\alpha \in \mathbb{F}_{q^d}$. Desuden er alle rødder i f simple, og givet ved de d forskellige elementer $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}} \in {\mathbb{F}_q}^d$.*

Bevis: Lad α være en rod i f i spaltningslegemet for f over $\mathbb{F}_q$. Hermed har vi fra Lemma 90 (ii), at $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$, og dermed er $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^d}$, hvorved $\alpha \in \mathbb{F}_{q^d}$.

Det skal nu vises, at hvis $\beta \in \mathbb{F}_{q^d}$ er en rod i f, så er β^q også en rod i f.
Lad

$$f(x) = a_d x^d + \cdots + a_1 x + a_0, \qquad \text{hvor } a_i \in \mathbb{F}_q, 0 \leq i \leq d.$$

Ved nu at benytte Lemma 79 og Lemma 80 fås:

$$\begin{aligned} f(\beta^q) &= a_d\beta^{qd} + \cdots + a_1\beta^q + a_0 = a_d^q\beta^{qd} + \cdots + a_1^q\beta^q + a_0^q \\ &= (a_d\beta^d + \cdots + a_1\beta + a_0)^q = f(\beta)^q = 0. \end{aligned}$$

Derfor gælder det, da α er en rod i f, at også $\alpha^q, \ldots, \alpha^{q^{d-1}}$ er rødder i f.

Det skal nu bare vises, at disse elementer er forskellige.
Antag det modsatte, eksempelvis at $\alpha^{q^i} = \alpha^{q^k}$ for $0 \leq i < k \leq d-1$. Ved at opløfte denne lighed til q^{d-k} fås:

$$\alpha^{q^{i+d-k}} = \alpha^{q^d} = \alpha.$$

Det følger nu af Lemma 81, at $f(x)|(x^{q^{i+d-k}} - x)$, og af Lemma 87 er dette kun muligt, hvis $d|(i+d-k)$. Men da $0 \leq i+d-k < d$, har vi opnået en modstrid, og dermed er $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ forskellige. □

Endelig kan det tredje og sidste hovedresultat i Appendiks A bevises.

Sætning 78 *Lad $\alpha \in \mathbb{F}_{q^m}$, og lad $f \in \mathbb{F}_q[x]$ være minimalpolynomiet for α. Da er de konjugerede af α med hensyn til $\mathbb{F}_q$, som er givet ved $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$, forskellige, hvis og kun hvis $deg(f) = m$.*
Hvis derimod $deg(f) = d < m$, så vil det gælde, at $d|m$, og de konjugerede af α med hensyn til $\mathbb{F}_q$ er de forskellige elementer $\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}$, som hver er gentaget $\frac{m}{d}$ gange.

Bevis: Antag først, at $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ alle er forskellige. Graden af f vil som en konsekvens af Sætning 76 være mindre end eller lig m.
Lad $deg(f) = s$ og antag, at $s < m$. Sætning 77 giver, at $\alpha, \alpha^q, \ldots, \alpha^{q^{s-1}}$ alle er forskellige og rødder i $f(x)$.
Lad nu β være en af disse rødder. Det vil sige, at $f(\beta) = 0$. Dermed er også $(f(\beta))^q = 0$.
Da $f = \sum_{i=1}^{s} c_i x^i \in \mathbb{F}_q[x]$, vil dette, ifølge Lemma 79 og Lemma 80, medføre, at

$$0 = (f(\beta))^q = \sum_{i=1}^{s} (c_i\beta^i)^q = \sum_{i=1}^{s} c_i(\beta^q)^i = f(\beta^q).$$

Dette betyder, at β^q også er rod i $f(x)$. Hvis $\beta = \alpha^{q^{s-1}}$, så betyder dette, at $\beta^q = (\alpha^{q^{s-1}})^q = \alpha^{q^s}$ også er en rod i $f(x)$ og udfra begyndelsesbetingelsen

om, at $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ alle er forskellige, må denne nye rod være forskellig fra de øvrige s rødder, og dermed er der flere rødder end graden af f, og da f var antaget at være forskellig fra nulpolynomiet, er der opnået en modstrid, så hermed kan det konkluderes, at $deg(f) = s = m$.

Dernæst antages, at $deg(f) = m$. Minimalpolynomiet er som tidligere nævnt et irreducibelt polynomium, hvormed Sætning 77 kan benyttes til at konkludere, at $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ er forskellige.

Hvis derimod $deg(f) = d < m$, giver Sætning 76, at $d|m$, og igen kan Sætning 77 benyttes til at se, at $\alpha, \alpha^q, \ldots \alpha^{q^{d-1}} \in \mathbb{F}_{q^d}$ er forskellige. Da $\alpha \in \mathbb{F}_{q^d}$, er $\alpha^{q^d} = \alpha$. Dermed er følgende opfyldt:

$$\begin{array}{ccccccccc}
\alpha & = & \alpha^{q^d} & = & \alpha^{q^{2d}} & = & \cdots & = & \alpha^{q^{jd}} \\
\alpha^q & = & \alpha^{q^{d+1}} & = & \alpha^{q^{2d+1}} & = & \cdots & = & \alpha^{q^{jd+1}} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots \\
\alpha^{q^{d-1}} & = & \alpha^{q^{d+(d-1)}} & = & \alpha^{q^{2d+(d-1)}} & = & \cdots & = & \alpha^{q^{jd+(d-1)}}
\end{array}$$

Da $d|m$ er $m = rd$, så ses det af ovenstående, hvis $r - 1 = j$, at

$$\alpha^{q^{(r-1)d+(d-1)}} = \alpha^{q^{rd-1}} = \alpha^{q^{m-1}}.$$

Altså er elementerne, listet ovenfor, de resterende af de konjugerede af α med hensyn til $\mathbb{F}_q$, $\alpha^{q^d}, \alpha^{q^{d+1}}, \ldots, \alpha^{q^{m-1}}$.
Hermed vil de d forskellige $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$ blive gentaget $\frac{m}{d}$ gange blandt de m konjugerede af α med hensyn til $\mathbb{F}_q$. □

Appendiks B

Dette appendiks har til formål at vise en sætning, som skal benyttes både i Kapitel 3 og i Kapitel 5.

B.1

Det ønskes i dette afsnit vist, at hvis φ er en homomorfi mellem to grupper $(G, \circ)$ og $(\varphi(G), *)$, så er ækvivalensklasserne i G alle af samme størrelse.
Først vises følgende resultat:

Sætning 92 *Lad $(G, \circ)$ være en gruppe med neutralelement e, og R være en mængde hvorpå operationen $*$ er defineret. Hvis φ er en homomorfi fra G til R, så er $(\varphi(G), *)$ en gruppe.*

Bevis: Idet $\varphi(G) \subseteq R$, er operationen $*$ defineret på mængden $\varphi(G)$.
Det skal nu vises, at $\varphi(G)$ opfylder følgende tre betingelser:

(i) For alle $\varphi(a), \varphi(b), \varphi(c) \in \varphi(G)$ gælder det, at:

$$(\varphi(a) * \varphi(b)) * \varphi(c) = \varphi(a) * (\varphi(b) * \varphi(c)).$$

(ii) Der eksisterer et element $\varphi(e) \in \varphi(G)$, sådan at for alle $\varphi(a) \in \varphi(G)$ er

$$\varphi(a) * \varphi(e) = \varphi(e) * \varphi(a) = \varphi(a).$$

(iii) For ethvert element $\varphi(a) \in \varphi(G)$ findes et $\varphi(a') \in \varphi(G)$ sådan, at

$$\varphi(a) * \varphi(a') = \varphi(a') * \varphi(a) = \varphi(e).$$

For at bevise ovenstående tre punkter benyttes, at $\varphi(a \circ b) = \varphi(a) * \varphi(b)$ for alle $a, b \in G$, hvilket skyldes, at φ er en homomorfi.
Bevis for de tre punkter:
(i) : Lad $a, b, c \in G$, da er:

$$\begin{array}{rcccc} (\varphi(a) * \varphi(b)) * \varphi(c) & = & \varphi(a \circ b) * \varphi(c) & = & \varphi((a \circ b) \circ c) \\ & = & \varphi(a \circ (b \circ c)) & = & \varphi(a) * \varphi(b \circ c) \\ & = & \varphi(a) * (\varphi(b) * \varphi(c)). & & \end{array}$$

(ii) : Lad $a \in G$, da er

$$\begin{array}{rcccc} \varphi(a) & = & \varphi(a \circ e) & = & \varphi(a) * \varphi(e) \\ \varphi(a) & = & \varphi(e \circ a) & = & \varphi(e) * \varphi(a). \end{array}$$

Altså er $\varphi(e)$ neutralelement i $\varphi(G)$.
(iii) : Lad $a, a', e \in G$ sådan, at $a \circ a' = e$, da er

$$\varphi(e) = \varphi(a \circ a') = \varphi(a) * \varphi(a') = \varphi(a') * \varphi(a).$$

Dermed er $\varphi(a')$ det inverse element til $\varphi(a)$, og da a var vilkårligt valgt, så har samtlige elementer i $\varphi(G)$ en invers.
Hermed er de tre punkter bevist, og altså er $(\varphi(G), *)$ en gruppe. □

Lad kernen af φ have størrelsen m, det vil sige, at:

$$\#\ker(\varphi) = \#\{a \in G : \varphi(a) = \varphi(e)\} = m.$$

Hvis $t \in \varphi(G)$ og $\varphi^{-1}(t) = \{b \in G : \varphi(b) = t\}$, skal det vises, at $\#\varphi^{-1}(t) = m$, altså at alle ækvivalensklasser i G er af samme størrelse.

Sætning 93 *Lad $\varphi\colon G \to R$ være en homomorfi fra gruppen $(G, \circ)$ med neutralelement e til mængden R, hvorpå operationen $*$ er defineret.*
Lad desuden $\#\ker(\varphi) = m$. Så er $\#\varphi^{-1}(t) = m$, hvor $t \in \varphi(G)$ og $\varphi^{-1}(t) = \{b \in G : \varphi(b) = t\}$.

Bevis: Udfra Sætning 92 er $(\varphi(G), *)$ en gruppe med neutralelement $\varphi(e)$.
Først vises det, at $\#\varphi^{-1}(t) \geq m$.

Lad $b \in \varphi^{-1}(t) \subseteq G$ og $a \in \ker(\varphi)$. Dermed gælder det, at

$$\varphi(a \circ b) = \varphi(a) * \varphi(b) = \varphi(e) * \varphi(b) = \varphi(b) = t,$$

for alle $a \in \ker(\varphi)$. Altså er mængden af punkter i G, som afbilledes over i t større end eller lig antallet af elementer i kernen.

Herefter vises det, at $\#\varphi^{-1}(t) \leq m$. Dette vises ved hjælp af en modstrid. Så antag, at der eksisterer et $t \in \varphi(G)$ sådan, at $\#\varphi^{-1}(t) > m$.
Idet $(\varphi(G), *)$ er en gruppe findes der et $\overline{t} \in \varphi(G)$ således, at $t * \overline{t} = \varphi(e)$. Lad $c \in \varphi^{-1}(\overline{t})$, så har vi for alle $b \in \varphi^{-1}(t)$, at:

$$\varphi(b \circ c) = \varphi(b) * \varphi(c) = t * (\overline{t}) = \varphi(e).$$

Det vil sige, at $b \circ c \in \ker(\varphi)$, og da dette gælder for alle $b \in \varphi^{-1}(t)$ er der opnået en modstrid med, at $\#\ker(\varphi)$ kun er lig m. Altså er $\#\varphi^{-1}(t) \leq m$, og dermed er sætningen bevist. □

Idet et vektorrum opfylder de samme betingelser, som er opfyldt for en additiv gruppe, så kan Sætning 93 også benyttes for vektorrum. Det vil sige, hvis $\varphi\colon \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ er en vektorrumshomomorfi, hvor $\mathbb{F}_{q^m}$ og $\mathbb{F}_q$ begge er endelige legemer set som vektorrum over $\mathbb{F}_q$, så har ækvivalensklasserne i $\mathbb{F}_{q^m}$ samme størrelse.

B. _____

Litteratur

[1] R.B.J.T. Allenby *"Rings, fields and groups"*, Butterworth-Heinemann, 2001.

[2] David Cox, John Little, Donal O'Shea *"Ideals, Varieties, and Algorithms"*, Springer-Verlag, 1997.

[3] Joachim von zur Gathen, Jürgen Gerhard *"Modern Computer Algebra -Second Edition"*, Cambridge University Press, 2003.

[4] Olav Geil *"On codes from norm-trace curves"*, Finite Fields and Their Applications, 2003, 351-371.

[5] Tom Høholdt, Jørn Justesen *"A course in error-correcting codes"*, European Mathematical Society, 2004.

[6] Rudolf Lidl, Harald Niederreiter *"Introduction to finite fields and their applications"*, Cambridge University Press, 1986.

[7] R. Refslund Nielsen, Tom Høholdt *"List decoding og linear block codes"* Phd. afhandling DTU, 2001.

[8] Tom Høholdt, Olav Geil *"Footprints or generalized Bezout's theorem"*, IEEE Transactions on information theory, Vol.46, No. 2, March 2000.

[9] Tom Høholdt, Jacobus H. van Lint, Ruud Pellikaan, *"Algebraic Geometry Codes* Kap. 10 i *"Handbook of Coding Theory"* Volume I af V.S. Pless, W.C. Huffman, NH Elsevier Science B.V., 1998.

Retteark

B.1.1 Kapitel 2 Reed-Solomon koder

Side 7_{10-11}:	Erstat x_i med x og r_i med r.
Side 9_{2-4}:	Erstat *Det skal desuden sikres, at* $\deg(Q_j(x))$ *er større end eller lig nul, da* (2.1) *i modsat fald ikke ville tælle antallet af koefficienter i* $Q(x,y)$.
ă	*Da* $\deg(Q_l(x))$ *er mindre end eller lig* $\deg(Q_j(x))$
ă	*for* $j = 1, \ldots, l-1$ *er det nok, at...* med
ă	*Det skal desuden sikres, at samtlige parenteser i* (2.1)
ă	ă*er større end eller lig nul, da* (2.1) *i modsat fald*ă *ikke ville tælle antallet af koefficienter.*ă
ă	*Idet* $(n-\tau) - l(k-1) \leq (n-\tau) - j(k-1)$ *for* $j = 0, \ldots, l$, *er det nok at sikre, at...*
Side 10_8:	Erstat $\tau > \frac{d}{2}$ med $\tau \geq \frac{d}{2}$.
Side 11_1:	Erstat $\frac{k}{n} < \frac{1}{3} + \frac{1}{n}$ med $\frac{k}{n} \leq \frac{1}{3} + \frac{1}{n}$.
Side $13_{1,4}$:	Erstat $\frac{k}{n} < \frac{1}{2l-1} + \frac{1}{n}$ med $\frac{k}{n} \leq \frac{1}{2l-1} + \frac{1}{n}$.
Side 15^{7-8}:	$\deg(Q_j(x))$ *er større end eller lig nul, eller at* slettes.
Side 16^7:	Erstat *så har* $Q(x, f(x))$ $n-\tau$ *s-dobbelte rødder* med *så har* $Q(x, f(x))$ *mindst* $n-\tau$ *s-dobbelte rødder*
Side 16_5 og Side 17^6:	Erstat $q_{k,j} \neq 0$, hvis $j \leq l$ og $k \leq s(n-\tau) - 1 - j(k-1)$ med $q_{k,j} = 0$, hvis $j > l$ og $k > s(n-\tau) - 1 - j(k-1)$, og $q_{k,j} \neq 0$, for nogle $j \leq l$ og $k \leq s(n-\tau) - 1 - j(k-1)$.
Side 18_9:	Erstat $\frac{k}{n} < \frac{s}{l+1} + \frac{1}{n}$ med $\frac{k}{n} \leq \frac{s}{l+1} + \frac{1}{n}$.
Side 18_3 og Side 17^2:	Erstat $\frac{k}{n} < \frac{s}{2l-s} + \frac{1}{n}$ med $\frac{k}{n} \leq \frac{s}{2l-s} + \frac{1}{n}$.

B.1.2 Kapitel 3 Bestemmelse af førstegradsfaktorer i $Q(x,y)$

Side 27^{13}:	Erstat *ringhomomorfien* med *ringisomorfien.*
Side 32_{11}:	Erstat $\deg(a) < k$ med $\deg(a) < n$.

B.1.3 Kapitel 5 Koder udtrykt ved hjælp af norm-trace polynomier

Side 58_6: Erstat $\mathbb{F}_q$ med $\mathbb{F}_q^*$.
Side 63_{10}: Erstat *af polynomierne tilhørende...* med *på....*
Side 64_{10}: Erstat k med $\mathbf{K}$.

B.1.4 Kapitel 6 Egenskaber ved NTP-koder

Side 87 ligning (6.3): Erstat β_k med β.

B.1.5 Kapitel 7 Dekodning af NTP-koder

Side 92^8: Erstat $\lambda_i \in \mathbb{F}_q$ med $\lambda_i \in \mathbb{F}_{q^m}$.
Side 93_8: Erstat $\mathtt{LT}(NT(x,y)) = y^{q^{m-1}}$ med $\mathtt{LT}(NT(x,y)) = -y^{q^{m-1}}$.

B.1.6 Appendiks A

Side 114_9: Erstat *den endelige udvidelse af...* med *den endelige udvidelse....*
Side 115_9: Erstat *...antages det, at det irreducible polynomium f er et minimalpolynomium.* med *...vil minimalpolynomietă med hensyn til α over $\mathbb{F}_q$ have grad n, da f er irreducibel.*

B.1.7 Appendiks B

Side 121^9: Erstat $(\overline{t})$ med $\overline{t}$.