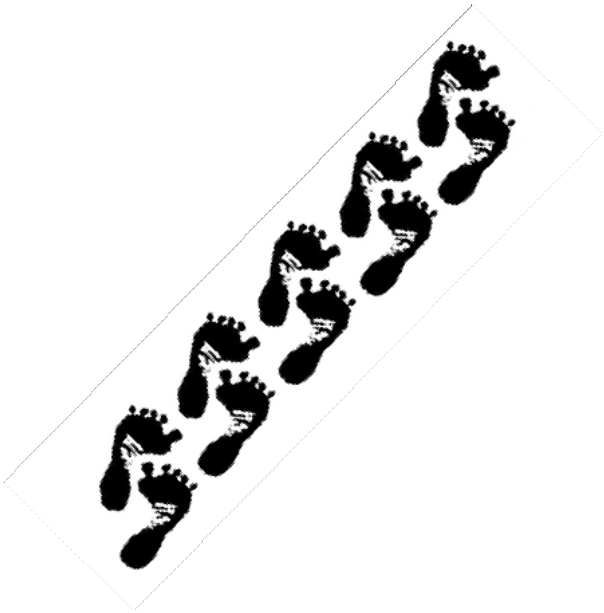
NTP-koder

- deres egenskaber og dekodning

af

Elisabeth Kuhr Rasmussen

Marts 2005



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

Institut for Matematiske Fag
Aalborg Universitet

Titel:
NTP-koder
-deres egenskaber og dekodning

Projekt:
Mat 6/ Speciale

Forfatter:
Elisabeth Kuhr Rasmussen

Vejledere:
Hans Olav Geil
Christian Thommesen

Antal eksemplarer: 7

Antal sider: 147

Synopsis:
I dette speciale betragtes en generalisering af Reed-Solomon koder, som i denne rapport benævnes NTP-koder.
Før definitionen af NTP-koder introduceres, gennemgåes teori, som gør dette muligt. Herunder teori om Gröbner baser og fodaftryk af idealer.
Efter definitionen af NTP-koderne bestemmes minimumsafstanden herfor udfra egenskaber vedrørende fodaftrykket af et ideal, og teori om semigrupper anvendes til at afgøre, hvad dimensionen og dualkoden er for NTP-koderne.
Resten af rapporten omhandler dekodning af NTP-koder. Først præsenteres en grundalgoritme, som kan rette op til $\frac{d-g}{2}$ fejl. Efterfølgende erstattes dele af denne grundalgoritme med en basisalgoritme, som i første omgang ikke er en bedre algoritme, da den kun kan rette $\frac{n-s-g-1}{2}$ fejl ($n - s \leq d$). En forbedring med et majoritetsprincip bringer dog antallet af fejl, som kan rettes, op på $\frac{n-s-1}{2}$. Tilsidst præsenteres en algoritme, som ikke kan rette flere fejl, men den bliver mere effektiv, da kompleksiteten nedsættes.

Forord

Denne rapport er udarbejdet som et speciale fra slutningen af januar 2004 til slutningen af marts 2005, ved det Teknisk-Naturvidenskabelige Fakultet, Institut for Matematiske Fag på Aalborg Universitet.

Der gøres opmærksom på, at den del af specialet, som omhandler definition, egenskaber og den første dekodningsalgoritme af NTP-koder, samt Appendiks A og Appendiks B er udarbejdet i samarbejde med Maria Sondrup Iversen og Jane Gravgård Knudsen, før jeg tog barselsorlov.
Desuden er kapitlet om Gröbner baser udarbejdet på MAT-5 fra først i september til midt i december 2003, ligeledes i samarbejde med Maria Sondrup Iversen og Jane Gravgård Knudsen.

Kildehenvisninger vil gennem rapporten blive angivet således: [kilde, henvisning], hvor kilden er anført i Litteraturlisten, se side 139. Henvisningen kan være til et kapitel, et afsnit eller en hel specifik sætning eller lignende.
I rapporten 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, marts 2005.

Elisabeth Kuhr Rasmussen

Indhold

Kapitel 1

Indledning

Det overordnede emne i dette speciale er diskret matematik, og det mere specifikke emne er kodningsteori.
Herindenfor har jeg valgt at beskæftige mig med en generalisering af Reed-Solomon koder, som jeg i denne rapport kalder for NTP-koder, da de er udtrykt ved det såkaldte norm - trace polynomium.

Ved definitionen af NTP-koderne skal der, ligesom for Reed-Solomon koderne, bestemmes punkter og polynomier, således at man 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 linear kombination af monomierne i fodaftrykket af idealet $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$, hvor $\prec_w$ er den monomielle ordning.
For at bestemme fodaftrykket skal der først kunne bestemmes en Gröbner basis for idealet, og Kapitel 2 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 vender jeg mig mod dekodningen af disse NTP-koder. Den første dekodningsalgoritme bruger ideen fra dekodning af Reed-Solomon koder, hvor det ønskes at bestemme et interpolationspolynomium, da dette kan bestemme fejlpositionerne i det modtagne ord. Herefter kan syndromer benyttes til at finde fejlværdierne. Denne dekodningsalgoritme kan rette op til $\frac{d-g}{2}$ fejl, hvor d betegner kodens minimumsafstand og g er genus.

I de efterfølgende algoritmer søges fejlpositionerne bestemt på en anden måde, hvorefter fejlværdierne bestemmes ved hjælp af syndromerne med samme princip som i den første dekodningsalgoritme. Målet er at få bestemt et fejllokaliserende polynomium, som er et polynomium, som har den egenskab at blandt dets nulpunkter findes fejlpositionerne. Basisalgoritmen benytter de såkaldte dobbeltsyndromer til dette, hvorved den kan rette op til $\frac{n-s-g-1}{2}$ fejl, hvor n er kodens længde, g er genus og s er kodens indeks, det vil sige koden, som betragtes, er $NTP(s)$. Den efterfølgende algoritme kan ved majoritetsbestemmelse af ukendte syndromer forbedre denne procedure, så der nu kan rettes op til $\frac{n-s-1}{2}$ fejl.

Den sidste algoritme, som jeg beskriver, bygger på de to foregående algoritmer, så her kan igen rettes op til $\frac{n-s-1}{2}$ fejl, men dette er en mere effektiv algortime, da kompleksiteten her bliver nedsat.

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

Kapitel 2

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 [3, Kapitel 2].

2.1 Dicksons lemma

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

Definition 2.1.1 (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 2.1.2 *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 2.1.3 *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 2.1.4 (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 2.1.2, 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 2.1.2, 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.

2.2 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 2.2.1 (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 2.2.2 *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 2.2.3 *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 2.2.4 *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 2.2.5 *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 2.2.6 (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 2.2.5 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 2.1.2 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 2.2.7 (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 2.2.5 (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 2.2.8 (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.

□

2.3 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 2.3.1 *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 2.1.2, 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 2.3.2 *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 2.3.1, 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 2.3.3 (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 2.3.4 *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

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i &= \sum_{i=1}^{s} c_i d_i p_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + \\ &\quad (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s. \quad (2.1)\end{aligned}$$

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

$$S(f_j, f_k) = \frac{x^{\delta}}{\mathtt{LT}(f_j)} f_j - \frac{x^{\delta}}{\mathtt{LT}(f_k)} f_k = \frac{x^{\delta}}{d_j x^{\delta}} f_j - \frac{x^{\delta}}{d_k x^{\delta}} f_k = p_j - p_k. \quad (2.2)$$

Derved får ligning (2.1) 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 (2.2) 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 2.3.5 (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 2.3.2, 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

$$f = \sum_{i=1}^{t} h_i g_i. \tag{2.3}$$

Lemma 2.2.3 giver da, at

$$mdeg(f) \leq \max(mdeg(h_i g_i)), \text{ for } i = 1, \ldots t. \tag{2.4}$$

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 2.1.2 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 (2.3). Lad $m(i) = mdeg(h_i g_i)$, og definer $\delta = \max(m(1), \ldots, m(t))$. Det vil sige, at ligning (2.4) bliver

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

Polynomiet f kan muligvis opskrives i forskellige variationer, dog vil alle disse være på formen som i (2.3), 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 (2.3), 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 (2.3). Denne kan også skrives, som

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} \mathtt{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathtt{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{2.5}$$

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 2.3.4, 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 2.3.4 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

$$\sum_{m(i)=\delta} \mathtt{LT}(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k), \tag{2.6}$$

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

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{i,jk} g_i, \tag{2.7}$$

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

$$mdeg(a_{i,jk} g_i) \leq mdeg(S(g_j, g_k)) \text{ for alle } i, j, k. \tag{2.8}$$

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

$$x^{\delta-\gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i. \tag{2.9}$$

Dette giver sammen med ligning (2.8), og konklusionen fra Lemma 2.3.4, at

$$mdeg(b_{ijk} g_i) \leq mdeg(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta. \tag{2.10}$$

Ved nu at kombinere ligning (2.6) og (2.9), 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 (2.10), at for alle i, er

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

Ved nu at vende tilbage til ligning (2.5) 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 2.3.6 *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 2.3.5 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

$$\langle \mathtt{LT}(G') \rangle \subseteq \langle \mathtt{LT}(G) \rangle. \tag{2.11}$$

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 (2.11) 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 2.2.8, 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 3

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.

3.1 Bestemmelse af punkter

Dette afsnit bygger hovedsageligt på [8, 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:

$$x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y. \tag{3.1}$$

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 A.1.1.

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

Definition 3.1.1 (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 A.0.10 en divisor for m. Desuden gælder det af Sætning A.0.11, 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 A.0.12 netop de konjugerede af α med hensyn til $\mathbb{F}_q$ som rødder. Så en opskrivning af dette polynomium giver

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + \cdots + a_0 \\ &= (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}). \end{aligned} \tag{3.2}$$

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 A.1.2 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 A.1.1, 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 3.1.2 (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 (3.2), 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 A.1.1 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 3.1.3 *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 A.1.2, 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 A.1.1, 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 A.1.1.

(*v*) Af Lemma A.1.1 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 B.1.2, 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 3.1.4 *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 B.1.2, 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 A.1.1.

(*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 A.1.1 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 3.1.5 *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* $\beta^{q^{m-1}} + \cdots + \beta^q + \beta = 0$

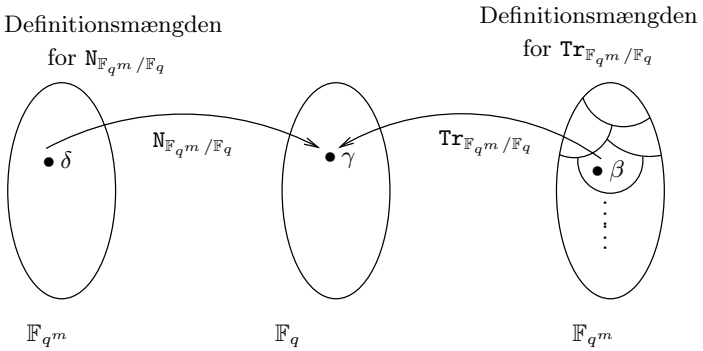
eller

(*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 3.1.5 og beviset herfor er en generalisering af [6, 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 3.1.3 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 3.1, hvor $\mathbb{F}_{q^m}$ er vist to gange for overblikkets skyld.



Figur 3.1: *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.*

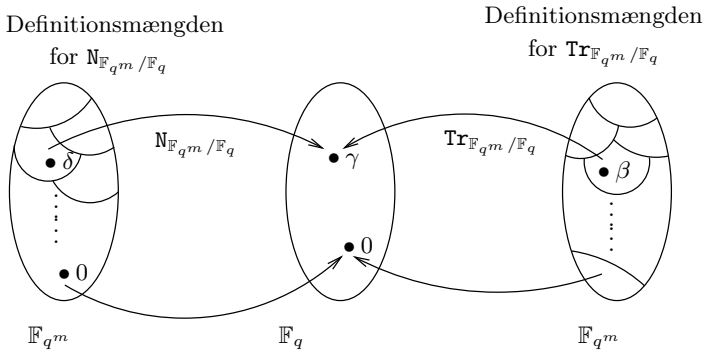
Antallet af kombinationer af δ og β, hvor $\mathtt{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\delta) = \mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)$ er dermed lig $q^m \cdot q^{m-1} = q^{2m-1}$, hvilket netop er antallet af punkter i $\mathbf{V}(I)$.

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 3.2.

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 homomorfi ifølge Sætning 3.1.4. Hvormed $\mathbb{F}_{q^m}^*$ ifølge Sætning B.1.2 er inddelt i $q-1$ ækvivalensklasser med $\frac{q^m-1}{q-1}$ elementer i hver, se Figur 3.2.



Figur 3.2: *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.

3.2 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.

3.2.1 Fodaftryk af et ideal

Dette underafsnit bygger primært på [3, Afsnit 5.3].

Når der er valgt en monomiel ordning på $\mathbf{K}[x_1, \ldots, x_n]$, som defineret i Definition 2.2.1, 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 3.2.1 (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 3.2.2.

Proposition 3.2.2 *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 $\mathbf{K}$. Entydigheden af r følger af Sætning 2.3.1.

(*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 3.2.2 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 3.2.3 *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 3.2.2 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

$$\overline{f + g}^G = \overline{f}^G + \overline{g}^G. \tag{3.3}$$

For at vise dette skal det først vises, at

$$\overline{f}^G = \overline{g}^G \Leftrightarrow f - g \in I. \tag{3.4}$$

$\Rightarrow$: 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 (3.4) 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 (3.4) giver, at $\overline{\overline{f+g}^G}^G = \overline{\overline{f}^G + \overline{g}^G}^G$, 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

$$\overline{cf}^G = c\overline{f}^G. \tag{3.5}$$

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 (3.4), 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 3.2.4 *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

$$m \leq \dim(\mathbf{K}[x_1, \ldots, x_n]/I), \tag{3.6}$$

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

$$\begin{array}{ccc} \varphi\colon \mathbf{K}[x_1, \ldots, x_n]/I & \longrightarrow & \mathbf{K}^m \\ \varphi(f + I) & \longmapsto & (f(p_1), \ldots, f(p_m)), \end{array} \tag{3.7}$$

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 3.2.4.

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 3.2.4 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.

3.2.2 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 3.2.5 (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 [5, Definition 1, side 353].

Definition 3.2.6 (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 2.2.1 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 $w(x^i y^j) = i(q^{m-1}) + j(\frac{q^m-1}{q-1})$.

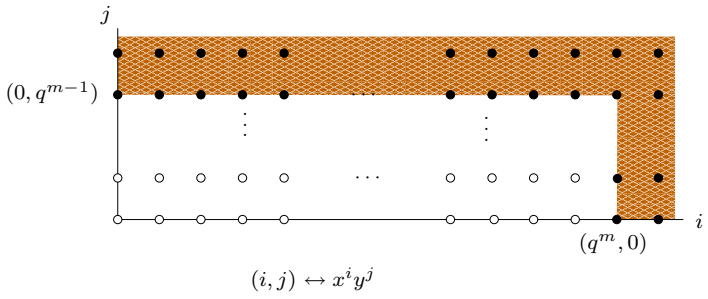
Det kan nu vises, at $\{x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\}$ er en Gröbner basis for idealet $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$.

Proposition 3.2.7 *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 3.3.
Antallet af monomier i D er dermed $q^{m-1} \cdot q^m = q^{2m-1}$.



Figur 3.3: *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 3.1.5 har vi, at antallet af punkter i varieteten $\mathbf{V}(I)$ er q^{2m-1}, og ifølge Sætning 3.2.4 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 3.1.5.

Lad nu I være givet som i Proposition 3.2.7, så giver kommentaren efter Sætning 3.2.4, at følgende afbildning, ψ, er en surjektiv vektorrumshomomorfi,

$$\begin{array}{rccc} \psi\colon & \mathbb{F}_{q^m}[x,y]/I & \longrightarrow & \mathbb{F}_{q^m}^n \\ & \psi(f+I) & \longmapsto & (f(p_1), \ldots, f(p_n)), \end{array} \tag{3.8}$$

hvor $\{p_1, \ldots, p_n\} = \mathbf{V}(I)$.
Da Sætning 3.2.3 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 3.2.8 (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 4

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.

4.1 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 4.1.1 *Lad* **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 [9, 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:

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

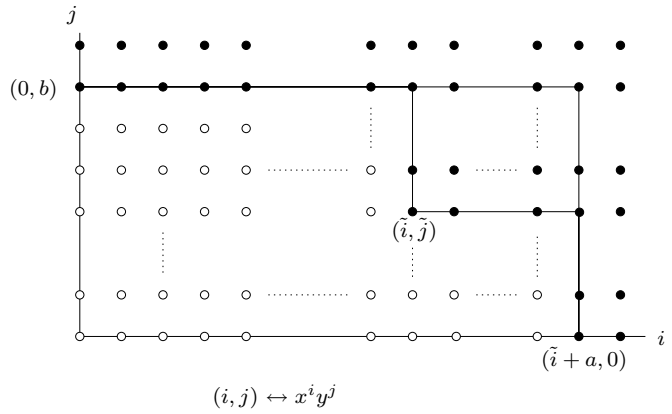
For at begrænse fodaftrykket af $\tilde{I}$ betragtes desuden S-polynomiet, $S(F, \tilde{G}_t)$, som er endnu et polynomium i idealet $\tilde{I}$.

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

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

Denne begrænsning er illustreret på Figur 4.1.
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 4.1.2 *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 4.1.1 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 4.1.3 *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 4.1.1 kan nu anvendes til at bestemme en nedre grænse for minimumsafstanden for NTP-koden.

Sætning 4.1.4 *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 4.1.1 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 4.1.5 *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:

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

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 4.1.3 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 4.1.1, 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.

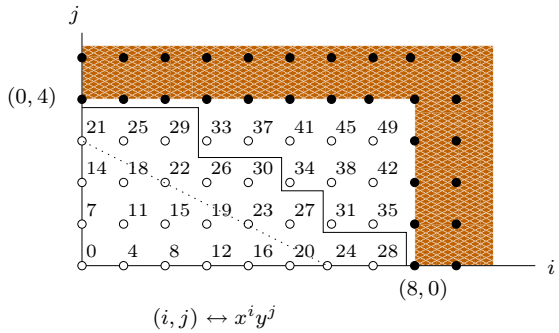
For hvert valgt δ_r, som er rod i $f(x,y)$, eksisterer der q^{m-1} β_t'er, så (δ_r, β_t) er rod i norm-trace polynomiet. Antallet af δ_r'er er i, så dette giver anledning til $i(q^{m-1})$ fælles nulpunkter.
Idet $j < q^{m-1}$, vælges der kun β_t'er fra $Tr_{\gamma_{q-1}}$.
For hvert valgt β_t vil der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

4.2 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 3.2.2, vil også en delmængde af dem være lineært uafhængige. Afbildes monomierne i denne delmængde med ψ givet som i ligning (3.8), 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 4.2 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 4.2: *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 4.2.
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.

4.2.1 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 [10, Afsnit 10.5].

Definition 4.2.1 (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 4.2.2 (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 4.2.3 *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 4.2.4 (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 4.2.3 benyttes i efterfølgende proposition.

Proposition 4.2.5 *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 4.2.4 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 4.2.3, at $c(\Gamma) = 2g$, hvor g er antallet af gaps, og Γ er dermed symmetrisk. Det vil sige, at $g = \frac{(a-1)(b-1)}{2}$. □

4.2.2 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 4.2.5 til at bestemme genus og konduktor.

Sætning 4.2.6 *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 4.1.2, 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 4.2.4.

Det blev i beviset for Lemma 4.1.3 vist, at $\gcd(q^{m-1}, \frac{q^m-1}{q-1}) = 1$. Dermed følger det af Proposition 4.2.5, 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 4.2.7 (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 4.1.3 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 4.2.

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.

4.3 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 4.3.2 får vi brug for følgende lemma:

Lemma 4.3.1 *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 [6, Theorem 14.1.4].

Sætning 4.3.2 *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 4.2.7. 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 4.2.7 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 $\Delta_{\prec_w}(I) = \{x^i y^j : 0 \le i < q^m, 0 \le j < q^{m-1}\}$. For et vilkårligt kodeord, $\overline{c}_1$, i $NTP(s)$ vil der eksistere et polynomium, $F \in \mathbb{F}_{q^m}[x,y]$, i $\mathrm{Span}\{M \in \Delta_{\prec_w}(I) : w(M) \le s\}$, 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 $\mathrm{Span}\{M \in \Delta_{\prec_w}(I) : w(M) \le (n+c(\Gamma)-2-s)\}$, 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 3.1.5 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

$$\sum_{\beta^{q^m-1}+\cdots+\beta^q+\beta=0} 0^{i_1+i_2}\beta^{j_1+j_2}+\sum_{k=0}^{q-2}\sum_{\substack{\beta^{q^m-1}+\cdots+\beta^q+\beta=\\ \delta^{k\frac{q^m-1}{q-1}}}} \beta^{j_1+j_2}\sum_{l=0}^{\frac{q^m-1}{q-1}-1}\left(\delta^{k+l(q-1)}\right)^{i_1+i_2}, \tag{4.1}$$

hvor δ er et primitivt element i $\mathbb{F}_{q^m}$.
Er $i_1+i_2=0$ vil den første sum i (4.1) 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 (4.1) kan omskrives til:

$$\sum_{\beta\in\mathbb{F}_{q^m}}\beta^{j_1+j_2}. \tag{4.2}$$

For $j_1+j_2=0$ er (4.2) lig q^m, hvilket er nul, da vi regner med karakteristik p. Det gælder desuden, at $j_1+j_2 \le \frac{q^m}{q}-1+\frac{q^m}{q}-1 = 2\frac{q^m}{q}-2$. Da $q\ge 2$, vil det derfor være opfyldt, at $j_1+j_2 < q^m-1$. Dermed bliver ligning (4.2) ifølge Lemma 4.3.1 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 (4.1) blive nul, og det resterende kan skrives op som følgende

$$\sum_{k=0}^{q-2}\delta^{k(i_1+i_2)}\sum_{\substack{\beta^{q^m-1}+\cdots+\beta^q+\beta=\\ \delta^{k\frac{q^m-1}{q-1}}}}\beta^{j_1+j_2}\sum_{l=0}^{\frac{q^m-1}{q-1}-1}\delta^{l(q-1)(i_1+i_2)}. \tag{4.3}$$

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 (4.3) 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 (4.3) 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 (4.3), som nu får udseendet

$$\sum_{k=0}^{q-2} \delta^{kh(\frac{q^m-1}{q-1})} \sum_{\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)=\delta^{k(\frac{q^m-1}{q-1})}} \beta^{j_1+j_2} \sum_{l=0}^{\frac{q^m-1}{q-1}-1} (\delta^{q^m-1})^{lh}. \qquad (4.4)$$

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 (4.4) kan skrives som:

$$\sum_{k=0}^{q-2} \delta^{kh(\frac{q^m-1}{q-1})} \sum_{\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)=\delta^{k(\frac{q^m-1}{q-1})}} \beta^{j_1+j_2}. \tag{4.5}$$

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 (4.5) omskrives til

$$\sum_{\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)\neq 0} (\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta))^h \cdot \beta^{j_1+j_2}. \tag{4.6}$$

Da $\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta) = 0$ ikke vil bidrage med noget yderligere til summen, så er (4.6) det samme som

$$\sum_{\beta\in\mathbb{F}_{q^m}} (\mathtt{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta))^h \cdot \beta^{j_1+j_2}. \tag{4.7}$$

Det skal alså vises, at denne sum er lig nul, og fra Lemma 4.3.1 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 (4.7) 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 (4.7) 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 (4.7) 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 (4.3) 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 5

Første dekodningsalgoritme

I de følgende tre kapitler vi jeg se nærmere på dekodning af NTP-koder. Her får jeg brug for at benytte nogle af de egenskaber, som blev fundet i forrige kapitel. Her var der nogle steder begrænsninger for, hvornår sætningerne gjaldt, så derfor vælger jeg i det følgende at arbejde inden for disse begrænsniger. Dette betyder, at jeg antager, at der arbejdes med en $NTP(s)$-kode, hvor det gælder, at

$$c(\Gamma) - 1 \leq s < q^{2m-1} (= n), \tag{5.1}$$

hvor $c(\Gamma) = (\frac{q^m-1}{q-1} - 1)(q^{m-1} - 1)$. Denne begrænsning stammer fra dimensionen af NTP-koden, se Definition 4.2.7, og er dermed også en begrænsning for at kunne bestemme dualkoden.

I dette kapitel, som er baseret på [6, Afsnit 14.2], vil jeg komme frem til en algoritme, som ligger til grund for de efterfølgende algoritmer.

5.1 Grundalgoritmen

Betragt koden $NTP(s)$, givet som i Definition 3.2.8, 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 5.1.1 *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 $\lambda_i \in \mathbb{F}_{q^m}$ 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 5.1.2 *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 4.1.1, 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 3.2.2 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 4.1.3 alle har forskellig vægt.

Den simple repræsentant har dermed udseendet

$$\tilde{Q}(x,y,f(x,y)) = Q(x,y,f(x,y)) - g(x,y)NT(x,y), \tag{5.2}$$

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

$$n - \tau > s + \tau + g \geq w(Q(x,y,f(x,y))) \geq w(\tilde{Q}(x,y,f(x,y))). \tag{5.3}$$

Dermed er alle detaljerne på plads til at anvende Proposition 4.1.1. 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 (5.3) give, at

$$\#\mathbf{V}(\langle \tilde{Q}(x,y,f(x,y)), NT(x,y)\rangle) \leq s+\tau+g < n-\tau. \tag{5.4}$$

Ved at betragte $Q(x,y,f(x,y))$ og $\tilde{Q}(x,y,f(x,y))$, i ligning (5.2) 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 (5.4), 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 5.1.3 (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 5.1.4 (Første dekodningsalgoritme)
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 5.1.1 giver, at der altid vil eksistere en løsning til det opskrevne ligningssystem, hvorefter Sætning 5.1.2 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 ifølge [6, Theorem 1.2.1]. 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 6

Basis- og majoritetsdekodning

De følgende to kapitler er hovedsagligt baseret på [10, Afsnit 6 og 7].

6.1 Dekodning med dobbeltsyndromer

I dette afsnit vil der blive beskrevet en lidt anderledes dekodningsalgoritme, som finder fejlpositionerne i et modtaget ord ved hjælp af de såkaldte dobbeltsyndromer, og derefter bestemmer fejlværdierne ligesom algoritmen beskrevet i Kapitel 5, det vil sige, at punkt 4 og 5 fra algoritmen på side 62 genbruges, mens punkt 1, 2 og 3 erstattes af noget tilsvarende.

Allerede efter definitionen af NTP-koder er det konkluderet, at der til et polynomium, som er en linear kombination af monomierne i fodaftrykket, hører et entydigt kodeord. Derfor vil der i dette og følgende afsnit ofte blive refereret til polynomierne, som værende kodeord, selvom det er polynomierne evalueret, der er de egentlige kodeord.

I dette og de følgende afsnit vil vægten af et polynomium blive anvendt. Der startes derfor med at kigge lidt nærmere på dette.

6.1.1 Vægten af et polynomium

Vægten af et polynomium blev præsenteret allerede i afsnit 3.2.2, men i dette og følgende afsnit skal nogle af dens egenskaber også benyttes, så definitionen bliver her præciseret.

Definition 6.1.1 (Vægten af et polynomium) *Lad* $J = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y \rangle$ *og lad* $f \in \mathbb{F}_{q^m}[x,y]/J$ *og benævn* $f = F + J$, *hvor* $supp(F)$ *tilhører fodaftrykket af* J *med den monomielle ordning* $\prec_w$. *Da er vægten af* f *givet ved*

$$\omega(f) = \max_{\prec_w}\{w(x^i y^j) : x^i y^j \in supp(F)\},$$

hvor $w(x^i y^j) = i(q^{m-1}) + j(\frac{q^m-1}{q-1})$.

Denne definition er veldefineret, da monomier i fodaftrykket af J alle har forskellige vægte (se Lemma 4.1.3) og vektorrummet udspændt af monomierne i fodaftrykket er isomorf med $\mathbb{F}_{q^m}[x,y]/J$ (set som vektorrum) (se Sætning 3.2.3).

Det er nu muligt at vise følgende egenskaber ved funktionen ω. Det er dog ikke alle, der skal benyttes i dette afsnit, men de bliver nyttige senere. Definition på betegnelserne $mdeg(f)$ og lignende kan ses i Definition 2.2.2.

Lemma 6.1.2 *Lad* $f_i, f_j, h \in \mathbb{F}_{q^m}[x,y]/J$. *Da gælder følgende egenskaber:*

(*i*) $\omega(f_i f_j) = \omega(f_i) + \omega(f_j)$.

(*ii*) *Hvis* $f_i + f_j \neq 0$, *så er* $\omega(f_i + f_j) \leq \max_{\prec_w}\{\omega(f_i), \omega(f_j)\}$.

(*iii*) *Hvis* $\omega(f_i) < \omega(f_j)$ *og* $h \neq 0$, *så er* $\omega(hf_i) < \omega(hf_j)$.

(*iv*) *Lad* $\varepsilon \in \mathbb{F}_{q^m}^*$, *så er* $\omega(\varepsilon f) = \omega(f)$.

(*v*) $\omega(f_i) \leq i + g - 1$, *hvor der gælder lighedstegn, hvis* $i > g$.

Bevis: Benævn gennem beviset $f_i = F_i + J$, $f_j = F_j + J$ og $h = H + J$, hvor $supp(F_i), supp(F_j)$ og $supp(H)$ tilhører fodaftrykket af J med den monomielle ordning $\prec_w$.

Lad $F_i = \sum_\alpha a_\alpha x^{\alpha_1} y^{\alpha_2}$ og $F_j = \sum_\beta b_\beta x^{\beta_1} y^{\beta_2}$. Lad vektoren $\overline{u}$ være vægtvektoren, det vil sige $\overline{u} = (q^{m-1}, \frac{q^m-1}{q-1})$.

(i) : Det gælder, at

$$\begin{aligned}\omega(f_i f_j) &= \max_{\prec_w}\{w(x^i y^j) : x^i y^j \in supp(F_i F_j)\} \\ &= \overline{u} \cdot mdeg(F_i F_j).\end{aligned}$$

Da der her betragtes et produkt af to polynomier, og da $\prec_w$ er en monomiel ordning på $\mathbb{F}_{q^m}[x,y]$ er

$$\begin{aligned}mdeg(F_i F_j) &= \max_{\prec_w}\{\alpha+\beta \in \mathbb{N}_0^n : a_{\alpha+\beta} \neq 0\} \\ &= \max_{\prec_w}\{\alpha \in \mathbb{N}_0^n : a_\alpha \neq 0\} + \max\{\beta \in \mathbb{N}_0^n : b_\beta \neq 0\} \\ &= mdeg(F_i) + mdeg(F_j).\end{aligned}$$

Dermed bliver

$$\begin{aligned}\omega(f_i f_j) &= \overline{u} \cdot (mdeg(F_i) + mdeg(F_j)) \\ &= \overline{u} \cdot mdeg(F_i) + \overline{u} \cdot mdeg(F_j) \\ &= \omega(f_i) + \omega(f_j).\end{aligned}$$

(ii) : Lemma 2.2.3 kan benyttes til at få ulighedstegnet ind i følgende omskrivning:

$$\begin{aligned}\omega(f_i + f_j) &= \max_{\prec_w}\{w(x^i y^j) : x^i y^j \in supp(F_i + F_j)\} \\ &= \overline{u} \cdot mdeg(F_i + F_j) \\ &\leq \overline{u} \cdot (\max_{\prec_w}\{mdeg(F_i), mdeg(F_j)\}) \\ &= \max_{\prec_w}\{\overline{u} \cdot mdeg(F_i), \overline{u} \cdot mdeg(F_j)\} \\ &= \max_{\prec_w}\{\omega(f_i), \omega(f_j)\}.\end{aligned}$$

(iii) : Dette er en konsekvens af punkt (i).

(iv) : Dette er ligeledes en konsekvens af punkt (i), da $\omega(\varepsilon) = 0$.

(v) : Lad Γ være den ordnede mængde af mulige vægte af polynomier og lad $g(l)$ være antallet af gaps, som er mindre end $\omega(f_l)$ i denne mængde. Som tidligere er g det samlede antal gaps, hvilket betyder, at $g(l) \leq g$.

Det gælder, at $\omega(f_i)$ er det $(\omega(f_i)+1)$'te element i $\mathbb{N}_0$, det vil sige, at $\omega(f_i)$ er det $(\omega(f_i)+1-g(i))$'te element i Γ. Dermed er

$$i = \omega(f_i) + 1 - g(i) \geq \omega(f_i) + 1 - g, \tag{6.1}$$

så $\omega(f_i) \leq i + g - 1$.

Det gælder, at $g(l) = g$ hvis og kun hvis, at $\omega(f_l) \geq c$. Kondukteren c er det $(c+1)$'te element i $\mathbb{N}_0$ og det $(c+1-g)$'te element i Γ. Det vil sige $c = \omega(f_{c+1-g})$.

Lad det nu være opfyldt, at $i > c-g = g$ (da $c = 2g$). Så er $\omega(f_i) \geq \omega(f_{c+1-g}) = c$ og dermed er $g(i) = g$. Det kan nu sættes ind i ligning (6.1), og så bliver $\omega(f_i) = i + g - 1$. □

I næste afsnit introduceres nogle brugbare vektorrum frem mod basisalgoritmen.

6.1.2 Dobbeltsyndrom og nyttige vektorrum

Til definitionen af dobbeltsyndromer skal der benyttes paritetstjek, $\overline{h}$, som jo er kodeordene i dualkoden. Dualkoden til en $NTP(s)$-kode er kendt ifølge Sætning 4.3.2 til også at være en NTP-kode, hvor indekset er $n+c(\Gamma)-s-2$. Dualkodens dimension benævnes i det følgende med l, for at den ikke skal blive forvekslet med den oprindelige kodes dimension, k. Er der valgt et s til definitionen af en NTP-kode, kan l bestemmes udfra dette s og formler for dimensionen. Ifølge Sætning 4.2.7 er dimensionen af en $NTP(s)$-kode givet ved $s+1-g$, når det er opfyldt, at $c(\Gamma) - 1 \leq s < n$, hvor $c(\Gamma) = (\frac{q^m-1}{q-1} - 1)(q^{m-1} - 1)$, $n = q^{2m-1}$ og $g = \frac{(\frac{q^m-1}{q-1}-1)(q^{m-1}-1)}{2}$. Denne dimension kan også bestemmes udfra dualkodens dimension, l, og da er den givet ved $n - l$. Dermed kan l bestemmes til

$$l = n + g - s - 1. \tag{6.2}$$

Tilsvarende bliver

$$s = n + g - l - 1. \tag{6.3}$$

Ovenstående omskrivninger gælder dog kun inden for begrænsningen på s, hvilket også giver en begrænsning på l, da det jo også skal være opfyldt, at

$$\begin{array}{ccc} c(\Gamma) - 1 \leq n + g - l - 1 < n \\ \Updownarrow \qquad\qquad \Updownarrow \\ l \leq n - g \quad g - 1 < l, \end{array}$$

det vil sige omskrivninger er kun tilladt, når $c(\Gamma) - 1 \leq s < n$ eller når $g - 1 < l \leq n - g$.

I de følgende afsnit er det nogle gange hensigtsmæssigt at kunne skelne mellem forskellige NTP-koder. Derfor vil en NTP-kode nogle gange blive specifiseret med s_l for at indikere, at dualkodens dimension er l.

Der findes altså l monomier, $f_1, \ldots, f_l$, som evalueret i de n punkter danner basis for dualkoden. Da dualkoden også er en NTP-kode vælges de l monomier til denne sådan, at når $i < j < l$ er $\omega(f_i) < \omega(f_j) < \omega(f_l)$ og det monomium med størst vægt er f_l. Paritetstjekkene til $NTP(s)$ koden er således $\overline{h}_i = \psi(f_i)$ for $i \leq l$.

Monomierne som benyttes i dualkoden til $NTP(s_l)$ kan også ses som en basis for et vektorrum, som benævnes L_l. Dette vektorrum benyttes i følgende definition, som er nødvendig for, at definitionen af dobbeltsyndromerne bliver brugbar. Følgende funktion defineres således:

Definition 6.1.3 (Funktionen $l(i,j)$)
Tallet $l(i,j)$ defineres til at være det mindste heltal l, hvorom det gælder, at $f_i f_j$ tilhører vektorrummet L_l.

Når der arbejdes i en NTP-kode, er det ganske simpelt at finde $l(i,j)$, hvilket kan ses af følgende eksempel.

Eksempel 6.1.4 Monomierne i dette eksempel er hentet i Eksempel 6.1.12, se tabel side 75. Tag følgende monomier: $f_2 = x$, $f_5 = xy$, så er $f_2 f_5 = x^2 y$. Det gælder, at $x^2 y = f_8$, så $l(2,5) = 8$.

Dette kan også indses ved at se på vægten af monomierne: Det gælder, at $\omega(f_2) = 4$, $\omega(f_5) = 9$. Da vil $\omega(f_2 f_5) = 13$, så $f_2 f_5$ vil tilhøre det vektorrum L_l, hvorom

det gælder, at $\omega(f_l) = 13$. Dette er netop tilfældet for $l = 8$. Dermed kan det ses, at $\omega(f_i f_j) = \omega(f_i) + \omega(f_j) = \omega(f_{l(i,j)})$.

Det er også muligt at vise følgende lemma om funktionen $l(i,j)$

Lemma 6.1.5 *Funktionen $l(i,j)$ er voksende i begge dens argumenter.*

Bevis: Det benyttes, at $\omega(f_i f_j) = \omega(f_{l(i,j)})$, og at $\omega(f_k) < \omega(f_{k+1})$. Da giver Lemma 6.1.2 (iii), at

$$\omega(f_{l(i,j)}) = \omega(f_i f_j) < \omega(f_{i+1} f_j) = \omega(f_{l(i+1,j)}) \quad \text{og at}$$
$$\omega(f_{l(i,j)}) = \omega(f_i f_j) < \omega(f_i f_{j+1}) = \omega(f_{l(i,j+1)}),$$

hvilket betyder, at funktionen $l(i,j)$ er voksende i begge dens argumenter. □

Nu skal dobbeltsyndrom defineres, hvilket gøres således:

Definition 6.1.6 (Dobbeltsyndrom) *Lad $\overline{r} \in \mathbb{F}_{q^m}^n$ og lad h_i for $1 \leq i \leq n$ være paritetstjek for en NTP-kode. Da er dobbeltsyndromet af $\overline{r}$ givet ved*

$$s_{i,j}(\overline{r}) = \overline{r} \cdot (\overline{h}_i * \overline{h}_j),$$

hvor $\overline{h}_i * \overline{h}_j = (h_{i,1}h_{j,1}; \ldots; h_{i,n}h_{j,n})$.

Desuden er dobbeltsyndrommatricen givet ved

$$S(i,j) = (s_{i',j'}(\overline{r}) : 1 \leq i' \leq i, 1 \leq j' \leq j).$$

Da det gælder, at

$$\begin{aligned}
\overline{h}_i * \overline{h}_j &= (h_{i,1}h_{j,1}, \ldots, h_{i,n}h_{j,n}) \\
&= (\psi(f_i)_1 \psi(f_j)_1, \ldots, \psi(f_i)_n \psi(f_j)_n) \\
&= (f_i(p_1) f_j(p_1), \ldots f_i(p_n) f_j(p_n)) \\
&= (f_i f_j(p_1), \ldots, f_i f_j(p_n)) \\
&= \psi(f_i f_j)
\end{aligned}$$

vil $\overline{h}_i * \overline{h}_j$ også være et paritetstjek, så længe $l(i,j) \leq l$. Hvis $\overline{r}$ er et modtaget ord, således at $\overline{r} = \overline{c} + \overline{e}$, hvor $\overline{c}$ er et kodeord i $NTP(s)$-koden og $\overline{e}$ er en fejlvektor, da er $s_{i,j}(\overline{r}) = s_{i,j}(\overline{e})$ for alle i, j, hvorom det gælder, at $l(i,j) \leq l$.

Nu defineres to nyttige vektorrum og derefter vises det, at disse er identiske under visse forudsætninger. Det første vektorrum defineres således:

Definition 6.1.7 (K-vektorrum) *Antag at $l(i,j) \leq l$ og lad $\overline{r} \in \mathbb{F}_{q^m}^n$. Da defineres K-vektorrummet udfra $\overline{r}$ således:*

$$K_{ij}(\overline{r}) = \{f \in L_j : \overline{r} \cdot \psi(gf) = 0 \text{ for alle } g \in L_i\}.$$

Denne definition gør, at $K_{ij}(\overline{r})$ er et underrum af L_j, hvilket dog ikke vil blive bevist her.

Betragt istedet dobbeltsyndrommatricen, $S(i,j)$, som, da $\psi(f_i f_j) = \overline{h}_i * \overline{h}_j$, ser ud på følgende måde:

$$\begin{array}{c} \\ f_1 \\ f_2 \\ \vdots \\ f_i \end{array} \begin{array}{c} \begin{array}{cccccccc} f_1 & & f_2 & \cdots & f_k & \cdots & f_j \end{array} \\ \begin{bmatrix} \overline{r} \cdot \psi(f_1 f_1) & \overline{r} \cdot \psi(f_1 f_2) & \cdots & \overline{r} \cdot \psi(f_1 f_k) & \cdots & \overline{r} \cdot \psi(f_1 f_j) \\ \overline{r} \cdot \psi(f_2 f_1) & \overline{r} \cdot \psi(f_2 f_2) & \cdots & \overline{r} \cdot \psi(f_2 f_k) & \cdots & \overline{r} \cdot \psi(f_2 f_j) \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ \overline{r} \cdot \psi(f_i f_1) & \overline{r} \cdot \psi(f_i f_2) & \cdots & \overline{r} \cdot \psi(f_i f_k) & \cdots & \overline{r} \cdot \psi(f_i f_j) \end{bmatrix} \end{array}.$$

Denne matrix kan definere en lineær afbildning, T, fra $L_j \to L_i$ med $f_1, \ldots, f_j$ og $f_1, \ldots, f_i$ som baser for henholdsvis L_j og L_i. Det vil gælde, at $K_{ij}(\overline{r})$ er nulrummet for denne lineare afbildning T. Da afbildningen T netop er repræsenteret ved $S(i,j)$, gælder der, at $K_{ij}(\overline{r}) = K_{ij}(\overline{e})$, når $l(i,j) \leq l$.

Det næste vektorrum defineres nu således:

Definition 6.1.8 (L af J-vektorrum) *Lad J være en delmængde af mængden {1, ..., n}. Da defineres L af J-vektorrummet således:*

$$L_j(J) = \{f \in L_j : \psi(f)_k = 0 \text{ for alle } k \in J\},$$

hvor $\psi(f)_k$ benævner den k-te koordinat i $\psi(f)$.

Lad $I = \text{supp}(e) = \{k \in \{1, \ldots, n\} : e_k \neq 0\}$. Polynomierne i $L_j(I)$ vil netop være de polynomier, som giver nul på mindst de positioner, hvor fejlvektoren har en værdi forskellig fra nul. Derfor kaldes disse polynomier for fejllokaliserende polynomier. Målet ved denne dekodningsdel er netop at få bestemt disse polynomier, da fejlpositionerne dermed er lokaliseret. Det ønskes derfor at kunne bestemme $L_j(I)$. Efterfølgende lemma viser, at dette er muligt ved hjælp af dobbeltsyndromer. I lemmaet benyttes $\omega_H(\overline{v})$, som er Hammingvægten af vektoren $\overline{v}$.

Lemma 6.1.9 *Antag, at $l(i,j) \leq l$. Hvis $I = supp(e) = \{k \in \{1, \ldots, n\} : e_k \neq 0\}$, da er $L_j(I) \subseteq K_{ij}(\overline{r})$. Hvis det desuden gælder, at $d(NTP(s_i)) > \omega_H(\overline{e})$, så er $L_j(I) = K_{ij}(\overline{r})$.*

Bevis: Antag først, at $f \in L_j(I)$. Dette betyder, at $\psi(f)_k = 0$ for alle k, hvorom det gælder, at $e_k \neq 0$. Dermed er

$$\overline{e} \cdot (\psi(f) * \psi(g)) = \sum_{e_k \neq 0} e_k \left(\psi(f) * \psi(g)\right)_k = 0$$

for alle $g \in L_i$. Dette betyder netop, at $f \in K_{ij}(\overline{e}) = K_{ij}(\overline{r})$.

Dernæst antages det, at $d(NTP(s_i)) > \omega_H(\overline{e})$, og at $f \in K_{ij}(\overline{r}) = K_{ij}(\overline{e})$. Lad $\overline{a} = \psi(f)$. Udfra definitionen af $K_{ij}(\overline{r})$ kan det konkluderes, at

$$\begin{aligned}(\overline{e} * \overline{a}) \cdot \psi(g) &= e_1 a_1 \psi(g)_1 + \cdots + e_n a_n \psi(g)_n \\ &= \overline{e} \cdot (a_1 \psi(g)_1, \ldots, a_n \psi(g)_n) \\ &= \overline{e} \cdot (\psi(f) * \psi(g)) = 0\end{aligned}$$

for alle $g \in L_i$. Dette betyder, at $\overline{e} * \overline{a} \in NTP(s_i)$, da L_i netop indeholder paritetstjekkene til denne kode. Det gælder, at $\omega_H(\overline{e} * \overline{a}) \leq \omega_H(\overline{e})$ og da det er antaget, at $\omega_H(\overline{e}) < d(NTP(s_i))$, bliver $\omega_H(\overline{e} * \overline{a}) < d(NTP(s_i))$. Derfor må det nødvendigvis gælde, at $\overline{e} * \overline{a} = \overline{0}$. Dermed er $e_k a_k = e_k \psi(f)_k = 0$ for alle $k \in \{1, \ldots, n\}$. Derfor må det gælde, at $\psi(f)_k = 0$ for alle $k \in I$ og dette er netop betingelsen for, at $f \in L_j(I)$. □

6.1.3 Basisalgoritmen

Det er nu muligt at opstille en algorime og vise, at den virker. Algoritmen lyder som følger:

Algoritme 6.1.10 *[Basisalgoritme] Denne algoritme kan rette* $\lfloor \frac{n-s_l-g-1}{2} \rfloor$ *fejl for* $NTP(s_l)$*-koden, hvor* $g = \frac{(\frac{q^m-1}{q-1}-1)(q^{m-1}-1)}{2}$.

Input: Et modtaget ord $\overline{r}$.
Output: Fejlpositionerne i fejlvektoren $\overline{e}$.

1. *Vælg* $i = \lfloor \frac{l}{2} \rfloor$ *og* $j = t + 1$.
2. *Bestem* $K_{ij}(\overline{r})$.
3. *Vælg et polynomium* $f \in K_{ij}(\overline{r})$ *forskellig fra nulpolynomiet.*
4. *Fejlpositionerne er nu blandt de positioner, som svarer til nulpunkterne i polynomiet* f.

Bevis: Det antages, at $t = \frac{n-s_l-g-1}{2}$, hvor t er antallet af fejl, der maksimalt må være sket. Dette giver ved omskrivning til l udfra ligning (6.3) følgende:

$$t = \frac{n - s_l - g - 1}{2} = \frac{n - (n + g - l - 1) - g - 1}{2}$$

$$\Updownarrow$$

$$t = \frac{l - 2g}{2} = \frac{l}{2} - g,$$

hvilket skal benyttes senere i beviset.

Udfra Lemma 6.1.2 (v) er $w(f_j) \leq \frac{l}{2}$ og $w(f_i) = \lfloor \frac{l}{2} \rfloor + g - 1$. Da det gælder, at $w(f_i f_j) = w(f_i) + w(f_j)$ er $w(f_i f_j) \leq l + g - 1 = \omega(f_l)$. Dermed er $l(i,j) \leq l$, hvilket er en betingelse for, at $K_{ij}(\overline{r}) = K_{ij}(\overline{e})$.

Valget af $j = t + 1$ har desuden den fordel, at $L_j(I)$ ikke kun består af nulpolynomiet. Dette skyldes, at L_j har dimension $j = t + 1$, men I giver højst t betingelser til udvælgelse af polynomier i L_j, og dermed vil der være flere løsninger end nulpolynomiet.

Sætning 4.1.4 giver sammen med ligning (6.3), at

$$d(NTP(s_i)) \geq n - s_i = n - n - g + i + 1 = i + 1 - g = \left\lfloor \frac{l}{2} \right\rfloor + 1 - g.$$

Dermed er

$$d(NTP(s_i)) > \frac{l}{2} - g = t,$$

så Lemma 6.1.9 giver, at $L_j(I)$ kan bestemmes ved at bestemme $K_{ij}(\overline{r})$. Altså er det muligt at bestemme et fejllokaliserende polynomium, da det vil være polynomierne i $K_{ij}(\overline{r})$, og nulpunkterne i et fejllokaliserende polynomium er mindst de punkter, som er fejlpositioner i det modtagne ord. Polynomierne i $K_{ij}(\overline{r})$ tilhører L_j, og så giver Proposition 4.1.1, at polynomiet f har højst $\omega(f)$ nulpunkter. Da $\omega(f) \leq j = t+1 = \frac{n-s-g+1}{2} \leq \frac{d-g+1}{2} \leq d-1$ vil fejlvektoren være entydigt bestemt, se eventuelt [10, Proposition 6.1]. □

Følgende eksempel viser, hvorledes denne basisalgoritme virker. Heri benyttes følgende definition, som også benyttes i afsnit 7.1.2.

Definition 6.1.11 (S-funktion) *Lad $\overline{y} \in \mathbb{F}_q^n$. Da defineres S-funktionen til at være*

$$S_{\overline{y}}(f) = \overline{y} \cdot \psi(f).$$

Det kan ses, at $S_{\overline{y}}(f_i) = s_i$ og $S_{\overline{y}}(f_i f_j) = s_{ij}(\overline{y})$. Hvis $\overline{r}$ er et modtaget ord med fejlvektor $\overline{e}$, vil det dermed gælde, at hvis $\omega(f) \leq \omega(f_l)$ er $S_{\overline{r}}(f) = S_{\overline{e}}(f)$.

Eksempel 6.1.12 Vælg $m = 2$ og $q = 4$. Dermed bliver vægtvektoren $u = (i, j) = (4, 5)$, og der arbejdes over $\mathbb{F}_{4^2}[x, y]/\langle x^5 + y^4 + y, x^{16} + x, y^{16} + y\rangle$. Som primitivt polynomium vælges $t^4 + t + 1$, og da bliver $\alpha = t$ et primitivt element. Desuden er $n = q^{2m-1} = 64$ og $g = \frac{(i-1)(j-1)}{2} = 6$. Her vælges $y \prec_{lex} x$.

Betragt nu $NTP(43)$, så bliver $l = n + g - s - 1 = 26$, $d = n - s = 21$ og $k = s + 1 - g = 38$, og basisalgoritmen kan rette $t = \frac{n-s-g-1}{2} = 7$ fejl. Der laves derfor syv fejl i punkterne $p_1 = (1, \alpha), p_2 = (\alpha^8, \alpha^3), p_3 = (\alpha, \alpha^7), p_4 = (\alpha^2, \alpha^3), p_5 = (\alpha^{11}, \alpha^3), p_6 = (\alpha^5, \alpha^3)$ og $p_7 = (\alpha^{14}, \alpha^3)$ med følgende værdier

$e_1 = \alpha^6, e_2 = \alpha^8, e_3 = \alpha^7, e_4 = \alpha, e_5 = 1, e_6 = \alpha^6$ og $e_7 = \alpha^{10}$. Da $s_k(\overline{r}) = s_k(\overline{e})$ for $k \leq l$, er det nu muligt at finde syndromerne op til og med l, selvom det kun er fejlvektoren og ikke det modtagne ord som kendes. Eksempelvis er

$$\begin{aligned} s_2(\overline{r}) = s_2(\overline{e}) &= (\alpha^6, \alpha^8, \alpha^7, 1, \alpha, \alpha^6, \alpha^{10}, 0, \ldots, 0) \cdot (1, \alpha^8, \alpha, \alpha^2, \alpha^{11}, \alpha^5, \alpha^{14}, \ldots) \\ &= \alpha^6 + \alpha + \alpha^8 + \alpha^3 + \alpha^{11} + \alpha^{11} + \alpha^9 + 0 = \alpha^{14}. \end{aligned}$$

Dette giver ved udregning af alle de andre syndromer følgende skema:

l	1	2	3	4	5	6	7	8	9	10
f_l	1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3
$\omega(f_l)$	0	4	5	8	9	10	12	13	14	15
$s_l(\overline{r})$	α^9	α^{14}	0	α^5	α^9	α^9	α^7	α^{14}	α^{11}	α^6

l	11	12	13	14	15	16	17	18	19	20
f_l	x^4	x^3y	x^2y^2	xy^3	y^4	x^4y	x^3y^2	x^2y^3	xy^4	y^5
$\omega(f_l)$	16	17	18	19	20	21	22	23	24	25
$s_l(\overline{r})$	α^2	α^{12}	0	α^4	α^5	α^5	α^{12}	α^7	α^7	α^6

l	21	22	23	24	25	26
f_l	x^4y^2	x^3y^3	x^2y^4	xy^5	y^6	x^4y^3
$\omega(f_l)$	26	27	28	29	30	31
$s_l(\overline{r})$	α^6	α^3	α^6	α^4	α^{11}	α^{10}

I basisalgoritmen vælges $i = \left\lfloor \frac{l}{2} \right\rfloor = 13$ og $j = t + 1 = 8$, så et element i $K_{13,8}$ vil være på formen

$$\lambda_1 + \lambda_2 x + \lambda_3 y + \lambda_4 x^2 + \lambda_5 xy + \lambda_6 y^2 + \lambda_7 x^3 + \lambda_8 x^2 y,$$

hvor λ'erne skal opfylde, at

$$\begin{bmatrix} \alpha^9 & \alpha^{14} & 0 & \alpha^5 & \alpha^9 & \alpha^9 & \alpha^7 & \alpha^{14} \\ \alpha^{14} & \alpha^5 & \alpha^9 & \alpha^7 & \alpha^{14} & \alpha^{11} & \alpha^2 & \alpha^{12} \\ 0 & \alpha^9 & \alpha^9 & \alpha^{14} & \alpha^{11} & \alpha^6 & \alpha^{12} & 0 \\ \alpha^5 & \alpha^7 & \alpha^{14} & \alpha^2 & \alpha^{12} & 0 & \alpha^5 & \alpha^5 \\ \alpha^9 & \alpha^{14} & \alpha^{11} & \alpha^{12} & 0 & \alpha^4 & \alpha^5 & \alpha^{12} \\ \alpha^9 & \alpha^{11} & \alpha^6 & 0 & \alpha^4 & \alpha^5 & \alpha^{12} & \alpha^7 \\ \alpha^7 & \alpha^2 & \alpha^{12} & \alpha^5 & \alpha^5 & \alpha^{12} & 1 & \alpha^5 \\ \alpha^{14} & \alpha^{12} & 0 & \alpha^5 & \alpha^{12} & \alpha^7 & \alpha^5 & \alpha^6 \\ \alpha^{11} & 0 & \alpha^4 & \alpha^{12} & \alpha^7 & \alpha^7 & \alpha^6 & \alpha^3 \\ \alpha^6 & \alpha^4 & \alpha^5 & \alpha^7 & \alpha^7 & \alpha^6 & \alpha^3 & \alpha^6 \\ \alpha^2 & \alpha^5 & \alpha^5 & 1 & \alpha^5 & \alpha^6 & \alpha^8 & \alpha^{13} \\ \alpha^{12} & \alpha^5 & \alpha^{12} & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^{13} & \alpha \\ 0 & \alpha^{12} & \alpha^7 & \alpha^6 & \alpha^3 & \alpha^6 & \alpha & \alpha^{10} \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \\ \lambda_5 \\ \lambda_6 \\ \lambda_7 \\ \lambda_8 \end{bmatrix} = \overline{0}.$$

Denne matrix er dobbeltsyndrommatricen $S(13, 8)$, hvor det er benyttet, at $S_{\overline{r}}(x^5) = S_{\overline{r}}(y^4 + y) = \alpha^5 + 0 = \alpha^5$, og lignende omskrivninger er benyttet til

$S_{\overline{r}}(x^6), S_{\overline{r}}(x^5y), S_{\overline{r}}(x^7), S_{\overline{r}}(x^6y)$ og $S_{\overline{r}}(x^5y^2)$. Dette ligningssystem kan nu løses, (eventuelt ved hjælp af Maple) og det giver, at

$$\begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \\ \lambda_5 \\ \lambda_6 \\ \lambda_7 \\ \lambda_8 \end{bmatrix} = \begin{bmatrix} \alpha^{11}(\lambda_6 + \alpha^8\lambda_8) \\ \alpha^{13}(\lambda_6 + \alpha^9\lambda_8) \\ \alpha^{13}(\lambda_6 + \alpha^3\lambda_8) \\ \alpha^3\lambda_8 \\ \alpha^{10}(\lambda_6 + \alpha^9\lambda_8) \\ \lambda_6 \\ 0 \\ \lambda_8 \end{bmatrix},$$

er en løsning. Ved at vælge $\lambda_6 = 1$ og $\lambda_8 = 0$ fåes, at

$$\alpha^{11} + \alpha^{13}x + \alpha^{13}y + \alpha^{10}xy + y^2 \in K_{13,8},$$

som da vil være et fejllokaliserende polynomium, hvilket også stemmer overens med at $p_1, \ldots, p_8$ er nulpunkter heri. Dette polynomium har dog, blandt punkterne anvendt til koden, også $(\alpha^{11}, \alpha^{14}), (\alpha^{14}, \alpha^{12}), (\alpha^4, \alpha^6)$ som nulpunkter, men disse giver en fejlværdi på nul ved bestemmelse af fejlværdierne, så dette er reelt ikke en fejl. Dette skyldes, at fejlvektoren er entydigt bestemt, som nævnt sidst i beviset for Basisalgoritmen.

6.2 Dekodning med majoritetsprincip

I dette afsnit vil der blive præsenteret endnu en metode til at dekode en $NTP(s)$-kode med. For at præsentere ideen ved denne dekodningsalgoritme er det nødvendigt først at introducere størrelsen N. Her er er $J = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y \rangle$ ligesom i afsnit 4.1. Tilsvarende er $\Delta_{\prec_w}(J)$ fodaftrykket af J, hvor $\prec_w$ er den monomielle ordning. For f_i'erne, som anvendes i det følgende gælder det, at $\omega(f_i) < \omega(f_j)$ for $i < j$.

Størrelsen N har nu den egenskab, at

$$Span\{\psi(f_i) : f_i \in \Delta_{\prec_w}(J), \text{ og } i = 1, \ldots, N\} = \mathbb{F}_{q^m}^n, \quad \text{mens}$$
$$Span\{\psi(f_i) : f_i \in \Delta_{\prec_w}(J), \text{ og } i = 1, \ldots, (N-1)\} \subsetneq \mathbb{F}_{q^m}^n,$$

Det vil sige, at $N \geq n$.

For en NTP-kode gælder det, at $f_N = x^{q^m-1}y^{q^{m-1}-1}$, da det er det sidste monomium, som er med i fodaftrykket for $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q -$

$y, x^{q^m} - x, y^{q^m} - y\rangle$, hvor $\prec_w$ er den monomielle ordning. Dermed er $\omega(f_N) = (q^m - 1)q^{m-1} + (q^{m-1} - 1)\left(\frac{q^m-1}{q-1}\right)$, og så kan Lemma 6.1.2($v$) benyttes til at konkludere, at

$$N = (q^m - 1)q^{m-1} + (q^{m-1} - 1)\left(\frac{q^m - 1}{q - 1}\right) - g + 1.$$

Lad nu H være en $N \times n$ matrix, som har paritetstjekket h_i som den i'te række for $1 \leq i \leq N$.

Ideen i denne dekodning er at finde værdierne for alle syndromer, også dem som umiddelbart ikke kan bestemmes, og derved finde fejlvektoren ved at løse ligningssystemet $H\overline{x} = S$, hvor S er syndromvektoren fundet udfra fejlvektoren $\overline{e}$. I processen er det muligt at genbruge dekodning med dobbeltsyndrom, men ved at finde de såkaldte ukendte syndromer, er det muligt at rette flere fejl.

Syndromerne, som er indgangene i syndromvektoren S, vil i det følgende blive benævnt s_i, og $\overline{r}$ vil være et modtaget ord med fejlvektoren $\overline{e}$. Det gælder, så længe $i \leq l$ kan s_i bestemmes ved hjælp af $\overline{r}$, da

$$s_i = s_i(\overline{r}) = \overline{r} \cdot \overline{h}_i = \overline{e} \cdot \overline{h}_i = s_i(\overline{e}).$$

Dermed kaldes s_i for et kendt syndrom, når $i \leq l$ og for et ukendt syndrom, når $i > l$. Hovedproblemet i dette afsnit er at finde ud af, hvordan de ukendte syndromer kan bestemmes, altså hvordan s_i bestemmes for $l < i \leq N$.

Dobbeltsyndromerne blev i forrige afsnit defineret til

$$s_{i,j}(\overline{e}) = \overline{e} \cdot \psi(f_i f_j) = \overline{e} \cdot (h_i * h_j).$$

Så længe $l(i,j) \leq l$ vil $f_i f_j \in L_l$, og da er $s_{i,j}(\overline{e}) = s_{i,j}(\overline{r})$. Det vil sige, at $s_{i,j}(\overline{e})$ er kendt for alle i, j, hvorom det gælder, at $l(i,j) \leq l$.

6.2.1 Nyttige definitioner og tilhørende lemmaer

Følgende mængde er nyttig i dette afsnit

Definition 6.2.1 (M_l-mængden) *Mængden M_l defineres således:*

$$M_l = \{(i,j) \in \mathbb{N}^2 : l(i,j) = l + 1\}.$$

Antallet af talpar i mængden M_l benævnes ν_l.

Det vil sige, at for $(i,j) \in M_l$ vil de tilsvarende $s_{i,j}$'er være de første ukendte dobbeltsyndromer, som forekommer. Da $f_1, \ldots, f_l$ er en basis for L_l og $f_i f_j$ tilhører L_l, når $l(i,j) \leq l$, gælder det, at

$$f_i f_j = \sum_{k=1}^{l} \mu_{ijk} f_k.$$

Når $(i,j) \in M_l$ vil denne sum istedet gå til $l+1$, og så vil det samtidig gælde, at $\mu_{ij(l+1)} \neq 0$.

Dette betyder ligeledes, at når $(i,j) \in M_l$, er

$$s_{i,j} = \sum_{k=1}^{l+1} \mu_{ijk} s_k = \mu_{ij(l+1)} s_{l+1} + \sum_{k=1}^{l} \mu_{ijk} s_k, \tag{6.4}$$

hvor $\mu_{ij(l+1)} \neq 0$.

Dette betyder, at alle $s_{i,j}$'erne, hvorom det gælder, at $(i,j) \in M_l$, kan skrives som en linear kombination af s_i, hvorom det gælder, at $i \leq (l+1)$, og denne linear kombination kan altid findes, og den er den samme for alle fejlvektorer. Er et $s_{i,j}$ blevet bestemt, kan resten af $s_{i,j}$'erne med (i,j) i M_l bestemmes her ud fra.

Ligning (6.4) kan desuden omskrives til

$$s_{l+1} = \frac{s_{i,j} - \sum_{k=1}^{l} \mu_{ijk} s_k}{\mu_{ij(l+1)}}. \tag{6.5}$$

Betragt nu følgende matrix:

$$S(i,j) = (s_{i',j'}(\overline{e}) : 1 \leq i' \leq i, 1 \leq j' \leq j),$$

som her er defineret udfra $\overline{e}$ i modsætning til forrige afsnit, hvor den var defineret udfra $\overline{r}$. Den ser ud på følgende måde:

$$\begin{bmatrix} s_{1,1} & \cdots & s_{1,j-1} & s_{1,j} \\ \vdots & & \vdots & \vdots \\ s_{i-1,1} & \cdots & s_{i-1,j-1} & s_{i-1,j} \\ s_{i,1} & \cdots & s_{i,j-1} & s_{i,j} = ? \end{bmatrix},$$

hvor $s_{i,j}$, som antydet, er det eneste ukendte dobbeltsyndrom, hvis $l(i,j) = l+1$, hvilket skyldes, at funktionen $l(i,j)$ er strengt voksende i begge dens argumenter, se Lemma 6.1.5.

Hvis $s_{i,j}$ kan bestemmes, kan s_{l+1} bestemmes ved hjælp af ligning (6.5), så delmålet er nu at få bestemt $s_{i,j}$ for $(i,j) \in M_l$. Hertil kræves følgende definition.

Definition 6.2.2 *Lad $(i,j) \in M_l$, hvilket vil sige, at $l(i,j) = l+1$. Da defineres følgende:*

> **Kandidat** *Hvis de tre matricer $S(i-1,j-1), S(i,j-1)$ og $S(i-1,j)$ har ens rang, kaldes talparret (i,j) for en kandidat.*
>
> **Kandidatværdi** *Hvis talparret (i,j) er en kandidat, kaldes den værdi af $s_{i,j}$, som får matricerne $S(i,j)$ og $S(i-1,j-1)$ til at have samme rang, for kandidatværdi. En kandidatværdi benævnes s'_{ij}.*
>
> **Sande kandidater** *En kandidat kaldes sand, hvis $s'_{ij} = s_{i,j}$. Antallet af sande kandidater benævnes T.*
>
> **Falske kandidater** *En kandidat kaldes falsk, hvis $s'_{ij} \neq s_{i,j}$. Antallet af falske kandidater benævnes F.*

Når en kandidatværdi skal bestemmes, ønskes det, at de to matricer $S(i,j)$ og $S(i-1,j-1)$ har samme rang. Matricen $S(i-1,j-1)$ har allerede samme rang som $S(i,j-1)$ (og $S(i-1,j)$), så rækkereduceres matricen $S(i,j-1)$ vil det ende med, at alle indgangene i den i'te række er nul. Dette betyder, når også $S(i,j)$ og $S(i-1,j-1)$ skal have samme rang, at der er en entydig værdi af s'_{ij}. Kandidatværdien kan dermed findes ved at rækkereducere $S(i,j)$, for så skal det gælde, at den (i,j)'te indgang, som stammer fra $s_{i,j}$, skal være nul.

Definition 6.2.3 *Et talpar $(i,j) \in \mathbb{N} \times \mathbb{N}$ kaldes en diskrepans, hvis matricerne $S(i-1,j-1), S(i-1,j)$ og $S(i,j-1)$ har ens rang, mens matricerne $S(i,j)$ og $S(i-1,j-1)$ ikke har samme rang.*

Er talparret (i,j) en falsk kandidat, betyder det, at matricerne $S(i,j)$ og $S(i-1,j-1)$ faktisk ikke har samme rang, hvilket er indeholdt i definitionen på

en diskrepans. Det vil sige, at en falsk kandidat er sammenfaldende med en diskrepans.

Når $S(i,j), S(i-1,j-1), S(i,j-1)$ og $S(i-1,j)$ har samme rang, betyder det, at rækkereduceres de, vil de have samme antal pivotpositioner. Har $S(i,j)$ ikke samme rang som de tre andre matricer, må det betyde, at der vil være pivotposition i den $(i,j)'$te indgang. Dermed svarer en pivotposition til en diskrepans. Følgende lemma, som stammer fra [10, Afsnit 4.2] udtaler sig om antallet af pivotpositioner og dermed om antallet af diskrepanser.

Lemma 6.2.4 *Lad $\overline{e} \in \mathbb{F}_q^n$ og lad $D(\overline{e})$ være diagonalmatricen med $\overline{e}$ i diagonalen. Lad H være den $N \times n$ matrix, som har paritetstjekket h_i som den i'te række for $1 \leq i \leq N$.*

Da gælder følgende om $S(\overline{e}) = (s_{i,j}(\overline{e}) : 1 \leq i,j \leq N)$,

$$S(\overline{e}) = HD(\overline{e})H^T \quad og \quad rang(S(\overline{e})) = \omega_H(\overline{e}),$$

hvor $\omega_H(\overline{e})$ er Hamming vægten af vektoren $\overline{e}$.

Bevis: Det gælder pr. definition, at

$$\begin{aligned} S(\overline{e}) &= (s_{i,j}(\overline{e}) : 1 \leq i,j \leq N) \\ &= (\overline{e} \cdot (\overline{h}_i * \overline{h}_j) : 1 \leq i,j \leq N) \\ &= (\textstyle\sum_{k=1}^{n} e_k h_{ik} h_{jk} : 1 \leq i,j \leq N) \\ &= HD(\overline{e})H^T \end{aligned}$$

Matricen H er valgt, så rækkerne udspænder hele $\mathbb{F}_{q^m}^n$, dermed er søjlerne uafhængige af hinanden, det vil sige, at $rang(H) =$ antal søjler $= n$. Regneregler for rang, som kan findes i [7, s. 293, opgave 9-11], giver nu, at

$$rang(S(\overline{e})) = rang(HD(\overline{e})H^T) = \omega_H(\overline{e})$$

□

Dette lemma giver, at antallet af fejl er lig rangen af $S(\overline{e})$, som er lig det totale antal af diskrepanser.

Dette benyttes i følgende lemma, som er meget vigtig i denne dekodningsproces.

Lemma 6.2.5 *Lad ν_l være antallet af talpar i mængden M_l. Hvis antallet af fejl i et modtaget ord i koden $NTP(s_l)$ er mindre end eller lig $\frac{\nu_l-1}{2}$, vil flertallet af kandidater angive den sande værdi af s_{l+1}.*

Bevis: Lad $\overline{r}$ været et modtaget ord, som højst har $\frac{\nu_l-1}{2}$ fejl, hvor l er dimensionen af dualkoden til den respektive kode $NTP(s_l)$.

Lad K benævne antallet af diskrepanser i den kendte del af matricen $S(\overline{e})$. Da alle falske kandidater falder sammen med en diskrepans, betyder dette, at

$$K + F \leq \text{ det totale antal diskrepanser } = \omega_H(\overline{e}). \tag{6.6}$$

Hvis indgangen (i, j) er en kendt diskrepans, vil det gælde, at hvis $j' > j$ vil $S(i-1, j'-1)$ og $S(i, j'-1)$ ikke have samme rang, da indgang (i, j) vil være pivotposition i $S(i, j'-1)$. Dette betyder, at alle indgange (i, j') med $j' > j$ ikke kan være kandidater. På samme måde vil det gælde, at alle indgange (i', j) med $i' > i$ ikke kan være kandidater.

Samtidig gælder det, at hvis $(i, j) \in M_l$, men ikke er en kandidat, har matricerne $S(i-1, j-1)$, $S(i-1, j)$ og $S(i, j-1)$ ikke samme rang. Dette betyder, at der vil være en diskrepans i den i'te række, den j'te søjle eller i både den i'te række og den j'te søjle.

Tilsammen giver de to ovenstående udsagn, at hver gang der er en kendt diskrepans, er der højst to ikke-kandidater. Dette giver, at

$$\text{antal ikke-kandidater} \leq 2K.$$

Antallet af kandidater blandt talparrene (i, j) i M_l er $T + F$. Dette giver alt i alt, at

$$\nu_l = \text{ antal kandidater } + \text{ antal ikke-kandidater } \leq (T + F) + 2K \tag{6.7}$$

Antagelsen om, at der er sket højst $\frac{\nu_l-1}{2}$ fejl betyder, at

$$\omega_H(\overline{e}) \leq \frac{\nu_l - 1}{2}. \tag{6.8}$$

Ved nu først at kombinere ligning (6.6) og (6.8) og heri bruge ligning (6.7), fåes følgende:

$$\begin{aligned} & K + F \leq \omega_H(\overline{e}) \leq \frac{\nu_l - 1}{2} \\ \Downarrow & \\ & K + F \leq \frac{T + F + 2K - 1}{2} \\ \Updownarrow & \\ & F + 1 \leq T \\ \Downarrow & \\ & F < T. \end{aligned}$$

Altså er antallet af sande kandidater større end antallet af falske kandidater, og da de sande kandidater alle giver den samme værdi for s_{l+1}, vil flertallet af kandidater angive den sande værdi af s_{l+1}. □

Dette lemma giver, at ved hjælp af kandidaterne er det muligt at finde alle de syndromer, som der behøves, hvis $\omega_H(\overline{e}) \leq \frac{\nu_l - 1}{s}$. Følgende lemma, som stammer fra [10, Afsnit 5] ser lidt nærmere på størrelsen ν_l.

Lemma 6.2.6 *Lad Γ være mængden af mulige vægte af polynomier og sæt $D(l) = \{(x, y) : x, y$ er gaps i Γ og $x + y = \omega(f_{l+1})\}$. Sæt $g(l) =$ antal gaps mindre end $\omega(f_l)$ i Γ. Da er*

$$\nu_l = l + 1 - g(l + 1) + \#D(l).$$

Hvis desuden $l \geq g$ er $g(l + 1) = g$, og hvis $l > 2c - g - 2$ er $g(l + 1) = g$ og $\#D(l) = 0$.

Bevis: Hold l fast og definer $A(l) = \{(x, y) \in \mathbb{N}_0 \times \mathbb{N}_0 : x + y = \omega(f_{l+1})\}$, $B(l) = \{(x, y) \in A(l) : x$ er gap$\}$ og $C(l) = \{(x, y) \in A(l) : y$ er gap$\}$. Det skal også benyttes, at $M_l = \{(i, j) \in \mathbb{N}^2 : l(i, j) = l + 1\} = \{(x, y) \in A(l) : x, y$ er nongaps$\}$. Da gælder det, at

$$A(l) = B(l) \cup C(l) \cup M_l, \quad M_l \cap (B(l) \cap C(l)) = \emptyset, \quad D(l) = B(l) \cap C(l).$$

Det betyder, at

$$\nu_l = \#M_l = \#A(l) - \#B(l) - \#C(l) + \#D(l).$$

Det ønskes nu at finde udtryk for $\#A(l), \#B(l), \#C(l)$, og også $\#D(l)$, selvom det kun er muligt under visse omstændigheder.

Da mængden $A(l)$ består af ordnede talpar fra $\mathbb{N}_0$, gælder det, at $\#A(l) = \omega(f_{l+1}) + 1$.

Lad $x \in \mathbb{N}_0$. Er $x < \omega(f_{l+1})$ vil der eksistere et entydigt $y \in \mathbb{N}_0$, så $(x, y) \in B(l)$. Da $\omega(f_{l+1})$ er et nongap, gælder det, at hvis $(x, y) \in B(l)$, så er $y \neq 0$, og dermed er $x < \omega f_{l+1}$. Dermed eksisterer der et gap $x < \omega(f_{l+1})$ hvis og kun hvis der eksisterer et entydigt y, så $(x, y) \in B(l)$. Så det gælder, at $\#B(l) = g(l + 1)$. Tilsvarede kan det vises, at $\#C(l) = g(l + 1)$.

Det gælder, at nongapet $\omega(f_l)$ er det $(\omega(f_l) + 1)$'te element af $\mathbb{N}_0$, så $\omega(f_l)$ er det $(\omega(f_l) + 1 - g(l))$'te element af mængden Γ. Dermed er

$$\begin{aligned} & l = \omega(f_l) + 1 - g(l) \\ \Updownarrow & \\ & g(l) = \omega(f_l) - l + 1. \end{aligned}$$

Det er nu muligt at lave følgende omskrivning:

$$\begin{aligned} \nu_l &= \#A(l) - \#B(l) - \#C(l) + \#D(l) \\ &= \omega(f_{l+1}) + 1 - g(l + 1) - g(l + 1) + \#D(l) \\ &= \omega(f_{l+1}) + 1 - (\omega(f_{l+1}) - (l + 1) + 1) - g(l + 1) + \#D(l) \\ &= l + 1 - g(l + 1) + \#D(l). \end{aligned}$$

Dermed er første del af lemmaet bevist. Til næste konklusion skal det benyttes, at når $l > g$, gælder det ifølge Lemma 6.1.2 (v), at $\omega(f_l) = l + g - 1$. Her antages det at være opfyldt, at $l \geq g$ og så er er $l + 1 > g$. Dermed er

$$\begin{aligned} g(l + 1) &= \omega(f_{l+1}) + 1 - (l + 1) \\ &= (l + 1) + g - 1 + 1 - (l + 1) \\ &= g \end{aligned}$$

Til sidste konklusion i lemmaet antages det at være opfyldt, at $l > 2c - g - 2$.

For en NTP-kode er det ikke muligt, at $q = 1$, så dermed er det ikke muligt, at $\omega(x) = q^{m-1} = 1^{m-1} = 1$. Dermed er det ikke muligt, at $g = 0$, for så skal det gælde, at $\omega(x) = 1$ og $\omega(y) = 2$. Derfor vil det gælde, at $g > 0$. Dette betyder, at $c \geq 2$, hvilket der kan laves følgende omskrivning på:

$$\begin{aligned} c &\geq 2 \\ &\Updownarrow \\ c - 2 - g &\geq (-g) \\ &\Updownarrow \\ 2c - g - 2 &\geq c - g, \end{aligned}$$

og da det her er antaget, at $l > 2c - g - 2$ er $l \geq c - g = g$, så det er igen opfyldt, at $g(l + 1) = g$. Det gælder ifølge Lemma 6.1.2 (v) og antagelsen om, at $l > 2c - g - 2$, at

$$\omega(f_{l+1}) = (l + 1) + g - 1 = l + g > 2c - 2. \tag{6.9}$$

Lad nu x, y være gaps, det vil sige, at $x, y \leq c - 1$ og hvis $x + y = \omega(f_{l+1})$, må det betyde, at $\omega(f_{l+1}) \leq 2c - 2$. Men dette stemmer ikke overens med ligning (6.9), så et sådan x, y kan ikke eksistere. Dermed er mængden $D(l)$ tom, når $l > 2c - g - 2$. □

6.2.2 Majoritetsalgoritmen

Nu er jeg nået frem til at opstille endnu en dekodningsalgoritme. Heri benytter jeg Lemma 6.2.6 til at omskrive grænsen for $\omega_H(\overline{e})$ i Lemma 6.2.5, selvom det giver en begrænsning på l. Det er dog muligt at vise, at følgende algoritme virker for alle l, se [10, Afsnit 6].

Algoritme 6.2.7 *[Majoritetsalgoritme] Lad det gælde, at $l > 3g - 2$, hvor $g = \frac{\left(\frac{q^m-1}{q-1}-1\right)(q^{m-1}-1)}{2}$. Denne algoritme kan da rette $\lfloor \frac{n-s_l-1}{2} \rfloor$ fejl for $NTP(s_l)$-koden.*

Input: Et modtaget ord $\overline{r}$.
Output: Fejlpositionerne i fejlvektoren $\overline{e}$.

1. *For $t = l + 1$ til $t = l + g$ gør følgende:*
   - *Opskriv den kendte del af syndrommatricen $S(\overline{e}) = (s_{i,j}(\overline{e}) : 1 \leq i, j \leq N)$ og lokaliser de dobbeltsyndromer, $s_{i,j}$, om hvilket det er opfyldt, at $l(i, j) = t$. (Dette svarer til at lokalisere de dobbeltsyndromer, som er de første ukendte dobbeltsyndromer. Dette gøres, da de alle indeholder det første ukendte syndrom, s_t).*
   - *Rækkereducer denne matrix uden at bytte om på rækkerne og ved kun at trække et multiplum af en række fra en anden række, som står længere nede i matricen.*
   - *Tilskriv s_t den værdi, som flertallet af kandidaterne angiver udfra ligning* (6.5)*, side 78.*
2. *Udfør basisalgoritmen (Algoritme 6.1.10) med koden $NTP(s - g)$.*

Lemma 6.2.5 giver sammen med Lemma 6.2.6, at så længe

$$\omega_H(\overline{e}) \leq \frac{\nu_l - 1}{2} = \frac{(l - g + 1) - 1}{2} = \frac{(n + g - s_l - 1) - g}{2} = \frac{n - s_l - 1}{2}$$

giver første punkt i algoritmen de sande værdier til de ukendte syndromer. Første punkt kunne godt gentages op til $t = N$, men når $t = l + g$ nåes, kan basisalgoritmen anvendes med koden $NTP(s - g) = NTP(s_{l+g})$, da den nu kan rette ligeså mange fejl, som majoritetsdekodningen ville kunne. Herved bestemmes fejlpositionerne og for at bestemme selve fejlvektoren, skal punkt 4. og 5. fra Algoritme 5.1.4 anvendes.

Hvis der vælges at fortsættes til $t = N$ med punkt *1.* kan fejlvektoren bestemmes direkte udfra ligningssystemet $H\overline{x} = S$, som nævnt i starten af dette afsnit.

Eksempel 6.2.8 I dette eksempel arbejdes med samme grundlag som i Eksempel 6.1.12. Her betragtes blot koden $NTP(49)$. Så bliver $l = n + g - s - 1 = 20$, $d = n - s = 15$ og $k = s + 1 - g = 44$ og majoritetsalgoritmen kan rette $\frac{d-1}{2} = 7$ fejl. Der laves derfor de samme syv fejl som i Eksempel 6.1.12. Det er nu muligt at skrive noget af syndrommatricen op. Af praktiske årsager er det blot eksponeneterne af α, som er skrevet i følgende matricen, hvor $*$ indikerer, at værdien

af dobbeltsyndromet er nul. De første ukendte dobbeltsyndromer, som vil blive bestemt ved første gennemløb af algortimen, er indikeret med et $\times$.

$$\begin{bmatrix}
9 & 14 & * & 5 & 9 & 9 & 7 & 14 & 11 & 6 & 2 & 12 & * & 4 & 5 & 5 & 12 & 7 & 7 & 6 & \times \\
14 & 5 & 9 & 7 & 14 & 11 & 2 & 12 & * & 4 & 5 & 5 & 12 & 7 & 7 & 5 & \times & & & & \\
* & 9 & 9 & 14 & 11 & 6 & 12 & * & 4 & 5 & 5 & 12 & 7 & 7 & 6 & \times & & & & & \\
5 & 7 & 14 & 2 & 12 & * & 5 & 5 & 12 & 7 & 0 & 5 & \times & & & & & & & & \\
9 & 14 & 11 & 12 & * & 4 & 5 & 12 & 7 & 7 & 5 & \times & & & & & & & & & \\
9 & 11 & 6 & * & 4 & 5 & 12 & 7 & 7 & 6 & \times & & & & & & & & & & \\
7 & 2 & 12 & 5 & 5 & 12 & 0 & 5 & \times & & & & & & & & & & & & \\
14 & 12 & * & 5 & 12 & 7 & 5 & \times & & & & & & & & & & & & & \\
11 & * & 4 & 12 & 7 & 7 & \times & & & & & & & & & & & & & & \\
6 & 4 & 5 & 7 & 7 & 6 & & & & & & & & & & & & & & & \\
2 & 5 & 5 & 0 & 5 & \times & & & & & & & & & & & & & & & \\
12 & 5 & 12 & 5 & \times & & & & & & & & & & & & & & & & \\
* & 12 & 7 & \times & & & & & & & & & & & & & & & & & \\
4 & 7 & 7 & & & & & & & & & & & & & & & & & & \\
5 & 7 & 6 & & & & & & & & & & & & & & & & & & \\
5 & 5 & \times & & & & & & & & & & & & & & & & & & \\
12 & \times & & & & & & & & & & & & & & & & & & & \\
7 & & & & & & & & & & & & & & & & & & & & \\
7 & & & & & & & & & & & & & & & & & & & & \\
6 & & & & & & & & & & & & & & & & & & & & \\
\times & & & & & & & & & & & & & & & & & & & &
\end{bmatrix}$$

Nu rækkereduceres denne matrix uden at bytte om på rækkerne og ved kun at trække et multiplum af en række fra en anden række, som står længere nede i matricen. Dette giver følgende matrix:

$$\begin{bmatrix}
9 & 14 & * & 5 & 9 & 9 & 7 & 14 & 11 & 6 & 2 & 12 & * & 4 & 5 & 5 & 12 & 7 & 7 & 6 & \times \\
* & 8 & 9 & 6 & * & 10 & 7 & 6 & 1 & 13 & 13 & 1 & 12 & 0 & 6 & 0 & \times & & & & \\
* & * & 13 & 1 & 11 & 1 & 9 & 7 & 10 & 12 & 12 & 7 & 5 & 14 & 10 & \times & & & & & \\
* & * & * & 5 & * & * & 10 & 8 & * & * & 4 & 13 & \times & & & & & & & & \\
* & * & * & * & * & * & 5 & * & * & * & 8 & \times & & & & & & & & & \\
* & * & * & * & * & * & * & * & * & * & \otimes & & & & & & & & & & \\
* & * & * & * & 5 & 0 & * & 10 & \times & & & & & & & & & & & & \\
* & * & * & * & * & * & * & \otimes & & & & & & & & & & & & & \\
* & * & * & * & * & * & \times & & & & & & & & & & & & & & \\
* & * & * & * & * & * & & & & & & & & & & & & & & & \\
* & * & * & * & * & \otimes & & & & & & & & & & & & & & & \\
* & * & * & * & \times & & & & & & & & & & & & & & & & \\
* & * & * & \times & & & & & & & & & & & & & & & & & \\
* & * & * & & & & & & & & & & & & & & & & & & \\
* & * & * & & & & & & & & & & & & & & & & & & \\
* & * & \times & & & & & & & & & & & & & & & & & & \\
* & \times & & & & & & & & & & & & & & & & & & & \\
* & & & & & & & & & & & & & & & & & & & & \\
* & & & & & & & & & & & & & & & & & & & & \\
* & & & & & & & & & & & & & & & & & & & & \\
\times & & & & & & & & & & & & & & & & & & & &
\end{bmatrix}$$

Da der netop kun er kandidatposition, hvor der ikke er pivotposition i samme række eller søjle, er det posistion (6,11), (8,8) og (11,6), som er kandidatpositioner og markeret med et $\otimes$ i ovenstående matrix. Rækkereduceringen giver, at følgende udtryk skal være lig nul:

$$s_{6,11} + \alpha^6, \quad s_{8,8} + \alpha^6, \quad s_{11,6} + \alpha^6.$$

Da det desuden gælder, at $s_{21} = s_{6,11} = s_{8,8} = s_{11,6}$, er alle tre kandidater enige om, at $s_{21} = \alpha^6$.

På samme måde bestemmes det, at $s_{22} = \alpha^3, s_{23} = \alpha^6, s_{24} = \alpha^4, s_{25} = \alpha^{11}$ og $s_{26} = \alpha^{10}$, hvilket stemmer overens med værdierne i Eksempel 6.1.12. Nu kan basisalgoritmen anvendes, og det giver selvfølgelig samme resultat, som i Eksempel 6.1.12.

Kapitel 7

Implementering

I dette kapitel vil teorien fra det foregående kapitel blive benyttet til at opstille en algoritme og en udvidelse hertil, som endnu engang kan benyttes til at bestemme fejlpositionerne i en fejlvektor. Ved at anvende denne algoritme kan det undgåes at skulle løse de ligningssystemer, som indgår i det foregående kapitel. Dette vil kunne nedsætte kompleksiteten af dekodningen, selvom det dog ikke er noget, jeg vil komme nærmere ind på.

Algoritmens vigtigste del er en delalgoritme, som skal benyttes rekursivt i den egentlige algoritme. Denne delalgoritme vil derfor blive udledt grundigt. I visse tilfælde vil der blive brug for en udvidelse til algoritmen, for at delalgoritmen kan gennemløbes et tilstrækkeligt antal gange. Denne udvidelse bliver gennemgået efter den egentlige algoritme.

7.1 Delalgoritmen

Først er der brug for nogle nye definitioner og dernæst vil et antal lemmaer føre frem til den vigtige delalgoritme.

7.1.1 Bineær operation

Tallet $l(i,j)$ blev defineret til at være det mindste heltal l, så det gælder, at $f_i f_j$ tilhører vektorrummet L_l. Dette betyder, at $f_i f_j = f_{l(i,j)}$.

Dette kan benyttes til at definere en bineær operation på $\mathbb{N}$.

Definition 7.1.1 (Bineær operation) *Lad $i, j \in \mathbb{N}$.*

Da defineres den bineære operation $\oplus$ således:

$$i \oplus j = l(i,j).$$

Det kan dermed ses, at $\omega(f_i f_j) = \omega(f_{i \oplus j})$, og det er muligt at vise følgende lemma.

Lemma 7.1.2 *Den bineære operation $\oplus$ er associativ.*

Bevis: Det skal gælde, at $(i \oplus j) \oplus k = i \oplus (j \oplus k) \; \forall \, i, j, k \in \mathbb{N}$. Det gælder, at

$$(i \oplus j) \oplus k = l(i,j) \oplus k = l(l(i,j), k). \tag{7.1}$$

Ligeledes er

$$i \oplus (j \oplus k) = i \oplus l(j,k) = l(i, l(j,k)). \tag{7.2}$$

Da det som før nævnt gælder, at $f_{l(i,j)} = f_i f_j$, er

$$\omega(f_{l(i,j)} f_k) = \omega(f_i f_j f_k) = \omega(f_i f_{l(j,k)}). \tag{7.3}$$

Ifølge ligning (7.1) og (7.2) er $(i \oplus j) \oplus k = i \oplus (j \oplus k)$ ensbetydende med, at

$$l(l(i,j), k) = l(i, l(j,k)).$$

Dette betyder, at følgende skal være opfyldt

$$\omega(f_{l(i,j)} f_k) = \omega(f_i f_{l(j,k)}).$$

Dette er opfyldt ifølge ligning (7.3), så dermed er $(i \oplus j) \oplus k = i \oplus (j \oplus k)$, hvilket var det ønskede resultat. □

Eksempel 7.1.3 Her arbejdes med samme grundlag, som i Eksempel 6.1.12 og 6.2.8. Lad $i = 3$, og $j = 5$. Det gælder, at $\omega(f_3) = 5$ og $\omega(f_5) = 9$. Da er $\omega(f_3 f_5) = \omega(f_3) + \omega(f_5) = 5 + 9 = 14$. Dermed er $3 \oplus 5 = 9$, da $\omega(f_9) = 14$.

Denne bineære operation kan dernæst benyttes til at definere en partiel orden på $\mathbb{N}$.

Definition 7.1.4 *Lad $i, j \in \mathbb{N}$.*

Da defineres den partielle orden $\leq_p$ således:

$$i \leq_p j, \text{ hvis der eksistere et } k \in \mathbb{N}, \text{ sådan at } i \oplus k = j.$$

Ovenstående k er entydig og vil blive benævnt $j \ominus i$.

Følgende lemma beviser, at den partielle orden $\leq_p$ rent faktisk er en ordensrelation.

Lemma 7.1.5 *Den partielle orden $\leq_p$ er reflektiv, transitativ og antisymmetrisk.*

Bevis:

Reflektiv: Det skal gælde, at $i \leq_p i \ \forall\, i \in \mathbb{N}$, det vil sige, der skal findes et k, sådan at $i \oplus k = i$.

Da det altid vil gælde, at $\omega(f_1) = 0$, vil $k = 1$ opfylde, at $i \oplus k = i$ for alle $i \in \mathbb{N}$.

Transitativ: Det skal gælde, at når $i \leq_p j$ og $j \leq_p n$, så er $i \leq_p n$ for alle $i, j, n \in \mathbb{N}$.

At $i \leq_p j$ og $j \leq_p n$ betyder, at der eksisterer $k_1, k_2 \in \mathbb{N}$, så

$$\begin{aligned} i \oplus k_1 &= j &&= l(i, k_1) \quad \text{og} \\ j \oplus k_2 &= n &&= l(j, k_2). \end{aligned}$$

Dette betyder, at

$$\begin{aligned} \omega(f_j) &= \omega(f_{i\oplus k_1}) = \omega(f_i f_{k_1}) = \omega(f_i) + \omega(f_{k_1}) \quad \text{og} \\ \omega(f_n) &= \omega(f_{i\oplus k_2}) = \omega(f_j f_{k_2}) = \omega(f_j) + \omega(f_{k_2}). \end{aligned}$$

Dette kan sammensættes, så $\omega(f_n) = \omega(f_i) + \omega(f_{k_1}) + \omega(f_{k_2}) = \omega(f_i) + \omega(f_{k_1} f_{k_2})$. Dermed vil $f_{k_3} = f_{k_1} f_{k_2}$ opfylde, at $i \oplus k_3 = n$, så dermed er $i \leq_p n$.

Antisymmetrisk: Det skal gælde, at når $i \leq_p j$ og $j \leq_p i$, medfører det, at $i = j$ for alle $i, j \in \mathbb{N}$.

At $i \leq_p j$ og $j \leq_p i$ betyder, at der eksisterer $k_3, k_4 \in \mathbb{N}$, så

$$\begin{aligned} i \oplus k_3 &= j = l(i, k_3) \quad \text{og} \\ j \oplus k_4 &= i = l(j, k_4). \end{aligned} \tag{7.4}$$

Dette betyder, at

$$\begin{aligned} \omega(f_j) &= \omega(f_i) + \omega(f_{k_3}) \quad \text{og} \\ \omega(f_i) &= \omega(f_j) + \omega(f_{k_4}). \end{aligned}$$

Sammensættes dette fåes, at $\omega(f_j) = \omega(f_j) + \omega(f_{k_3}) + \omega(f_{k_4})$. Da vægten af et polynomium tilhører $\mathbb{N}_0$, må det betyde, at $\omega(f_{k_3}) = \omega(f_{k_4}) = 0$. Dermed er $k_3 = k_4 = 1$. Indsættes dette nu i ligning (7.4) fåes, at $i \oplus 1 = i = j$, hvilket netop var det ønskede resultat.

□

Eksempel 7.1.6 Igen er her samme grundlag, som i Eksempel 6.1.12 og 6.2.8. Det gælder, at $4 \leq_p 7$, da $4 \oplus 2 = 7$. Men det gælder samtidig, at $3 \not\leq_p 4$, for der findes ikke noget k, så $3 \oplus k = 4$, da der ikke findes noget monomium med vægt 3, som er forskellen i vægt på f_3 og f_4.

7.1.2 $Span(f)$ og $fail(f)$

I dette afsnit vil der blive defineret to grundlæggende begreber, $span(f)$ og $fail(f)$, og bevist en række lemmaer om disse. Gennem afsnittet anvendes funktionen $S_{\overline{e}}$, se Defintion 6.1.11. Her holdes $\overline{e}$ dog fast og derfor undlades subscript $\overline{e}$ ved S-funktionen. Det vil sige, at

$$S(f) = S_{\overline{e}}(f).$$

Ligesom i afsnit 4.1 er $J = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y \rangle$.

Definition 7.1.7 *Lad $f \in \mathbb{F}_{q^m}[x,y]/J$, så $\omega(f) = \omega(f_j)$. Da defineres*

$$span(f) = i, \quad hvis\ S(ff_i) \neq 0,\ mens\ S(ff_k) = 0\ \forall\ k < i$$
$$og$$
$$fail(f) = span(f) \oplus j.$$

Udfra definitionen på $K_{i,j}(\overline{r})$ side 71 kan det ses, at $span(f) = i$ er det størst mulige tal, så f er med i vektorrummet $K_{i-1,j}(\overline{e})$. Ligeledes vil det gælde, at hvis $fail(f) = k$, så er $\omega(f_k)$ den mindste vægt, for hvilke det gælder, at et multiplum af f har denne vægt og et syndrom forskellig fra nul.

Følgende to lemmaer beviser relationer om *span* og $fail$, som vil blive benyttet i de følgende afsnit.

Lemma 7.1.8 *Lad $f \in \mathbb{F}_{q^m}[x,y]/J$, så $\omega(f) = \omega(f_k)$ og $span(f) = i$. Hvis det gælder, at $g \in \mathbb{F}_{q^m}[x,y]/J$, så $j \leq_p i$ og $\omega(g) = \omega(f_{i \ominus j})$, så er*

$$span(g) \leq k \oplus j$$
$$fail(g) \leq i \oplus k = fail(f).$$

Bevis: Når $\omega(g) = \omega(f_{i \ominus j})$ er $\omega(gf_j) = \omega(f_{(i \ominus j) \oplus j}) = \omega(f_i)$. Da $span(f) = i$, betyder det dermed, at $S(f(gf_j)) \neq 0$. Det gælder, at $S(g(ff_j)) = S(f(gf_j)) \neq 0$, så det må gælde, at $span(g)$ er mindre end det indeks, som svarer til vægten af ff_j. Da $\omega(ff_j) = \omega(f_{k \oplus j})$, gælder det dermed, at

$$span(g) \leq k \oplus j.$$

Hermed bliver

$$\begin{aligned} fail(g) &= span(g) \oplus (i \ominus j) \\ &\leq k \oplus j \oplus i \ominus j = k \oplus i = fail(f). \end{aligned}$$

□

Lemma 7.1.9 *Lad $f \in \mathbb{F}_{q^m}[x,y]/J$, så $\omega(f) = \omega(f_k)$ og $span(f) = i$. Lad ligeledes $g \in \mathbb{F}_{q^m}[x,y]/J$, så $\omega(g) = \omega(f_j)$. Så gælder følgende:*

(*i*) *Hvis $j \leq_p i$, så er*

$$span(fg) = i \ominus j \text{ og } fail(fg) = k \oplus j = fail(f).$$

(*ii*) *Hvis istedet $j \not\leq_p i$, så er*

$$span(fg) > m \,\forall\, m, \text{ hvorom det gælder, at } j \oplus m < i$$

og så er

$$fail(fg) > k \oplus i.$$

Bevis: Når $span(f) = i$, betyder det, at hvis

$$\omega(gf_n) = \omega(f_i), \text{ så er } S(f(gf_n)) \neq 0.$$

Samtidig hvis $k < n$, så er $\omega(gf_k) < \omega(gf_n) = \omega(f_i)$, og dermed vil det gælde, at

$$\omega(gf_k) < \omega(f_i), \text{ og så er } S(f(gf_k)) = 0.$$

Det gælder, at $S(f(gf_n)) = S((fg)f_n) \neq 0$ og ligeledes er $S(f(gf_k)) = S((fg)f_k) = 0$ for alle $k < n$. Dermed kan det konkluderes, at $span(fg) = n$.

(*i*)**:** Her er $j \leq_p i$, hvilket betyder, at der eksisterer et n, så $j \oplus n = i$. Dermed gælder det, at $\omega(gf_n) = \omega(f_{j \oplus n}) = \omega(f_i)$, og så er $span(fg) = i \ominus j$. Det medfører, at $fail(fg) = span(fg) \oplus (k \oplus j) = i \ominus j \oplus k \oplus j = i \oplus k$.

(*ii*)**:** Her gælder det istedet, at $j \not\leq_p i$, så nu eksisterer der ikke noget n', så $j \oplus n' = i$. Dermed kan det kun konkluderes, at $span(fg) > m$ for alle m, hvorom det gælder, at $j \oplus m < i$.
Tilbage er nu udsagnet om $fail(fg)$. Dette bevises med et modstridsbevis. Hertil benyttes det, at $\omega(fg) = \omega(f_{k \oplus j})$. Lad nu $span(fg) = h$ og antag, at $fail(fg) \leq k \oplus i$. Pr. definition er $fail(fg) = h \oplus k \oplus j$. Udfra antagelsen vil det da gælde, at

$$\begin{aligned} & h \oplus k \oplus j \leq k \oplus i \\ \Downarrow & \\ & h \oplus j \leq i, \end{aligned}$$

men da $j \not\leq_p i$, så eksisterer der ikke noget h, så $j \oplus h = i$, det vil sige, at

$$h \oplus j < i.$$

Dette er netop betingelsen for, at første del i dette punkt kan benyttes til at konkludere, at $span(fg) > h$, men dette strider imod, at $span(fg) = h$, så antalgelsen om, at $fail(fg) \leq k \oplus i$ holder ikke. Dermed er $fail(fg) > k \oplus i$.

□

7.1.3 Lemmaer frem mod delalgoritmen

Ideen i delalgortimen er at dele de naturlige tal op i nogle passende mængder, hvorefter det herudfra er muligt at bestemme et fejllokaliserende polynomium. I dette afsnit vil disse mængder blive defineret og gennem en række lemmaer vil en del egenskaber ved disse mængder blive præsenteret, så disse er kendt, når delalgoritmen skal præsenteres og bevises.

Definition 7.1.10 *Lad $l \in \mathbb{N}$. Da defineres følgende mængder:*

$$\begin{aligned}
\Sigma_l &= \{i \in \mathbb{N} : \exists\, f \in \mathbb{F}_{q^m}[x,y]/J \text{ sådan at } \omega(f) = \omega(f_i) \text{ og } fail(f) > l\} \\
\sigma_l &= \text{ mængden af minimale elementer i } \Sigma_l \text{ taget med hensyn til } \leq_p \\
\Delta_l &= \{span(f) : f \in \mathbb{F}_{q^m}[x,y]/J, fail(f) \leq l\} \\
\delta_i &= \text{ mængden af maksimale elementer i } \Delta_l \text{ taget med hensyn til } \leq_p .
\end{aligned}$$

Lemma 7.1.11

$$\Sigma_l \cap \Delta_l = \emptyset.$$

Bevis: Lad $i \in \Delta_l$. Det vil sige, at der eksisterer et f i $\mathbb{F}_{q^m}[x,y]/J$, så $span(f) = i$ og $fail(f) \leq l$. Lad nu g tilhøre $\mathbb{F}_{q^m}[x,y]/J$, sådan at $\omega(g) = \omega(f_i)$. Ved nu at benytte Lemma 7.1.8 med $j = 1$ fåes, at $fail(g) \leq fail(f) \leq l$. Dermed kan i ikke tilhøre Σ_l. □

Det ønskes også bevist, at $\Sigma_l \cup \Delta_l = \mathbb{N}$, men dette er ikke så enkelt som ovenstående bevis, så derfor bevises nogle lemmaer og nogle definitioner præsenteres, før dette tages op igen. For at kunne løse ovenstående problem, gives følgende definition, som også viser sig at være meget brugbar i delalgoritmen.

Definition 7.1.12 ($Info_l$) *Lad F_l og G_l være følgende afbildninger:*

$$F_l : \sigma_l \to \mathbb{F}_{q^m}[x,y]/J \quad og \quad G_l : \delta_l \to \mathbb{F}_{q^m}[x,y]/J,$$

hvorom det gælder, at $f = F_l(i)$ er et element i $\mathbb{F}_{q^m}[x,y]/J$, så $\omega(f) = \omega(f_i)$ og $fail(f) > l$, og $g = G_l(i)$ er et element i $\mathbb{F}_{q^m}[x,y]/J$, så $span(g) = i$ og $fail(g) \leq l$. Da er

$$Info_l = \{\sigma_l, \delta_l, Im(F_l), Im(G_l)\},$$

hvor $Im(F_l) = \{F_l(i) : i \in \sigma_l\}$ og $Im(F_l) = \{G_l(i) : i \in \delta_l\}$.

Det vil senere vise sig, at $Info_l$ kan findes udfra $Info_{l-1}$. Denne egenskab vil blive anvendt i delalgoritmen.

Følgende lemma leder hen til en forståelse af, hvordan mængderne Σ_l og Δ_l ændres, når l vokser.

Lemma 7.1.13 *Lad $j \leq_p i$, så gælder følgende:*

(*i*) *Hvis $j \in \Sigma_l$, så vil $i \in \Sigma_l$.*

(*ii*) *Hvis $i \in \Delta_l$, så vil $j \in \Delta_l$.*

Bevis:

(*i*)**:** Når $j \in \Sigma_l$ betyder det, at der eksisterer et f i $\mathbb{F}_{q^m}[x,y]/J$, så $\omega(f) = \omega(f_j)$ og $fail(f) > l$. Hvis $j \leq_p i$, så eksisterer $f_{i \ominus j}$ og $\omega(ff_{i\ominus j}) = \omega(f_{j \oplus i \ominus j}) = \omega(f_i)$. Ved at benytte Lemma 7.1.9(*i*) kan det desuden ses, at $fail(ff_{i\ominus j}) = fail(f) > l$. Dermed eksisterer der et polynomium, nemlig $ff_{i\ominus j}$, hvorom det gælder, at $\omega(ff_{i\ominus j}) = \omega(f_i)$ og $fail(ff_{i\ominus j}) > l$. Dette er netop betingelsen for, at $i \in \Sigma_l$.

(*ii*)**:** Når $i \in \Delta_l$ betyder det, at der eksisterer et f i $\mathbb{F}_{q^m}[x,y]/J$, så $span(f) = i$ og $fail(f) \leq l$. Hvis $j \leq_p i$, så eksisterer $f_{i\ominus j}$ og ved igen at benytte Lemma 7.1.9(*i*), kan det ses, at $span(ff_{i\ominus j}) = i \ominus (i \ominus j) = j$ og desuden er $fail(ff_{i\ominus j}) = fail(f) \leq l$. Dermed eksisterer der et polynomium, nemlig $ff_{i\ominus j}$, hvorom det gælder, at $span(ff_{i\ominus j}) = j$ og $fail(ff_{i\ominus j}) \leq l$. Dette er netop betingelsen for, at $j \in \Delta_l$.

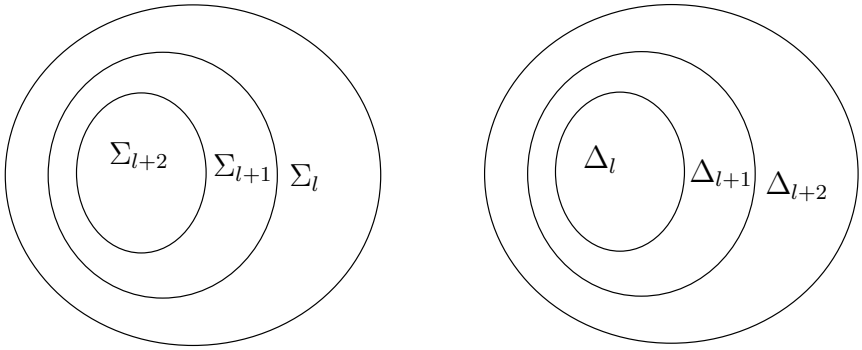
□

Lemma 7.1.13 giver et billede af, hvordan henholdsvis Σ-inddelingen og Δ-inddelingen udvikler sig, når l ændres, hvilket er illustreret på figur 7.1.

Dermed kan elementerne i mængderne bestemmes udfra deres tilhørende mængder af minimale/maksimale elementer på følgende måde:

$$\begin{aligned} \Sigma_l &= \{i \in \mathbb{N} : \exists\, j \in \sigma_l \text{ så } j \leq_p i\} \\ \Delta_l &= \{j \in \mathbb{N} : \exists\, i \in \delta_l \text{ så } j \leq_p i\}. \end{aligned} \tag{7.5}$$

Efterfølgende lemma benyttes direkte i den kommende delalgoritme, når F_l skal findes udfra F_{l-1}.



Figur 7.1: *Illustration af, hvorledes udviklingen af* Σ- *og* Δ-*mængderne foregår.*

Lemma 7.1.14 *Lad* $f, f', g, g' \in \mathbb{F}_{q^m}[x,y]/J$*, så følgende er opfyldt:*

$$\omega(f) = \omega(f_k), \quad \omega(f') = \omega(f_{k'}), \quad \omega(g) = \omega(f_i) \quad og \quad \omega(g') = \omega(f_{i'}),$$

$$span(f) = l, \quad span(f') = l', \quad så \quad fail(f) = l \oplus k \quad og \quad fail(f') = l' \oplus k'.$$

Desuden skal det gælde, at

$$k \oplus l > k' \oplus l', \quad i \leq_p l, \quad i' \leq_p l' \quad og \quad l \ominus i = l' \ominus i'.$$

Sæt $h' = f_{l \ominus i}$*. Da vil* $\mu = -\frac{S(fgh')}{S(f'g'h')}$ *medfører, at* $h = fg + \mu f'g'$ *opfylder, at*

$$\omega(h) = \omega(f_{k \oplus i}), \quad span(h) > l \ominus i \quad og \quad fail(h) > k \oplus l.$$

Bevis: Pr. definition er $\omega(fg) = \omega(f_{k \oplus i})$ og $\omega(\mu f'g') = \omega(f_{k' \oplus i'})$. Udfra antagelserne om, at $l \ominus i = l' \ominus i'$ og $k \oplus l > k' \oplus l'$ gælder det, at

$$\begin{aligned} k \oplus i &= k \oplus (l \ominus l' \oplus i') \\ &> k' \oplus l' \ominus l' \oplus i' = k' \oplus i'. \end{aligned}$$

Det vil sige, at $\omega(h) = \omega(f_{k \oplus i})$ for alle $\mu \in \mathbb{F}_{q^m}^*$.

Lad nu $\lambda = S(fgh')$ og $\lambda' = S(f'g'h')$. Da $\omega(gh') = \omega(f_{i \oplus l \ominus i}) = \omega(f_l)$ og $\omega(g'h') = \omega(f_{i' \oplus l' \ominus i'}) = \omega(f'_l)$ giver det, sammen med at $span(f) = l$ og $span(f') = l'$, at hverken λ eller λ' er nul.

Sæt dernæst $\mu = -\frac{\lambda}{\lambda'}$. Dette giver det ønskede resultat, hvilket vises i det følgende.

Ved at benytte Lemma 7.1.9(i), kan det ses, at $span(fg) = l \ominus i$ og $span(f'g') = l' \ominus i' = l \ominus i$. Så hvis $j < l \ominus i$ er

$$\begin{aligned} S((fg + \mu f'g')f_j) &= S(fgf_j + \mu f'g'f_j) \\ &= S(fgf_j) + \mu S(f'g'f_j) = 0 - 0 = 0 \end{aligned}$$

Hvis istedet $j = l \ominus i$ er

$$\begin{aligned} \lambda' S((fg - \frac{\lambda}{\lambda'} f'g')f_j) &= \lambda' S((fg - \frac{\lambda}{\lambda'} f'g')f_{l \ominus i}) \\ &= S((\lambda' fg - \lambda f'g')f_{l \ominus i}) \\ &= \lambda' S(fgf_{l \ominus i}) - \lambda S(f'g'f_{l \ominus i}) \\ &= S(f'g'f_{l \ominus i})S(fgf_{l \ominus i}) - S(fgf_{l \ominus i})S(f'g'f_{l \ominus i}) \\ &= 0. \end{aligned}$$

Det er konkluderet, at $\lambda' \neq 0$, så det betyder, at $S((fg - \frac{\lambda}{\lambda'} f'g')f_{l \ominus i}) = 0$. Dermed er $S(hf_j) = 0$ for $j \leq l \ominus i$, så

$$span(h) > l \ominus i.$$

Dette medfører pr. definition, at

$$\begin{aligned} & fail(h) = span(h) \oplus k \oplus i > l \ominus i \oplus k \oplus i \\ \Downarrow \\ & fail(h) > l \oplus k. \end{aligned}$$

□

7.1.4 Delalgoritme

Delalgoritme, som er det vigtigste redskab i den egentlige algoritme, finder $Info_l$ udfra $Info_{l-1}$. Denne delalgoritme vil blive formuleret i dette afsnit, men for

overskuelighedens skyld vil mange af elementerne, som indgår heri, blive behandlet først, da dette vil belyse, hvorfor algoritmen opstilles, som den gør. Herigennem vil det også blive bevist, at $\Sigma_l \cup \Delta_l = \mathbb{N}$. Til dette formål anvendes induktion, hvor basis er $\delta_0 = \emptyset, \sigma_0 = \{1\}, F_0(1) = 1$, og $G_0(\emptyset) = \emptyset$. Da er $\Sigma_0 = \mathbb{N}$ og $\Delta_0 = \emptyset$. Induktionsantagelsen er så, at $\Sigma_v \cup \Delta_v = \mathbb{N}$ for v op til $l-1$, og det skal så bevises for $v = l$.

Først præsenteres en definition og nogle lemmaer bevises.

Definition 7.1.15

$$\begin{aligned}
\delta'_l &= \{span(f) : f \in Im(F_{l-1}) \text{ og } fail(f) = l\} \\
\Delta'_l &= \{i \ominus j : i \in \delta'_l, j \leq_p i\} \cup \Delta_{l-1} \\
\sigma'_l &= \text{ mængden af minimale elementer } i \, \mathbb{N} \setminus \Delta'_l \text{ taget med hensyn til } \leq_p .
\end{aligned}$$

Det viser sig, at nogle af disse mængder er sammenfaldende med mængderne fra Definition 7.1.10. For at komme til den konklusion bevises først følgende lemma.

Lemma 7.1.16

$$\Delta'_l \subseteq \Delta_l.$$

Bevis: Fra Lemma 7.1.13 vides det, at $\Delta_{l-1} \subseteq \Delta_l$, så det mangler at blive bevist, at også $\{i \ominus j : i \in \delta'_l, j \leq_p i\} \subseteq \Delta_l$.

Lad $i \in \delta'_l$, det vil sige, at der eksisterer et f i $\mathbb{F}_{q^m}[x,y]/J$, så $span(f) = i$, $fail(f) = l$ og $f = F_{l-1}(k)$, hvor $k \in \sigma_{l-1}$, hvilket betyder, at $\omega(f) = \omega(f_k)$.

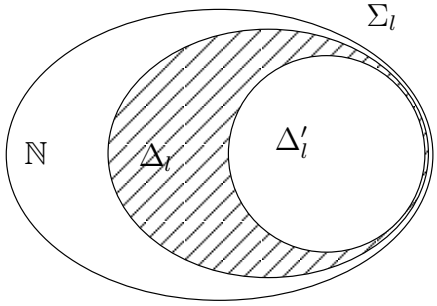
Det vides, at $j \leq_p i$, det vil sige, det er muligt at benytte Lemma 7.1.9(i), hvormed det kan konkluderes, at

$$span(ff_j) = i \ominus j \quad \text{og} \quad fail(ff_j) = k \oplus j = fail(f) = l.$$

Dette betyder, at elementet $i \ominus j$ fra mængden $\{i \ominus j : i \in \delta'_l, j \leq_p i\}$ er lig $span(ff_j)$. Samtidig gælder det, at $fail(ff_j) = l \leq l$. Dette er netop betingelserne for at tilhøre Δ_l. □

I delalgoritmen vil der for alle $i \in \sigma'_l$ blive konstrueret en funktion f, hvorom

det gælder, at $\omega(f) = \omega(f_i)$ og $fail(f) > l$. Dermed vil det gælde, at $\sigma'_l \subseteq \Sigma_l$. Da σ'_l er minimale elementer i $\mathbb{N} \setminus \Delta'_l$, giver Lemma 7.1.13, at det også må gælde, at $\mathbb{N} \setminus \Delta'_l \subseteq \Sigma_l$. Det er netop bevist, at $\Delta'_l \subseteq \Delta_l$, så $\mathbb{N} \setminus \Delta_l \subseteq \mathbb{N} \setminus \Delta'_l$. Det vil sige, at $\mathbb{N} \setminus \Delta_l \subseteq \Sigma_l$. Det blev vist i Lemma 7.1.11, at $\Sigma_l \cap \Delta_l = \emptyset$, så der er ikke plads til, at der er elementer i $\Delta_l \setminus \Delta'_l$. Dette er illustreret på figur 7.2. Dette betyder,



Figur 7.2: *Illustration af, at Δ'_l og Δ_l er sammenfaldende. Det skraverede område er tomt.*

at $\Delta_l = \Delta'_l$ og at $\Sigma_l = \mathbb{N} \setminus \Delta_l$. Dette giver igen, at $\Sigma_l \cup \Delta_l = \mathbb{N}$, at $\sigma'_l = \sigma_l$ og at δ_l også er mængden af maksimale elementer i Δ'_l. Udfra beskrivelsen af δ'_l kan det ses, at δ_l er indeholdt i $(\delta_{l-1} \cup \delta'_l)$. Disse to mængder vil muligvis indeholde for meget, da der er måske er et j i δ_{l-1} og et j' i δ'_l, så $j \leq_p j'$. Da skal j ikke være med i δ_l, da den kun skal indeholde maksimale elementer taget med hensyn til $\leq_p$. Dermed gælder det, at

$$\delta_l = \delta'_l \cup \{j \in \delta_{l-1} : j \not\leq_p j' \, \forall \, j' \in \delta'_l\}, \tag{7.6}$$

da disse to mængder ikke vil overlappe hinanden.

Det foregående gælder kun, når der for alle $i \in \sigma'_l$ kan konstrueres en funktion, så $\omega(f) = \omega(f_i)$ og $fail(f) > l$. Dette skal derfor beskrives, men først vil der lige blive vist endnu et lemma.

Lemma 7.1.17 *Lad $i \in \sigma'_l$. Da vil det gælde, at*

(*i*) *$i = k \oplus j$ for et $k \in \sigma_{l-1}$.*

(*ii*) *Lad $f = F_{l-1}(k)$. Hvis $fail(f) = l$ og $i \leq_p l$ gælder det, at $l \ominus i \notin \Sigma_{l-1}$.*

Bevis:

(i)**:** Når $i \in \sigma'_l$ betyder det pr. definition, at $i \in \mathbb{N} \setminus \Delta'_l$. Da det pr. definition gælder, at $\Delta_{l-1} \subseteq \Delta'_l$ vil det gælde, at $\mathbb{N} \setminus \Delta'_l \subseteq \mathbb{N} \setminus \Delta_{l-1} = \Sigma_{l-1}$, hvor det sidste lighedstegn kommer udfra induktionsantagelsen. Altså vil $i \in \Sigma_{l-1}$, hvilket udfra det øverste udsagn i ligning (7.5) side 97 giver, at $i = k \oplus j$ for et $k \in \sigma_{l-1}$.

(ii)**:** Lad $f = F_{l-1}(k)$ og benævn $span(f) = m$. Dermed er $fail(f) = m \oplus k = m \oplus i \ominus j$. Hvis $fail(f) = l$ og $i \leq_p l$ ønskes det bevist, at $l \ominus i \notin \Sigma_{l-1}$. Dette gøres ved et modstridsbevis. Det antages hermed, at $l \ominus i \in \Sigma_{l-1}$. Det vil sige, at $l \ominus i = k' \oplus j'$ for et $k' \in \sigma_{l-1}$. Lad nu $g = F_{l-1}(k')$, det vil sige, $\omega(g) = \omega(f_{k'})$ og $fail(g) > l - 1 \geq l$. Da $i = k \oplus j$ og $l = m \oplus k$ gælder det, at

$$k' = l \ominus i \ominus j' = m \oplus k \ominus (k \oplus j) \ominus j' = m \ominus (j \oplus j') = m \ominus j''.$$

Det betyder, at $j'' \leq_p m = span(f)$, og at $\omega(g) = \omega(f_{m \ominus j''})$ så nu kan Lemma 7.1.8 benyttes til at konkludere, at $fail(g) \leq fail(f) = l$. Valget af g gav, at $fail(g) \geq l$, så det må gælde, at

$$\begin{aligned} & fail(g) = l = span(g) \oplus k' \\ \Downarrow \\ & span(g) = l \ominus k' = l \ominus (l \ominus i \ominus j') = i \oplus j'. \end{aligned}$$

Dette betyder, at $i \oplus j' \in \delta'_l$, så $i \oplus j' \in \Delta'_l$, men da $i \leq_p i \oplus j$, så kan i ikke være maksimal element i $\mathbb{N} \setminus \Delta'_l$ og dermed kan i ikke tilhører σ'_l, som gjaldt helt fra starten. Dermed er der nået en modstrid, så når $fail(f) = l$, vil $l \ominus i \notin \Sigma_{l-1}$.

□

Det er nu muligt at beskrive, hvorledes der for et hvert i i σ'_l vil kunne konstrueres en funktion f, så $\omega(f) = \omega(f_i)$ og $failf > l$. Det deles i to tilfælde, i begge tilfælde tilhører i mængden σ'_l.

(1) $i \in \sigma_{l-1}$. Lad $f = F_{l-1}(i)$, det vil sige, $\omega(f) = \omega(f_i)$ og $fail(f) > l-1 \geq l$. Hvis $fail(f) > l$, sættes $F_l(i) = f$. At $fail(f) = span(f) \oplus i > l$ betyder, at enten er $i \not\leq_p l$ eller også er $i \leq_p l$, mens det er opfyldt, at $span(f) > l \ominus i$, hvilket giver, at $S(f f_{l \ominus i}) = 0$.

Hvis $fail(f) = l = span(f) \oplus i$, giver Lemma 7.1.17($ii$), at $l \ominus i \notin \Sigma_{l-1}$ (Her er $k = i$). Da induktionsantagelsen giver, at $\Sigma_{l-1} \cup \Delta_{l-1} = \mathbb{N}$, vil $l \ominus i \in \Delta_{l-1}$. Det vil sige, at der findes et l' i δ_{l-1} og et i' i $\mathbb{N}$, så

$$l \ominus i = l' \ominus i'.$$

Sæt nu $f' = G_{l-1}(l')$, og lad $\omega(f') = \omega(f_{k'})$, så er $span(f') = l'$ og $fail(f') = l' \oplus k' \leq l-1$. Sæt desuden $g = 1$ og $g' = f_{i'}$. Det ønskes nu at benytte Lemma 7.1.14, men dertil skal betingelserne først være opfyldt. Det skal gælde, at $fail(f) > fail(f')$, det vil sige, at $l > k' \oplus l'$. Dette er opfyldt, da $l' \oplus k' \leq l-1$. Det skal også gælde, at $1 \leq_p span(f) = l \ominus i$, hvilket er opfyldt, da 1 er mindre end eller lig alle naturlige tal, også med hensyn til $\leq_p$. Det skal desuden gælde, at $i' \leq_p l'$ og at $(l \ominus i) \ominus 1 = l' \ominus i'$, hvilket er opfyldt ved valg af de to tal l' og i'. (Tallet $l' \ominus i'$ eksisterer kun, hvis $i' \leq_p l'$). Da giver Lemma 7.1.14, at der findes et $\mu \in \mathbb{F}_{q^m}^*$, så $h = fg + \mu f'g'$ opfylder, at $\omega(h) = \omega(f_{i \oplus 1}) = \omega(f_i)$ og at $fail(h) > i \oplus l \ominus i = l$, så da sættes $F_l(i) = h$.

(2) $i \notin \sigma_{l-1}$. I følge Lemma 7.1.17(i) er $i = k \oplus j$, hvor $k \in \sigma_{l-1}$ (her vil j være større end 1). Sæt $f = F_{l-1}(k)$, det vil sige, at $\omega(f) = \omega(f_k)$ og $fail(f) > l-1 \geq l$. Sæt desuden $g = f_j$. Så er $\omega(fg) = \omega(f_{k \oplus j}) = \omega(f_i)$.

Det gælder, at i er minimal element i $\mathbb{N}/\Delta_l'$ og da $k \leq_p i$, må det gælde, at $k \in \Delta_l' \subseteq \Delta_l$. Det betyder, at $fail(f) \leq l$, så dermed vil $fail(f)$ være lig l. Dermed vil enten $i \not\leq_p l$ eller også vil $l \ominus i \notin \Sigma_{l-1}$, og da vil $l \ominus i \in \Delta_{l-1}$ (ligesom i tilfælde **(1)**).

$i \not\leq_p l$: Det ønskes, at benytte Lemma 7.1.9(ii). Da skal det være opfyldt, at $j \not\leq_p span(f) = l \ominus k$. Det gælder, at $j = i \ominus k$, så det skal altså være opfyldt, at $i \ominus k \not\leq_p l \ominus k$, hvilket netop er opfyldt under dette punkt, hvor $i \not\leq_p l$. Derfor kan Lemma 7.1.9 (ii) nu benyttes til at konkludere, at $fail(fg) > k \oplus l \ominus k = l$, så da sættes $F_l(i) = fg$.

$l \ominus i \in \Delta_{l-1}$: Her vil der eksistere et $l' \in \delta_{l-1}$ og et $i' \in \mathbb{N}$, så $l \ominus i = l' \ominus i'$. Sæt nu $f' = G_{l-1}(l'), g' = f_{i'}$. Nu ønskes det igen at benytte Lemma 7.1.14. Valgene er, på nær g, ligesom under punkt **(1)**, så det er kun

to af betingelserne, det er nødvendigt at tjekke her. Det skal her gælde, at $j \leq_p l \ominus k$. Da $j = i \ominus k$, skal det altså være opfyldt, at $i \ominus k \leq_p l \ominus k$, hvilket er opfyldt, da tallet $l \ominus i$ eksisterer og dermed er $i \leq_p l$. Derudover skal det gælde, at $(l \ominus k) \ominus j = l' \ominus i'$. Da $i = k \oplus j$, er $(l \ominus k) \ominus j = l \ominus (k \oplus j) = l \ominus i$, så denne betingelse er også opfyldt. Så Lemma 7.1.14 giver, at der eksisterer et $\mu \in \mathbb{F}_{q^m}^*$, så $h = fg + \mu f'g'$ opfylder, at $\omega(h) = \omega(f_{k \oplus j}) = \omega(f_i)$ og $fail(h) > k \oplus l \ominus k = l$, så da sættes $F_l(i) = h$.

Dermed er det nu for alle i i σ_l' gjort muligt at finde en funktion f, så $\omega(f) = \omega(f_i)$ og $fail(f) > l$, det vil sige, det er beskrevet, hvordan F_l kan findes fra F_{l-1}. Der er blevet argumenteret for, at $\sigma_l = \sigma_l'$ og i ligning (7.6), side 101 er δ_l blevet beskrevet. Tilbage er at få beskrevet hvordan G_l skal findes udfra G_{l-1} (eller $Info_{l-1}$). Elementerne i δ_l, for hvilke G_l skal bestemmes, tilhører enten δ_{l-1} eller δ_l'. Bestemmelsen af $G_l(i)$ deles derfor i to tilfælde.

$j \in \delta_{l-1}$**:** Da sættes $G_l(j) = G_{l-1}(j)$, fordi $span(G_{l-1}(j)) = j$ og $fail(G_{l-1}(j)) \leq (l-1) \leq l$, hvilke er krævene til $G_l(j)$.

$j \in \delta_l'$**:** Da sættes $G_l(j) = F_{l-1}(l \ominus j)$. At dette opfylder de ønskede krav, ses af følgende overvejelser. Når $j \in \delta_l'$ vil der eksistere et polynomium, f, så $span(f) = j$ og $fail(f) = l$. Desuden vil det pr. defintion gælde, at for et k i σ_{l-1} er dette $f = F_{l-1}(k)$. Dette betyder, at $\omega(f) = \omega(f_k)$, og så er $fail(f) = j \oplus k = l$, så det gælder, at $l \ominus j = k$, så tallet $l \ominus j$ eksisterer og tilhører σ_{l-1}. Dermed giver det mening at anvende $F_{l-1}(l \ominus j)$. Det vides derfor nu, at $f = F_{l-1}(k) = F_{l-1}(l \ominus j)$, så $span(F_{l-1}(l \ominus j)) = span(F_{l-1}(k)) = j$ og $fail(F_{l-1}(l \ominus j)) = fail(F_{l-1}(k)) = l \leq l$, hvilke er krævene til $G_l(j)$.

Det er nu muligt at opstille delalgoritmen.

Algoritme 7.1.18 (Delalgoritme)
Startværdier: $\delta_0 = \emptyset, \sigma_0 = \{1\}, F_0 = \{1\}, G_0 = \emptyset$.
Input: $Info_{l-1} = \{\sigma_{l-1}, \delta_{l-1}, Im(F_{l-1}), Im(G_{l-1})\}$.
Output: $Info_l = \{\sigma_l, \delta_l, Im(F_l), Im(G_l)\}$.

0. Sæt $\delta_l' = \{span(f) : f \in Im(F_{l-1}), fail(f) = l\}$.

Sæt $\Delta_l = \Delta_{l-1} \cup \{i \ominus j : i \in \delta'_l, j \leq_p i\}$.
Lad σ_l *være mængden af minimalelementer for* $\mathbb{N} \setminus \Delta_l$.

1. *For hvert* $i \in \sigma_{l-1}$, *sæt* $f = F_{l-1}(i)$.
   - *Hvis* $i \not\leq_p l$ *eller hvis* $S(ff_{l\ominus i}) = 0$, *så sæt* $F_l(i) = f$.
   - *ellers*
     * *hvis* $l \ominus i = l' \ominus i'$ *for et* $l' \in \delta_{l-1}$ *og et* $i' \in \mathbb{N}$, *så sæt* $F_l(i) = f - \frac{S(ff_{l\ominus i})}{S(G_{l-1}(l')f_{i'}f_{l\ominus i})} G_{l-1}(l')f_{i'}$.
     * *ellers sæt* $G_l(l \ominus i) = f$.
2. *For hvert* $i \in \sigma_l \setminus \sigma_{l-1}$, *find et* $k \in \sigma_{l-1}$ *og et* $j \in \mathbb{N} \setminus \{1\}$, *så* $i = k \oplus j$, *og sæt* $f = F_{l-1}(k)$.
   - *Hvis* $i \not\leq_p l$, *sæt* $F_l(i) = ff_j$,
   - *ellers find et* $l' \in \delta_{l-1}$ *og et* $i' \in \mathbb{N}$, *så* $l \ominus i = l' \ominus i'$, *og sæt* $F_l(i) = ff_j - \frac{S(ff_j f_{l\ominus i})}{S(G_{l-1}(l')f_{i'}f_{l\ominus i})} G_{l-1}(l')f_{i'}$.

Argumenterne, for at denne algortime virker, er allerede blevet præsenteret, så her vil blot lige blive nævnt, hvilket argumenter, der skal bruges hvor.

Punkt *1*. svarer stort set til tilfælde **(1)** på side 103. Det første "hvis" svarer til, når $fail(f) > l$. Det andet "hvis" svarer til, når $failf = l$ og i også tilhører σ_l, for så skal der bestemmes et $F_l(i)$. Findes der ikke noget l' i δ_{l-1}, så $l \ominus i = l' \ominus i'$, må det betyde, at $i \notin \sigma_l$, så i det tilfælde skal der ikke bestemmes noget $F_l(i)$. Når $fail(f) = l$ er $span(f) = l \ominus i$ og da $f \in Im(F_{l-1})$, vil det sige, at $l \ominus i \in \delta'_l$. Så i det sidste "ellers" skal $G_l(l \ominus i)$ istedet bestemmes.

Punkt *2*. svarer til tilfælde **(2)** på side 103.

7.2 Dekodningsalgoritmen

Nu da delalgoritmen er beskrevet, er det ganske simpelt at beskrive en dekodningsalgoritme.

Algoritme 7.2.1 (Ny basisalgoritme)
Input: Et modtaget ord $\overline{r}$.
Output: Fejlpositionerne i fejlvektoren.

1. *Kør delalgoritmen (Algoritme 7.1.18) fra 1 til l.*
2. *Vælg et u i σ_l og sæt $f = F_l(u)$.*
3. *Fejlpositionerne er nu blandt de positioner, som svarer til nulpunkterne i polynomiet f.*

Grunden til at denne algoritme virker, stammer fra definitionen af $span(f)$. Som nævnt efter Definition 7.1.7 er $span(f)$ det største tal, så f tilhører vektorrummet $K_{span(f)-1,j}$, hvor j er fundet udfra, at $\omega(f) = \omega(f_j)$. Om det f som vælges i algoritmen gælder, at $\omega(f) = \omega(f_u)$ og $fail(f) > l$. Benævn $span(f) = k$. Det vil sige, det gælder, at $k \oplus u > l$, så $k > l \ominus u$. Dermed er det sikkert, at $f \in K_{l\ominus u,u}$, så f er et fejllokaliserende polynomium, hvis $d(NTP(s_{l\ominus u})) > \omega_H(\overline{e})$, hvilket er betingelsen for, at $L_u(I) = K_{l\ominus u,u}(\overline{r})$, se Lemma 6.1.9. Om dette er opfyldt kan ikke vides på forhånd, og det kan også afhænge af, hvilket $u \in \sigma_l$ der vælges.

Denne algoritme svarer til at have benyttet Basisalgoritmen, så den må kunne forbedres med Majoritetsalgoritmen. I Majoritetsalgoritmen bestemmes de ukendte syndromer, hvilket svarer til, at l bliver større i den ovenstående algoritme og dermed kan der rettes flere fejl. Hermed kan det også opnåes, at $d(NTP(s_{l\ominus u})) > \omega_H(\overline{e})$ ligemeget hvilket u, der vælges i σ_l. Dette vil blive gennemgået i næste afsnit, hvorledes det er muligt.

7.3 Udvidelse af dekodningsalgoritmen

For at udvide den nye basisalgoritme (Algoritme 7.2.1) er der brug for en ny mængde og visse resultater om denne mængde. Den ny mængde defineres som følger:

$$\Gamma_l = \{b \in \Sigma_{l-1} : b \leq_p l, l \ominus b \in \Sigma_{l-1}\}.$$

De følgende tre lemmaer stammer fra [2, Kapitel 2].

Lemma 7.3.1 *Følgende tre udsagn er opfyldt for mængden* Γ_l*:*

(*i*) $b \in \Gamma_l \Leftrightarrow l \ominus b \in \Gamma_l$

(*ii*) $b \in \Gamma_l \cap \Delta_l \Leftrightarrow l \ominus b \in \Delta_l$

(*iii*) $b \in \Gamma_l \cap \Sigma_l \Leftrightarrow l \ominus b \in \Sigma_l$

Bevis:

(*i*)**:** Antag først, at $b \in \Gamma_l$. Definitionen af Γ_l giver, at $l \ominus b \in \Sigma_{l-1}$, og det må gælde, at $l \ominus b \leq_p l$. Da $l \ominus (l \ominus b) = b \in \Sigma_{l-1}$ er alle betingelserne for, at $l \ominus b \in \Gamma_l$ opfyldte.
Antag dernæst, at $l \ominus b \in \Gamma_l$. Argumenterne er stort set de samme. Pr. definition af Γ_l vil det gælde, at $l \ominus (l \ominus b) = b \in \Sigma_{l-1}$, og da $l \ominus b$ eksisterer gælder det, at $b \leq_p l$. Så alle betingelserne er opfyldt for, at $b \in \Gamma_l$.

(*ii*) **og** (*iii*)**:** Det er tidligere vist, at $\Delta_l \cup \Sigma_l = \mathbb{N}$, og at $\Delta_l \cap \Sigma_l = \emptyset$. Udfra definitionen på Σ_l (se Definitione 7.1.10) kan Δ_l derfor også beskrives således:

$$\Delta_l = \{i \in \mathbb{N} : \exists\, f \in \mathbb{F}_{q^m}[x,y]/J \text{ sådan at } \omega(f) = \omega(f_i) \text{ og } fail(f) \leq l\}$$

Dette anvendes i det følgende, hvor det antages, at b tilhører $\Gamma_l \cap \Delta_l$. Da $b \in \Sigma_{l-1}$, må det gælde, at $b \in \Delta_l \setminus \Delta_{l-1}$. Dette er kun muligt, netop når der eksisterer både et f, hvorom det gælder, at $\omega(f) = \omega(f_b)$ og $fail(f) = l$ (udfra ovenstående ligning) og et g, hvorom det gælder, at $span(g) = b$ og $fail(g) = l$ (udfra Definition 7.1.10). Dette giver, at $span(f) = l \ominus b$ og at $\omega(g) = \omega(f_{l \ominus b})$. Dette betyder jo netop, at også $l \ominus b \in \Delta_l \setminus \Delta_{l-1}$.

Hvis det istedet gælder, at $b\Gamma_l \in \Sigma_l$, kan negationen af det netop konkluderede benyttes til at konkludere, at også $l \ominus b \in \Sigma_l$.

□

Af beviset til dette lemma kan det også ses, at tilvækst fra Δ_{l-1} til Δ_l er mængden $\Delta_l \cap \Gamma_l$.
Det er desuden muligt at vise følgende egenskaber om minimimalelementerne, σ_{l-1}, i Σ_{l-1} i forbindelse med Γ_l.

Lemma 7.3.2 *Lad $b \in \Gamma_l$ og $j \in \sigma_{l-1}$, sådan at $j \leq_p b$. Da gælder følgende tre udsagn:*

(*i*) $j \in \Gamma_l$.

(*ii*) $b \in \Gamma_l \cap \Sigma_l \Leftrightarrow j \in \Gamma_l \cap \Sigma_l$.

(*iii*) $b \in \Gamma_l \cap \Delta_l \Leftrightarrow j \in \Gamma_l \cap \Delta_l$.

Bevis:

(*i*)**:** Tre ting skal være opfyldt for, at $j \in \Gamma_l$. Først skal $j \in \Sigma_{l-1}$, hvilket det jo gør, da $j \in \sigma_{l-1}$. Dernæst skal det gælder, at $j \leq_p l$, hvilket er opfyldt, fordi $b \in \Gamma_l$, for da er $j \leq_p b \leq_p l$. Til sidst skal $l \ominus j \in \Sigma_{l-1}$. Da $j \leq_p b$, vil det gælde, at $l \ominus b \leq_p l \ominus j$, og når $b \in \Gamma_l$ vil $l \ominus b \in \Sigma_{l-1}$. Da giver Lemma 7.1.13, at $l \ominus j \in \Sigma_{l-1}$, og dermed er punkt (*i*) bevist.

(*ii*)**:** Hvis $b \in \Gamma_l \cap \Sigma_l$, så giver Lemma 7.3.1 (*iii*), at $l \ominus b \in \Gamma_l \cap \Sigma_l$. Da $l \ominus b \leq_p l \ominus j$ gælder det, at $l \ominus j \in \Sigma_l$. Første punkt i dette lemma giver, at $j \in \Gamma_l$, hvilket betyder, at $l \ominus j \in \Sigma_{l-1}$, og at $l \ominus (l \ominus j) = j \in \Sigma_{l-1}$, og da $l \ominus j \leq_p l$ vil det derfor gælde, at $l \ominus j \in \Gamma_l$ og dermed er betingelserne opfyldt for, at $l \ominus j \in \Gamma_l \cap \Sigma_l$. Nu giver Lemma 7.3.1 (*iii*), at $j \in \Gamma_l \cap \Sigma_l$.
Hvis det istedet gælder, at $j \in \Gamma_l \cap \Sigma_l$, vil $b \in \Sigma_l$, da $j \leq_p b$. Elementet b er allerede valgt sådan, at det tilhører Γ_l, så dermed vil $b \in \Gamma_l \cap \Sigma_l$.

(*iii*)**:** Hvis $b \in \Gamma_l \cap \Delta_l$, giver punkt (*i*) i dette lemma, at $j \in \Gamma_l$. Da $j \leq_p b$ giver Lemma 7.1.13, at $j \in \Delta_l$, så dermed vil $j \in \Gamma_l \cap \Delta_l$.
Hvis istedet $j \in \Gamma_l \cap \Delta_l$ giver Lemma 7.3.1 (*ii*), at $l \ominus j \in \Gamma_l \cap \Delta_l$. Da $l \ominus b \leq_p l \ominus j$ benyttes Lemma 7.1.13 til at konkludere, at $l \ominus b \in \Delta_l$. Så giver Lemma 7.3.1, at $b \in \Gamma_l \cap \Delta_l$.

□

Følgende lemma er vigtig i udvidelsen af Algoritme 7.2.1.

Lemma 7.3.3 *Lad det være opfyldt, at $b \in \sigma_{l-1} \cap \Gamma_l$ og sæt $f = F_{l-1}(b)$. Da gælder det, at*

(*i*) $S(ff_{l\ominus b}) = 0 \Leftrightarrow b \in \Gamma_l \cap \Sigma_l$,

(*ii*) $S(ff_{l\ominus b}) \neq 0 \Leftrightarrow b \in \Gamma_l \cap \Delta_l$.

Bevis: Det vil flere steder i beviset blive benyttet, at valget af f betyder, at $fail(f) > l-1 \geq l$ og at $\omega(f) = \omega(f_b)$.

(*i*)**:** Hvis $S(ff_{l\ominus b}) = 0$ må $span(f) > l \ominus b$, og dermed er $fail(f) = span(f) \oplus b > (l \ominus b) \oplus b = l$. Det betyder, at $b \in \Sigma_l$, og da b er valgt til at tilhøre Γ_l, vil det altså gælde, at $b \in \Gamma_l \cap \Sigma_l$.
Hvis det istedet gælder, at $b \in \Gamma_l \cap \Sigma_l$, giver tilhørsforholdet til Σ_l, at $fail(f) > l$ og dermed er $span(f) = fail(f) \ominus b > l \ominus b$, og hermed kan det konkluderes, at $S(ff_{l\ominus b}) = 0$.

(*ii*)**:** Hvis $S(ff_{l\ominus b}) \neq 0$, må det betyde, at $span(f) \leq l \ominus b$ og dermed er $fail(f) = span(f) \oplus b \leq (l \ominus b) \oplus b = l$, men valget af f gør, at $fail(f) \geq l$, så $fail(f) = l$. Dermed vides nu også, at $span(f) = l \ominus b$. Hermed kan det konkluderes, at $l \ominus b \in \Delta_l$ og så giver Lemma 7.3.1 (*ii*), at $b \in \Gamma_l \cap \Delta_l$.
Hvis det istedet gælder, at $b \in \Gamma_l \cap \Delta_l$, giver tilhørsforholdet til Δ_l, at $fail(f) \leq l$. Tilhørsforholdet til Γ_l giver blandt andet, at $b \in \Sigma_{l-1}$, som betyder, at $fail(f) > l-1 \geq l$. Det vil sige, at $fail(f) = l$, så $span(f) = l \ominus b$, hvilket pr. definition betyder, at $S(ff_{l\ominus b}) \neq 0$.

□

Til næste proposition skal det benyttes, at $\#\Delta_l \leq \omega_H(\overline{e})$ for alle l. Dette kan udledes af følgende lemma. Lemmaet stammer fra [4, Afsnit 2].

Lemma 7.3.4 *Definer følgende mængde:*

$$\Delta = \bigcup_{l=0}^{\infty} \Delta_l.$$

Da gælder det, at $\#\Delta = \omega_H(\overline{e})$.

Bevis: Den første egenskab, som skal benyttes vil ikke blive bevist her, men dette gøres i både [4, Afsnit 2] og [2, Kapitel 2]. Det er, at

$$\Delta = \{Span(f) : f \notin L_j(I)\}.$$

$L_j(I)$ er mængden af fejllokaliserende polynomier, se Definition 6.1.8. Det kan vises, at $L_j(I)$ er et ideal, hvilket dog ikke vil blive gjort her.

Beviset gennemføres nu ved først at vise, at $(\mathbb{F}_{q^m}[x,y]/J)/L_j(I)$, set som vektorrum, har dimension $\omega_H(\overline{e})$. Dernæst vises, at hvis der for ethvert $k \in \Delta$ vælges et $h_k \in \mathbb{F}_{q^m}[x,y]/J$, hvorom det gælder, at $\omega(h_k) = \omega(f_k)$, så gælder det, at $\{h_k : k \in \Delta\}$ er en basis for $(\mathbb{F}_{q^m}[x,y]/J)/L_j(I)$. Dermed er det nemlig bevist, at $\#\Delta = \omega_H(\overline{e})$.

Først defineres en afbildning $ev : \mathbb{F}_{q^m}[x,y]/J \to \mathbb{F}_{q^m}^{\omega_H(\overline{e})}$, som evaluerer $f \in \mathbb{F}_{q^m}[x,y]/J$ i de punkter p_i, hvor $e_i \neq 0$. Dermed er $L_j(I)$ nulrummet for afbildningen ev. I beviset til Sætning 3.2.4 blev det bevist, at hvis man har de forskellige punkter $p_1, \ldots, p_m \in \mathbb{F}_{q^m}^n$, så findes der polynomier $g_1, \ldots, g_m \in \mathbb{F}_{q^m}[x,y]/J$, så det gælder for alle $1 \leq k \leq m$, at $g_k(p_k) = 1$, mens $g_k(p_j) = 0$ når $j \neq k$. Når disse g_k'er afbilledes med ev kan det ses, at ev er surjektiv. Dermed giver Isomorfi-sætningen [1, Theorem 4.3.1], at $(\mathbb{F}_{q^m}[x,y]/J)/L_j(I)$ er isomorf med $\mathbb{F}_{q^m}^{\omega_H(\overline{e})}$, så dermed er dimensionen af $(\mathbb{F}_{q^m}[x,y]/J)/L_j(I)$ netop $\omega_H(\overline{e})$.

For ethvert $k \in \Delta$ vælges nu et h_k, hvorom det gælder, at $\omega(h_k) = \omega(f_k)$. Betragt nu en ikke-triviel linear kombination af disse h_k'er, $v = \sum_{k\in\Delta} \lambda_k h_k$. Det gælder, at $\omega(v) = \omega(f_k)$ for et $k \in \Delta$, det vil sige, at $v \notin L_j(I)$. Dermed er h_k'erne lineært uafhængige modulo $L_j(I)$. Hernæst skal det vises, at disse h_k'er også udspænder $(\mathbb{F}_{q^m}[x,y]/J)/L_j(I)$. Det antages derfor, at der findes en eller flere funktioner $g \in \mathbb{F}_{q^m}[x,y]/J$, som ikke er med i $Span(h_k : k \in \Delta)$. Vælg blandt disse nu det g, så $\omega(g)$ er mindst mulig. Hvis $\omega(g) = \omega(f)$ for et $f \in L_j(I)$, gælder det, at $\omega(g - \lambda f) < \omega(g)$ for et $\lambda \in \mathbb{F}_{q^m}^*$. Da g var valgt til at have mindst mulig vægt, vil $(g - \lambda f) \in Span(h_k : k \in \Delta)$, men da $\lambda f \in L_j(I)$ betyder det, at g alligevel tilhører $Span(h_k : k \in \Delta)$.
Hvis $\omega(g) \neq \omega(f)$ for alle $f \in L_j(I)$, så er $\omega(g) = \omega(f_k)$ for et $k \in \Delta$. Dermed er $\omega(g) = \omega(h_k)$ for et $k \in \Delta$, så igen vil g tilhører $Span(h_k : k \in \Delta)$.
Dermed er beviset fuldført. □

Da $\Delta = \bigcup_{l=0}^{\infty} \Delta_l$, giver dette lemma, at det må gælde, at $\#\Delta_l \leq \omega_H(\overline{e})$. Dette kan nu anvendes i følgende proposition, som er vigtig i udvidelsen af Algoritme

7.2.1.

Proposition 7.3.5 *Lad $\omega_H(\overline{e}) = t$. Hvis $2t < \nu_l$, så er $\#(\Gamma_l \cap \Sigma_l) > \#(\Gamma_l \cap \Delta_l)$.*

Bevis: Lad $V_l = \Gamma_l \cap \Sigma_l$ og $W_l = \Gamma_l \cap \Delta_l$. Disse to mængder deler Γ_l. Ved at se på definitionen af Γ_l kan det ses, at $W_l \cap \Delta_{l-1} = \emptyset$, men $W_l \cup \Delta_{l-1} = \Delta_l$. Dermed kan konklusionen lige før denne proposition benyttes til at se, at

$$\#W_l + \#\Delta_{l-1} = \#\Delta_l \leq t. \tag{7.7}$$

Betragt nu mængden $C_l = \{a \in \mathbb{N} : a \leq_p l\}$. Det gælder dermed, at $\#C_l = \nu_l$. Da $\Gamma_l \subseteq C_l$, vil også $V_l \subseteq C_l$ og $W_l \subseteq C_l$. De elementer i C_l, som V_l og W_l ikke kan dække, kan deles i følgende to mængder:

$$A_l = \{a \in \Sigma_{l-1} : l \ominus a \in \Delta_{l-1}\} \quad \text{og} \quad B_l = \{a \in \Delta_{l-1} : a \leq_p l\}.$$

Det gælder, at $\#A_l \leq \#\Delta_{l-1}$ og $\#B_l \leq \#\Delta_{l-1}$, så dermed gælder det, at

$$2t < \nu_l \leq \#V_l + \#W_l + 2\#\Delta_{l-1}.$$

Ved nu at benytte ligning (7.7) kan det indses, at

$$\begin{aligned} & 2(\#W_l + \#\Delta_{l-1}) \leq 2t < \#V_l + \#W_l + 2\#\Delta_{l-1} \\ \Updownarrow & \\ & \#W_l < \#V_l, \end{aligned}$$

hvilket er det ønskede resultat. □

Den næste definition benyttes direkte i udvidelsen af Algoritme 7.2.1, men for at sikre sig, at denne definition er veldefineret er følgende lemma nødvendig. Det stammer fra [2, Kapitel 1].

Lemma 7.3.6 *Hvis $f, g \in \mathbb{F}_q[x, y]/J$, sådan at $\omega(f) = \omega(g)$, da findes der et entydigt $\varepsilon \in \mathbb{F}_{q^m}^*$, sådan at $\omega(f - \varepsilon g) < \omega(g)$.*

Bevis: Gennem beviset benyttes regneregler om vægten af et polynomium, som er bevist i Lemma 6.1.2.

Eksistens: Da $\omega(f) = \omega(g)$ gælder det, at $\omega(f - \varepsilon g) < \max_{\prec}(\omega(f), \omega(-\varepsilon g)) = \omega(g) = \omega(f)$.

Entydighed: Antag at både ε og ξ opfylder, at $\omega(f - \varepsilon g) < \omega(g)$ og $\omega(f - \xi g) < \omega(g)$. Det gælder, at $\omega(f - \xi g) = \omega(-1(f - \xi g))$, så $\omega(\xi g - f) < \omega(g)$. Dermed gælder det, at $\omega((f - \varepsilon g) + (\xi g - f)) \leq \max_{\prec}(\omega(f - \varepsilon g), \omega(\xi g - f)) < \omega(g)$. Dette giver, at

$$\omega((\xi - \varepsilon)g) < \omega(g), \tag{7.8}$$

men da $\omega(\lambda g) = \omega(g)$ hvis og kun hvis $\lambda \in \mathbb{F}_{q^m}^*$, er ligning (7.8) kun muligt, hvis $(\xi - \varepsilon) = 0$, det vil sige, at $\xi = \varepsilon$.

□

Følgende definition er, som før nævnt, nu veldefineret.

Definition 7.3.7 ($Vote(b)$) *Lad $b \in \Gamma_{l+1}$ og $j_b \in \sigma_l$, så det er opfyldt, at $j_b \leq_p b$. Vælg det $\varepsilon \in \mathbb{F}_{q^m}^*$, så $\omega(f_{l+1} + \varepsilon F_l(j_b) f_{(l+1)\ominus j_b}) < \omega(f_{l+1})$. Da defineres*

$$Vote(b) = S(f_{l+1} + \varepsilon F_l(j_b) f_{(l+1)\ominus j_b}).$$

Dette $vote(b)$ vil være kendt, da $\omega(f_{l+1} + \varepsilon F_l(j_b) f_{(l+1)\ominus j_b}) < \omega(f_{l+1})$.

Nu kan Algoritme 7.2.1 udvides til at se ud på følgende måde. Bemærk, at indekset l benyttes på 2 forskellige måder i punkt 2.

Algoritme 7.3.8 *[Udvidet Algoritme]*
Lad $l > 3g - 2$, hvor $g = \frac{\left(\frac{q^m - 1}{q-1} - 1\right)(q^{m-1} - 1)}{2}$. Denne algoritme kan da rette $t = \lfloor \frac{n-s-1}{2} \rfloor$ fejl.
Input: Et modtaget ord $\overline{r}$.
Output: Fejlpositionerne i fejlvektoren.

1. *Kør Delalgoritmen (Algoritme 7.1.18) fra 1 til l.*

2. *For $i = l + 1$ og indtil $(i \ominus u) - g + 1 > t$ for alle $u \in \sigma_i$, gøres følgende:*
   - *Bestem Γ_i.*
   - *For ethvert $b \in \Gamma_i$ vælg et $j_b \in \sigma_{i-1}$, sådan at $j_b \leq_p b$.*
   - *Sæt $f = F_{i-1}(j_b)$.*
   - *Vælg det $\varepsilon \in \mathbb{F}_{q^m}^*$, som opfylder, at $\omega(f_i + \varepsilon f f_{i \ominus j_b}) < \omega(f_i)$.*
   - *Bestem $vote(b) = S(f_i + \varepsilon f f_{i \ominus j_b})$.*
   - *Sæt s_i lig den værdi, som optræder flest gange i mængden $\{vote(b) : b \in \Gamma_i\}$*
   - *Kør Delalgoritmen (Algoritme 7.1.18) for $l = i$. (Her er l det indeks, som er anvendt i Delalgoritmen).*
3. *Vælg et u i σ_i og sæt $f = F_i(u)$.*
4. *Fejlpositionerne er nu blandt de positioner, som svarer til nulpunkterne i polynomiet f.*

Grunden til at denne algoritme virker er, at Lemma 7.3.3 giver, at $S(\varepsilon f f_{i \ominus j_b}) = 0$, når $j_b \in \Gamma_i \cap \Sigma_i$ og Proposition 7.3.5 giver, at så længe $2t < \nu_l$ sker dette flest gange, når alle $vote(b)$ for $b \in \Gamma_i$ bestemmes. Ved hjælp af Lemma 6.2.6 og ligning (6.2) side 68 kan denne grænse omskrives til $2t < l - g + 1 = (n + g - s - 1) - g + 1 = n - s$. Dermed kan denne algoritme rette $t \leq \frac{n-s-1}{2}$ fejl.
Udvidelsen (punkt *2.*) skal køre frem til, at $(i \ominus u) - g + 1 > t$ for alle $u \in \sigma_i$. Dette skyldes, at det ønskes, at $d(NTP(s_{l \ominus u})) > \omega_H(\overline{e}) = t$ og det gælder, at

$$d(NTP(s_{l \ominus u})) = n - s = n - (n + g - (l \ominus u) - 1) = (l \ominus u) - g + 1.$$

Det blev i Lemma 7.3.4 bevist, at $\#\Delta = \omega_H(\overline{e})$, hvor $\Delta = \bigcup_{l=0}^{\infty} \Delta_l$. Dette må betyde, at Δ_l'erne stabiliseres, altså at der findes et j, så $\Delta_j = \Delta_{j+1} = \Delta_{j+2} = \cdots$, se [4, Afsnit 2] eller [2, Kapitel 2] for flere detaljer om dette. Dette medfører ligeledes, at er $Info_j = Info_{j+1} = Info_{j+2} = \cdots$. Dermed er det muligt inden for et endeligt antal skridt at opnå, at $(i \ominus u) - g + 1 > t$ for alle $u \in \sigma_i$.
Det kan her bemærkes, at hvis s_i vedtages enstemmigt, er det ikke nødvendigt at gennemløbe delalgoritmen i dette gennemløb af den udvidede del. Dette skyldes, at så vil alle j_b tilhøre $\Gamma_i \cap \Sigma_i$ og netop da vil det være opfyldt, at $S(\varepsilon f f_{i \ominus j_b}) = 0$, og så ændres $F_{i-1}(j_b)$ ikke (se delalgoritmen, Algoritme 7.1.18, punkt *1.* - *Hvis* ...). Dermed er $Info_{i-1} = Info_i$, når s_i vedtages enstemmigt.

Eksempel 7.3.9 Dette er en gentagelse af Eksempel 6.2.8, nu blot dekodet med den nye dekodningsalgoritme, hvorfor det stadig er koden $NTP(49)$, der arbejdes med. Først skal delalgoritmen gennemløbes $l = 20$ gange, hvilket er opskrevet i Tabel 1 på side 116, som er taget fra [10, side 951-953]. Alle detaljer til denne tabel vil ikke blive udledt, her vil kun gennemløbet for $l = 4$ blive gennemgået.

Input: $Info_3 = \{\sigma_3 = \{2,3\}, \delta_3 = \{1\}, F_3 = \{x + \alpha^5, y\}, G_3 = \{1\}\}$.

(0)**:** Det kan bestemmes, at $span(x+\alpha^5) = 2$, hvormed $fail(x+\alpha^5) = 2 \oplus 2 = 4$, og ligeledes kan det bestemmes, at $span(y) = 2$, hvormed $fail(y) = 2 \oplus 3 = 5$. Dermed er

$$\delta_4' = \{span(f) : f \in Im(F_3), fail(f) = 4\} = \{2\}$$

og så bliver

$$\begin{aligned} \Delta_4 &= \Delta_3 \cup \{i \ominus j : i \in \delta_4', j \leq_p i\} = \{1\} \cup \{1,2\} = \{1,2\} \\ \sigma_4 &= \{3,4\}. \end{aligned}$$

(1)**:** $i = 2$: $f = F_3(2) = x + \alpha^5$. Da det hverken er opfyldt, at $2 \not\leq_p 4$ eller at $S(ff_2) = 0$ eller at der findes et $l' \in \delta_3$, så $4 \ominus 2 = 2 = l' \ominus i'$, sker der det, at her sættes

$$G_4(2) = f = x + \alpha^5.$$

$i = 3$: $f = F_3(3) = y$. Her er det opfyldt, at $3 \not\leq_p 4$, så her sættes

$$F_4(3) = f = y.$$

(2)**:** $i = 4$:, $4 = 2 \oplus 2$, hvor $k = 2 \in \delta_3$ og $j = 2 > 1$ og så er $f = F_3(2) = x + \alpha^5$. Da det her er opfyldt, at $4 \leq_p 4$, findes der $l' \in \delta_3$, så $4 \ominus 4 = 1 = l' \ominus i' = 1 \ominus 1$. Så her bliver

$$\begin{aligned} F_4(4) &= ff_2 - \tfrac{S(ff_2 f_{4 \ominus 4})}{S(G_3(1) f_1 f_{4 \ominus 4})} G_3(1) f_1 \\ &= (x + \alpha^5)x + \alpha^{14} \cdot 1 \cdot 1. \end{aligned}$$

Output: $Info_4 = \{\sigma_4 = \{3,4\}, \delta_4 = \{2\}, F_4 = \{y, x^2 + \alpha^5 x + \alpha^{14}\}, G_4 = \{x + \alpha^5\}\}$.

Efter at delalgoritmen er kørt igennem 20 gange er det ikke opfyldt for noget $u \in \sigma_{20}$, at $(20 \ominus u) - 6 + 1 > 7$, så her ses det, at udvidelsen er nødvendig. Kun det første gennemløb af tilføjelsen vil her blive gennemgået.

$i = 21$**:** $\Gamma_{21} = \{b \in \Sigma_{20} : b \leq_p 21, 21 \ominus b \in \Sigma_{20}\} = \{6, 8, 11\}$.

$b = 6$**:** $j_6 = 6$, $f = F_{20}(6) = y^2 + \alpha^{10}xy + \alpha^{13}y + \alpha^{13}x + \alpha^{11}$, $21 \ominus 6 = 11$, $\varepsilon = 1$, det vil sige

$$vote(6) = S(x^4y^2 + (y^2 + \alpha^{10}xy + \alpha^{13}y + \alpha^{13}x + \alpha^{11})x^4) = \alpha^6.$$

$b = 8$**:** $j_8 = 8$, $f = F_{20}(8) = x^2y+\alpha^4xy+\alpha^3x^2+\alpha y+\alpha^7x+\alpha^4$, $21 \ominus 8 = 8$, $\varepsilon = 1$, det vil sige

$$vote(8) = S(x^4y^2+(x^2y+\alpha^4xy+\alpha^3x^2+\alpha^3x^2+\alpha y+\alpha^7x+\alpha^4)x^2y) = \alpha^6.$$

$b = 11$**:** $j_{11} = 11$, $f = F_{20}(11) = x^4 + \alpha^3x^3 + \alpha^9x^2y + \alpha^4x^2 + \alpha^{14}xy + \alpha^6y + \alpha^5x + 1$, $21 \ominus 11 = 6$, $\varepsilon = 1$, det vil sige

$$\begin{aligned} &vote(11) = \\ &= S(x^4y^2 + (x^4 + \alpha^3x^3 + \alpha^9x^2y + \alpha^4x^2 + \alpha^{14}xy + \alpha^6y + \alpha^5x + 1)y^2) \\ &= \alpha^6. \end{aligned}$$

Det vil sige, her er der enstemmighed om, at $s_{21} = \alpha^6$, så her vil et gennemløb af delalgoritmen ikke ændre noget.

Der er tilsvarende enstemmighed om, at $S(f_{22}) = \alpha^3$, $S(f_{23}) = \alpha^6$, $S(f_{24}) = \alpha^4$, $S(f_{25}) = \alpha^{11}$ og $S(f_{26}) = \alpha^{10}$. Det er også muligt at bestemme, at $S(f_{27}) = \alpha$, men dette vedtages ikke enstemmigt, så her bliver $\sigma_{27} = \{6, 8\}$ og $F_{27} = \{y^2 + \alpha^{10}xy+\alpha^{13}y+\alpha^{13}x+\alpha^{11}, x^2y+\alpha^4xy+\alpha^3x^2+\alpha y+\alpha^7x+\alpha^4\}$. Disse to funktioner har de 7 punkter, hvori der er fejl, som nulpunkter (plus lidt flere punkter, som dog giver anledning til fejlværdi 0, da fejlvektoren er entydig bestemt, så længe antallet af fejl er mindre end d, se eventuelt [10, Proposition 6.1]).

Tabel 1

l	σ_l	elementer i σ_l	F_l til det pågældende element iσ_l
	δ_l	elementer i δ_l	G_l til det pågældende element i δ_l
0	σ_0	1	1
	δ_0		
1	σ_1	2	x
		3	y
	δ_1	1	1
2	σ_2	2	$x+\alpha^5$
		3	y
	δ_2	1	1
3	σ_3	2	$x+\alpha^5$
		3	y
	δ_3	1	1
4	σ_4	3	y
		4	$x^2+\alpha^5x+\alpha^{14}$
	δ_4	2	$x+\alpha^5$
5	σ_5	3	$y+\alpha x+\alpha^6$
		4	$x^2+\alpha^5x+\alpha^{14}$
	δ_5	2	$x+\alpha^5$
6	σ_6	4	$x^2+\alpha^5x+\alpha^{14}$
		5	$xy+\alpha x^2+\alpha^6x$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^6y+\alpha^{10}x$
	δ_6	2	$x+\alpha^5$
		3	$y+\alpha x+\alpha^6$
7	σ_7	4	$x^2+\alpha^{13}x+\alpha^5$
		5	$xy+\alpha x^2+\alpha^6x$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^6y+\alpha^{10}x$
	δ_7	2	$x+\alpha^5$
		3	$y+\alpha x+\alpha^6$
8	σ_8	4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
		5	$xy+\alpha x^2+\alpha^{14}x+\alpha^{13}$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^6y+\alpha^{10}x$
	δ_8	2	$x+\alpha^5$
		3	$y+\alpha x+\alpha^6$

fortsætter på næste side

fortsat fra forrige side

l	σ_l	elementer i σ_l	F_l til det pågældende element iσ_l
	δ_l	elementer i δ_l	G_l til det pågældende element i δ_l
9	σ_9	4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
		5	$xy+\alpha x^2+\alpha^{11}y+\alpha^5x+\alpha^{14}$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^6y+\alpha^{10}x$
	δ_9	2	$x+\alpha^5$
		3	$y+\alpha x+\alpha^6$
10	σ_{10}	4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
		5	$xy+\alpha x^2+\alpha^{11}y+\alpha^5x+\alpha^{14}$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^2y+\alpha^2x+\alpha^9$
	δ_{10}	2	$x+\alpha^5$
		3	$y+\alpha x+\alpha^6$
11	σ_{11}	5	$xy+\alpha x^2+\alpha^{11}y+\alpha^5x+\alpha^{14}$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^2y+\alpha^2x+\alpha^9$
		7	$x^3+\alpha^3xy+\alpha^{11}x^2+\alpha^4x+\alpha^2$
	δ_{11}	3	$y+\alpha x+\alpha^6$
		4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
12	σ_{12}	5	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
		6	$y^2+\alpha xy+\alpha^5x^2+\alpha^2y+\alpha^2x+\alpha^9$
		7	$x^3+\alpha^3xy+\alpha^{11}x^2+\alpha^8y+\alpha^{14}x+\alpha^{13}$
	δ_{12}	3	$y+\alpha x+\alpha^6$
		4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
13	σ_{13}	5	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
		6	$y^2+\alpha xy+y+\alpha^5x+\alpha^2$
		7	$x^3+\alpha^3xy+\alpha^{11}x^2+\alpha^8y+\alpha^{14}x+\alpha^{13}$
	δ_{13}	3	$y+\alpha x+\alpha^6$
		4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
14	σ_{14}	5	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
		6	$y^2+\alpha xy+y+\alpha^5x+\alpha^2$
		7	$x^3+\alpha^3xy+\alpha^{11}x^2+\alpha^8y+\alpha^{14}x+\alpha^{13}$
	δ_{14}	3	$y+\alpha x+\alpha^6$
		4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$
15	σ_{15}	5	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
		6	$y^2+\alpha xy+y+\alpha^5x+\alpha^2$
		7	$x^3+\alpha^3xy+\alpha^5x^2+\alpha^{14}y++\alpha^{10}$
	δ_{15}	3	$y+\alpha x+\alpha^6$
		4	$x^2+\alpha^3y+\alpha^{11}x+\alpha^6$

fortsætter på næste side

fortsat fra forrige side

l	σ_l	elementer i σ_l	F_l til det pågældende element iσ_l
	δ_l	elementer i δ_l	G_l til det pågældende element i δ_l
16	σ_{16}	6	$y^2+\alpha xy+y+\alpha^5x+\alpha^2$
		8	$x^2y+\alpha^{13}xy+\alpha^3x^2+\alpha^3y+\alpha^6x+\alpha^6$
		11	$x^4+\alpha^3x^2y+\alpha^5x^3+\alpha^{14}xy+\alpha^7y+\alpha x+\alpha^{13}$
	δ_{16}	5	$x^3+\alpha^3xy+\alpha^5x^2+\alpha^{14}y+\alpha^{10}$
		7	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
17	σ_{17}	6	$y^2+\alpha^{10}xy+\alpha^{13}y+\alpha^{13}x+\alpha^{11}$
		8	$x^2y+\alpha^{13}xy\alpha^3x^2+\alpha^3y+\alpha^6x+\alpha^6$
		11	$x^4+\alpha^3x^2y+\alpha^5x^3+\alpha^{14}xy+\alpha^7y+\alpha x+\alpha^{13}$
	δ_{17}	5	$x^3+\alpha^3xy+\alpha^5x^2+\alpha^{14}y+\alpha^{10}$
		7	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
18	σ_{18}	6	$y^2+\alpha^{10}xy+\alpha^{13}y+\alpha^{13}x+\alpha^{11}$
		8	$x^2y+\alpha^{13}xy+\alpha^3x^2+\alpha^3y+\alpha^6x+\alpha^6$
		11	$x^4+\alpha^3x^2y+\alpha^5x^3+\alpha^{14}xy+\alpha^7y+\alpha x+\alpha^{13}$
	δ_{18}	5	$x^3+\alpha^3xy+\alpha^5x^2+\alpha^{14}y+\alpha^{10}$
		7	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
19	σ_{19}	6	$y^2+\alpha^{10}xy+\alpha^{13}y+\alpha^{13}x+\alpha^{11}$
		8	$x^2y+\alpha^{13}xy+\alpha^3x^2+\alpha^3y+\alpha^6x+\alpha^6$
		11	$x^4+\alpha^9x^2y+\alpha^5x^3+x^2+\alpha^7y+\alpha^5x+\alpha^{13}$
	δ_{19}	5	$x^3+\alpha^3xy+\alpha^5x^2+\alpha^{14}y+\alpha^{10}$
		7	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$
20	σ_{20}	6	$y^2+\alpha^{10}xy+\alpha^{13}y+\alpha^{13}x+\alpha^{11}$
		8	$x^2y+\alpha^4xy+\alpha^3x^2+\alpha y+\alpha^7x+\alpha^4$
		11	$x^4+\alpha^3x^3+\alpha^9x^2y+\alpha^4x^2+\alpha^{14}xy+\alpha^6y+\alpha^5x+1$
	δ_{20}	5	$x^3+\alpha^3xy+\alpha^5x^2+\alpha^{14}y+\alpha^{10}$
		7	$xy+\alpha^{13}y+\alpha^{14}x+\alpha$

Kapitel 8

Afrunding

Jeg har i dette speciale beskæftiget mig med de såkaldte NTP-koder, som er en generalisering af Reed-Solomon koder.

Kodeordene for en NTP-kode blev bestemt til at være polynomier, som er linear kombinationer af monomierne i $\Delta_{\prec_w}(I)$, (som er fodaftrykket af $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$ med hensyn til $\prec_w$), evalueret i de q^{2m-1} punkter tilhørende $\mathbf{V}(\langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle)$.
Det blev bestemt, at minimumsafstanden for en $NTP(s)$-kode altid er mindre end eller lig $n - s$. Specielt gælder der lighed, hvis funktionen

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

er mindre end eller lig q, for det (i,j), hvorom det gælder, at $x^i y^j \in \Delta_{\prec_w}(I)$, så $i(q^{m-1}) + j\left(\frac{q^m-1}{q-1}\right) = s$.
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

$$NTP(n + c(\Gamma) - 2 - s),$$

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

Resten af tiden beskæftigede jeg mig med dekodning. Den første dekodningsalgoritme gør det muligt at rette op til $\frac{d-g}{2}$ fejl. Den finder et interpolationspolynomium til at bestemme fejlpositionerne og herefter benyttes syndromer til at bestemme fejlværdierne.

Basisalgoritmen, hvortil dobbeltsyndromer benyttes, finder fejlpositionerne udfra et fejllokaliserende polynomium og benytter derefter syndromer til at bestemme fejlværdierne på tilsvarende vis som den første dekodningsalgoritme. Basisalgoritmen kan rette $\frac{n-s-g-1}{2}$ fejl, hvilket faktisk er dårlige end den første algoritme, da $d \geq n - s$. Basisalgoritmen kan dog forbedres med majoritetsalgoritmen, som gør det mulig at bestemme de ukendte syndromer. Dermed kan der rettes op til $\frac{n-s-1}{2}$ fejl.

Tilsidst benyttes ideerne og noget af teorien fra basis- og majoritetsalgoritmen til at opstille en mere effektiv algoritme, hvilket betyder, at kompleksiteten nedsættes, mens antallet af fejl, som kan rettes, forbliver uændret.

English Summary

During this report I have worked with a generalization of Reed-Solomon codes which are called NTP-codes.

The codewords in the NTP-codes were determined to be the polynomials which are linear combinations of the monomials in $\Delta_{\prec_w}(I)$ (the footprint of the ideal $I = \langle x^{\frac{q^m-1}{q-1}} - y^{q^{m-1}} - \cdots - y^q - y, x^{q^m} - x, y^{q^m} - y\rangle$ where the monomiel order is $\prec_w$) 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, where (i,j) is such that $x^i y^j \in \Delta_{\prec_w}(I)$, so $i(q^{m-1}) + j\left(\frac{q^m-1}{q-1}\right) = s$
To identify the dimension of the code I introduced some theory concerning numerical semigroups, genus and conductor and the dimension is found to be

$$k(NTP(s)) = s + 1 - g,$$

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

The rest of the report concerns decoding. The first decoding algorithm is able to correct less than $\frac{d-g}{2}$ errors. It finds an interpolationspolynomium to determine the error positions and then uses syndroms to determine the error values.

The basic algorithm in which the dobblesyndroms are used determines the error positions by finding an error-locator polynoium. After that it uses the syndroms to find the error values in the same way as the first algorithm. The basic algorithm is able to correct less than $\frac{n-s-g-1}{2}$ errors which actually is not as good as the first algorithm, because $d \geq n - s$. The basic algorithm can be improved by the majority algorithm, which make it possibly to find the unknown syndroms. Then it is able to correct $\frac{n-s-1}{2}$ errors.

Finally the basic and the majority algorithm is implemented into a new algorithm, which has a lower complexity while the number of errors it is able to corret remain unchanged.

Appendiks A

Dette appendiks knytter sig primært til Kapitel 3, 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 [8].

Det første hovedresultat i Appendiks A er følgende:

Sætning A.0.10 *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 A.0.11 *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 A.0.12 *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 A.1.1 *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 A.1.2 *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 A.2.1 *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 A.2.2 (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 A.2.3 (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 A.2.4 (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 A.2.5 (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 A.2.6 *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 A.2.6, 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 *A*.2.1.

Bevis: Bevis for Lemma A.2.1.
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 A.2.5, at g er minimalpolynomiet for α over $\mathbb{F}_q$.
Hvis $h(\alpha) = 0$ medfører dette udfra Lemma A.2.6, 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 A.2.6 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 A.0.11.

Lemma A.3.1 *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 A.3.2 *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 A.3.3 *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 A.3.4 *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, [8, 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 $\mathbf{K}(\alpha)$ 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 A.2.6, 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 A.3.1 anvendes endnu en sætning, som dog ikke bevises her, men beviset kan findes i [8, Theorem 2.6, side 46].

Lemma A.3.5 (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 A.3.1.

Bevis: Bevis for Lemma A.3.1.

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 A.1.1.
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 A.3.3 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, vil minimalpolynomiet med hensyn til α over $\mathbb{F}_q$ hvae grad n, da f er irreducibel. Dermed kan vi benytte Lemma A.3.4 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 A.3.3 følger det da, at $m|n$.

Antag modsat, at $m|n$, så følger det af Lemma A.3.5, 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 A.3.4 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 A.2.1, 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 A.0.10 *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 A.2.6, 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 A.3.1 til at konkludere, at

$$\deg(f)|m.$$

□

Herefter kan det andet hovedresultat bevises, hvilket lød således:

Sætning A.0.11 *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 A.3.4 (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 A.1.1 og Lemma A.1.2 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 A.2.1, at $f(x)|(x^{q^{i+d-k}} - x)$, og af Lemma A.3.1 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 A.0.12 *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 A.0.10 være mindre end eller lig m.
Lad $deg(f) = s$ og antag, at $s < m$. Sætning A.0.11 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 A.1.1 og Lemma A.1.2, 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 A.0.11 kan benyttes til at konkludere, at $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ er forskellige.

Hvis derimod $deg(f) = d < m$, giver Sætning A.0.10, at $d|m$, og igen kan Sætning A.0.11 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 enkelt sætning, som skal benyttes i Kapitel 3.

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 B.1.1 *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:

$$\begin{array}{rcccl} (\varphi(a) * \varphi(b)) * \varphi(c) & = & \varphi(a \circ b) * \varphi(c) & = & \varphi((a \circ b) \circ c) \\ & = & \varphi(a \circ (b \circ c)) & = & \varphi(a) * \varphi(b \circ c) \\ & = & \varphi(a) * (\varphi(b) * \varphi(c)). & & \end{array}$$

(ii) : Lad $a \in G$, da er

$$\begin{array}{rcccl} \varphi(a) & = & \varphi(a \circ e) & = & \varphi(a) * \varphi(e) \\ \varphi(a) & = & \varphi(e \circ a) & = & \varphi(e) * \varphi(a). \end{array}$$

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 B.1.2 *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 B.1.1 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 B.1.2 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] Maria Bras Amorós *"Improving Evaluation Codes"* Universitat Politècnica de Catalunya, 2003.

[3] David Cox, John Little, Donal O'Shea *"Ideals, Varieties, and Algorithms"*, Springer-Verlag, 1997.

[4] David Cox, John Little, Donal O'Shea *"Using Algebraic Geometry - Second Edition"* Kapitel 10, Springer-Verlag, 2005.

[5] Olav Geil *"On codes from norm-trace curves"*, Finite Fields and Their Applications, 2003, 351-371.

[6] Tom Høholdt, Jørn Justesen *"A course in error-correcting codes"*, European Mathematical Society, 2004.

[7] David C. Lay *"Linear algebra and its applications - Second edition update"*, Addison Wesley Longman, 2000.

[8] Rudolf Lidl, Harald Niederreiter *"Introduction to finite fields and their applications"*, Cambridge University Press, 1986.

[9] Tom Høholdt, Olav Geil *"Footprints or generalized Bezout's theorem"*, IEEE Transactions on information theory, Vol.46, No. 2, March 2000.

[10] Tom Høholdt, Jacobus H. van Lint, Ruud Pellikaan, *"Algebraic Geometry Codes* Kapitel 10 i *"Handbook of Coding Theory"* Volume I af V.S. Pless, W.C. Huffman, NH Elsevier Science B.V., 1998.