Hovudoppgåve

Eli Winjum
Institutt for Informatikk
Universitetet i Bergen

1995

Vekthierarkiet for nokre kodeklassar

Takk til Nettdivisjonen Region Vest,
Telenor AS

for permisjonen som gjorde
det muleg for meg å ta
hovudfag !

Takk til professor Tor Helleseth
ved Institutt for Informatikk

for svært inspirerande og god
rettleiing og oppfølgjing
- og for heile tida å ha synt
interesse for arbeidet mitt med
hovudoppgåva !

Bergen 1. desember 1995

Eli Winjum

Innhald

Kapittel 1

Innleiing

1.1 Feilkorrigerande kodar

I eit kommunikasjonssystem vert informasjon sendt frå ei kjelde til ein mottakar over ein kanal. Støy på kanalen medfører at mottekne data ikkje alltid samsvarar med dei sende. Å avgjera kva melding som vart sendt på bakgrunn av mottekne data, vert det grunnleggjande problemet dei feilkorrigerande kodane skal løysa. Ein kodar meldinga, informasjons-symbola, ved å leggja til ekstra symbol, redundans. Ved hjelp av redundansen skal så mottekne data kunna gje ei best muleg tilnærming til den sende meldinga.

Ei enkel koding vil vera å repetera kvart einskild symbol mange gonger. Dersom ein repeterer mange nok gonger, og kanalen ikkje har for mykje støy, kan ein no ved å telja opp mottekne symbol, med stort sannsyn avgjera symbola frå kjelda. Prisen for ei slik enkel koding og dekoding er tida det tek å senda meldinga. Raten, informasjons-symbol pr sende symbol, vert lågare til fleire gonger symbola vert repetert. Vi ynskjer *både* enkel koding/dekoding *og* ein rate nær kapasiteten til kanalen.

C. Shannon synte alt i 1948 at påliteleg kommunikasjon er muleg ved einkvar rate, dersom raten er lågare enn kanalkapasiteten. Det finns såleis kodar som sikrar påliteleg kommunikasjon. Å konstruera desse kodane er eit av måla for forskinga innan kodeteori.

Det kan skiljast mellom feildetekterande og feilkorrigerande kodar. Eit kommunikasjonssystem som brukar ein feildetekterande kode, vil krevja at symbolet vert sendt på nytt når ein feil vert funnen. Ein feilkorrigerande kode derimot, skal både detektera og korrigera feilen. Vanlegvis er dette ei langt meir krevjande oppgåve. Optimal feilkorrigering vert rekna som eit svært vanskeleg problem. Effektive dekodingsalgoritmar er funne berre for få kjende kodeklassar. Dette er ei årsak til at dei fleste kommunikasjonssystem framleis nyttar feildetekterande kodar kombinert med retransmisjon.

Det finns to grunnleggjande metodar for koding, blokk-koding og konvolusjons-koding. Medan ein konvolusjonskodar nyttar foregåande symbolsekvens til å koda inneverande sekvens, er blokk-koding uavhengig av tidlegare symbol. Den koda sekvensen, utsekvensen, som vert sendt over kanalen, vert i beggje tilfelle kalla eit kodeord.

Dei lineære blokk-kodane er mest studerte. Desse kodane har ein indre struktur som gjer det enklare å konstruera og analysera dei enn om ein slik struktur manglar. Ein lineær kode er vanlegvis representert ved ei generatormatrise eller ei paritetssjekkmatrise. Dersom informasjonssekvensar med lengde k skal kodast til kodeord med lengde n, vil dei mulege kodeorda vera alle lineærkombinasjonane av k uavhengige sekvensar av n symbol. Dersom koden har q ulike symbol, vil han ha q^k kodeord. Om $q = 2$, er koden binær. Kodeorda i ein lineær kode kan dermed representerast ved ei k x n generatormatrise, $\underline{G}$, der rekkjene, $\underline{x}$, formar basisen for koden. (n-k) vert redundansen til koden. Det vil alltid finnast ei (n-k) x n paritetssjekkmatrise, $\underline{H}$, slik at dei q^k kodeorda utgjer løysingsrommet til (n-k) lineært uavhengige likningar, $\underline{H}\,\underline{x}^T = \underline{0}^T$.

Vanlegvis nyttar ein symbol frå ein endeleg kropp med q element, der q er ein potens av eit primtal. Kodeorda kan sjåast som vektorar i det n-dimensjonale vektorrommet $F_q^{\,n}$ over F_q. Dersom koden er eit lineært underrom av $F_q^{\,n}$, vil han få ein algebraisk struktur, og ein kan gjera bruk av den omfattande teorien for vektor-rom. Slike lineære kodar vart først konstruert kring 1950.

Sykliske kodar er ein viktig kodeklasse. Ein merkar koordinatposisjonane i eit kodeord som 0, 1,..., n -1 og ser posisjonane som ein sykel der 0 følgjer n -1.Ein lineær kode er syklisk dersom det for alle kodeord, $\underline{c} = (c_0, c_1,..., c_{n-1})$, gjeld at også kodeordet, $\underline{c} = (c_{n-1}, c_0,..., c_{n-2})$, er med i koden. Det andre kodeordet er eit syklisk skift av koordinatposisjonane i det første. Ein kan no identifisera kvart kodeord med q-ære polynom over F_q. Relasjonen mellom eit kodeord og eit polynom, $\underline{c} \leftrightarrow c(x)$, kan uttrykkjast $(c_0, c_1,..., c_{n-1}) \leftrightarrow c_0 + c_1x +...+ c_{n-1}x^{n-1}$.

Ein syklisk kode over $F_q^{\,n}$ kan representerast ved *eitt* polynom. Det finns eit unikt monisk polynom, $g(x)$, i ringen $F_q\,[x]/(x^n\text{-}1)$ slik at $g(x)|(x^n\text{-}1)$ og slik at $c(x)$ er eit kodeord i koden viss og berre viss $g(x)|c(x)$. $g(x)$ vert kalla generatorpolynomet til koden. Paritetssjekkpolynomet, $h(x)$, er gitt av $h(x) = (x^n\text{-}1)/g(x)$. $c(x)$ er eit kode-ord i koden viss og berre viss $h(x)c(x) = 0$ i $F_q\,[x]/(x^n\text{-}1)$.

Kodane som vert handsama i denne oppgåva, er binære, lineære, sykliske kodar.

1.2 Hammingvekt og minimumsavstand

Hammingvekta til ein vektor over F_q er talet på koordinatposisjonar som ikkje er "0". Hammingavstanden mellom to vektorar er talet på koordinatposisjonar der dei to vektorane er ulike. Minimumsavstanden til ein kode er den minste Hamming-avstanden mellom to kodeord i koden. Minimumsavstanden til ein lineær kode er lik den minste Hammingvekta (ulik 0) til eit kodeord i koden.

Minimumsavstanden, d, til ein kode er ein svært viktig parameter ettersom han avgjer kor mange feil koden kan korrigera. Til større minimumsavstanden er, til fleire feil kan koden korrigera. På den andre sida vil talet på mulege kodeord med gitt lengde reduserast.

1.3 Vekthierarki

Støttevekta til ein vektor over F_q er lik Hammingvekta til vektoren. Støtta til eit underrom i F_q^n er mengda av koordinatposisjonar der ikkje alle vektorar i underrommet er "0".

Dersom D er ein r-dimensjonal underkode i ein lineær kode, C, over F_q , så er støtta til D, $X(D)$, definert som mengda av koordinatposisjonar der ikkje alle kodeord i D er "0". Det minste talet på slike koordinatposisjonar for $1 \le r \le k$ vert kalla den r'te minimums støttevekta til koden, eller den r'te generaliserte Hammingvekta, d_r. Settet $\{d_1,d_2,...,d_k\}$, der d_1 er minimumsavstanden til koden, gir vekthierarkiet. $|X(D)|$ kan og sjåast som talet på ikkje-null-søyler i generatormatrisa for D.

Den r'te generaliserte Hammingvekta til ein lineær kode er ein ny parameter som først vart introdusert av V.K. Wei i 1991 [13]. Liknande eigenskapar for irredusible sykliske kodar vart studerte alt i 1977 av T. Helleseth, T. Kløve og J. Mykkeltveit [6].

Motivasjonen for å studera vekthierarkiet kan vera

i) applikasjonar innan kryptografi. Vekthierarkiet er ein viktig parameter for å avgjera kor sikkert systemet vil vera på ein avlytta kanal (Wire-tap Channel type II).

ii) trellisdekoding av blokk-kodar. Vanlegvis må dekoding av blokk-kodar baserast på at energien til signala frå kanalen først vert omsett til binære verdiar (hard decision). Ein misser dermed viktig informasjon om signalenergien. Trellisdekoding, som vert nytta for konvolusjonskodar, gjer det derimot muleg å bruka

verkelege verdiar i dekodinga (soft decision). Dette er den viktigaste fordelen konvolusjonskodar har framfor blokk-kodar. Om vekthierarkiet for ein blokk-kode er kjent, er det muleg å finna kompleksitet og diagram for trellis-dekoding. Då kan ein nytta all informasjon om signalenergien, også for ein blokk-kode.

iii) forkorting av kodar (shortening).

iv) konstruksjon av kodar for nokre typar kanalar (switched Multiple-Access Channel).

Ettersom vekthierarki er eit nytt felt innan kodeteorien, er det førebels få kodar der denne parameteren er funnen. Av kodar der heile vekthierarkiet er kjent, kan nemnast

i)	Simplex-kodane	[13]
ii)	Reed-Muller-kodane	[13]
iii)	Kasami-kodane	[9]
iv)	Semiprimitive kodar	[10]
v)	Kodar som held Griesmer-skranken	[7]
vi)	Nokre få andre klassar	[12]

For ein viktig kodeklasse som BCH-kodane, er vekthierarkiet berre delvis kjent for nokre av kodane. For dei primitive dobbel-feilkorrigerande er 2. og 3. generaliserte Hammingvekt kjent. For dei duale kodane til dei binære dobbel-feilkorrigerande BCH-kodane er den 2. generaliserte Hammingvekta funnen [4]. Opp til 5. generaliserte Hammingvekt er funnen for dei primitive, binære tre-feilkorrigerande BCH-kodane [3].

Kapittel 2

Om oppgåva

2.1 Definisjon

Oppgåva er å studera vekthierarkiet til to spesielle kodeklassar. Den eine klassen er kodar der paritetssjekkpolynomet er produktet av to primitive polynom med grad m. Den andre klassen er irredusible sykliske kodar. Vi er interesserte i å finna eit underrom med størst muleg dimensjon i dei aktuelle klassane.

2.2 Avgrensing

Kodeklassen der paritetssjekkpolynomet er produktet av to primitive polynom, inneheld dei duale til dei dobbel-feilkorrigerande BCH-kodane. Dette er ei viktig årsak til at kodeklassen er interessant. Dersom vekthierarkiet til ein kode er funne, vil ein ved hjelp av dualitets-teoremet enkelt kunna rekna ut vekthierarkiet til den duale koden. Som nemnt i innleiinga er lite av dette førebels kjent for BCH-kodane. Y. Niho har funne vektdistribusjonen for fleire kodar der $h(x) = m_1(x)m_s(x)$ [11]. Vi har valt å studera to av desse kodane, der

$$s = 2^{l+1}-1,\ m = 2l,$$

og der

$$s = (2^l-1)(2^{2l}+1) + 2,\ m = 4l.$$

Frå den andre kodeklassen har vi valt kodane med lengde $n = n_1(2^l-1)$. Vi har her skilt ut tre underklassar der

$$k/l = 2,$$
$$k/l = n_1$$

og der

$$k/l = n_1-1.$$

Desse kodane kan sjåast som ei undergruppe av BCH-kodane. T. Helleseth, T. Kløve og J. Mykkeltveit har funne vektdistribusjonen til desse kodane [6].

Oppgåva er dermed avgrensa til kodar der vektdistribusjonen er kjent, og der det difor i utgangspunktet finns teoretisk analyse. Vekthierarkiet er nyleg funne for den irredusible sykliske koden der $k/l = 2$ [10]. For dei andre kodane som skal studerast, er vekthierarkiet ukjent.

Oppgåva er vidare avgrensa til binære kodar.

2.3 Metode

I arbeida som omhandlar vekthierarkiet til andre kodeklassar, har forfattarane nytta nokså ulike innfallsvinklar, metodar og teknikkar. Det finns truleg ingen allment "god" metode eller framgangsmåte.

2.3.1 Numeriske data

Vi har valt å starta med å finna numeriske data. Til dette formålet er det laga ei rekkje program. Dei aktuelle kodane, evt. definerte underrom i dei, vert genererte ved hjelp av ulike metodar. $g(x)$, $h(x)$ og matematiske likningar er nytta for å generera kodane. Ved å variera parametrar kunne strukturar og eigenskapar ved kodane og ulike underrom i dei, avslørast.

Eit program for å finna tilnærmingar til vekthierarkiet er sjølvsagt også laga. Med utgangspunkt i Griesmer-skranken reknar programmet fortløpande ut optimal verdi for d_r, $1 \le r \le k$, og leitar systematisk etter underrom som tilfredsstiller desse verdiane. Programmet er testa på ein del kodar der vekthierarkiet er kjent. I desse tilfella vert D_r ,$1 \le r \le k$, funnen etter *ein* iterasjon. Tabellane i vedlegga IV - VI er resultat frå dette programmet. Kvart resultat er stadfesta gjennom svært mange iterasjonar. Identiske resultat er dessutan oppnådd for ekvivalente variantar av kodane. Det er difor grunn til å tru at programmet gir gode tilnærmingar til vekthierarkiet.

Desse programma har også vore eit godt verktøy for å finna ut kva parametrar som påverkar støttevekta til eit r-dimensjonalt underrom.

Programma er laga i programmeringsspråket C.

2.3.2 Teoretisk analyse

Saman med dei nemnde arbeida vedrørande vektdistribusjonen har dei numeriske resultata vore grunnlag for ein teoretisk analyse. Samstundes har arbeidet med ana

lysen heile tida ført til nye programvariantar og søk for å testa ulike idear og teoriar.

Målet for det teoretiske arbeidet har sjølsagt vore å prova d_r matematisk for eit størst muleg underrom. Eit delmål har vore å prova at dei numeriske resultata er øvre skrankar for d_r, slik at desse kan generaliserast til kodar med vilkårlege lengder. For beggje kodeklassane er det vist korleis ein ved å velja visse kodeord til generatormatrisa, kan setja saman underrom med gitt støttevekt. For å visa dette, har det vore naudsynt å studera både vektoppteljaren og kodeorda nøye. Arbeidet har ført til ein metode som gir gode øvre skrankar for d_r. Det er sterk grunn til å tru at dei øvre skrankane som er prova for Niho-kodane, om $k/4+1 \leq r \leq k$, gjeld med likskap. Metoden som er utvikla, kan truleg nyttast på ein langt større kodeklasse enn Niho-kodane.

Mesteparten av det teoretiske arbeidet har vore knytt til å prova $d_{k/4+1}$ for Niho-koden der $s = 2^{l+1}-1$. Dette har vore rekna som ein flaskehals med omsyn til å prova heile vekthierarkiet for beggje Niho-kodane. Ei rekkje innfallsvinklar har vore freista, utan at det har ført til det ønska resultatet. Derimot har arbeidet gitt svært mykje og detaljert kunnskap om beggje kodane.

For å prova vekthierarkiet til dei irredusible sykliske kodane, var framgangsmåten å først finna øvre skrankar for d_r etter same metode som vart brukt for Niho-kodane. Ein nedre skranke for d_r vart deretter funnen. Det synte seg å vera samsvar mellom øvre og nedre skranke.

2.4 Gjennomgang av oppgåva

Kapittel 3. I dette kapitlet definerer vi ein del sentrale omgrep vedrørande minimumsavstand og vekthierarki. Kapitlet gir også oversikt over ein del skrankar og andre viktige resultat innan dette feltet. Oversikten er avgrensa til resultat som er brukt i arbeidet med oppgåva.

Kapittel 4. Dette kapitlet kan reknast som hovudkapittel i oppgåva. Vi studerer her vekthierarkiet til dei to Niho-kodane. Som introduksjon gir vi i første avsnittet eit kort samandrag av ein del resultat frå arbeidet til Y. Niho. Deretter føl eit avsnitt der definisjonar og viktige resultat som gjeld beggje kodane er samla. Vi finn så d_r , om $1 \leq r \leq k/4$, for deretter å gå gjennom metoden som skal nyttast til å finna øvre skrankar for d_r , om $k/4+1 \leq r \leq k$.

Dei to kodane vert så handsama kvar for seg. Vi prøver å klarleggja problema kring $d_{k/4+1}$, før dei øvre skrankane for d_r vert funne.

I samandraget for kapitlet prøver vi først og fremst å summera opp problema som må løysast for å prova vekthierarkiet til desse kodane.

Kapittel 5. Dette kapitlet er bygt opp på same vis som kapittel 4, men temaet er her vekthierarkiet til irredusible sykliske kodar. Vi presenterer først nokre viktige resultat frå arbeidet til T. Helleseth, T. Kløve og J. Mykkeltveit. På grunnlag av dette finn vi d_r , om $1 \le r \le l$, og går gjennom ein metode for å finna nedre skrankar. Vi finn så d_r , om $l+1 \le r \le k$, for kvar av dei tre underklassane. Ei oppsummering følgjer i samandraget for kapitlet.

Kapittel 6. Kapitlet gir ei oppsummering av heile oppgåva og evaluerer resultata som er oppnådd.

Vedlegg I. Ein oversikt over notasjonar og ein del ord og uttrykk som er brukt i oppgåva.

Vedlegg II. Nokre resultat vedrørande $d_{k/4+1}$ for Niho-koden der $s = 2^{l+1}-1$.

Vedlegg III. Nokre resultat vedrørande $d_{k/4+1}$ for Niho-koden der $s = (2^l-1)(2^{2l}+1) + 2$.

Vedlegg IV. Tabellar med numeriske resultat for alle kodar der paritetssjekkpolynomet $h(x) = m_1(x)m_s(x)$, $m \le 8$ og $\gcd(n, s) = 1$.

Vedlegg V. Tabellar med numeriske resultat for dei to Niho-kodane.

Vedlegg VI. Tabellar med numeriske resultat for dei irredusible sykliske kodane.

Teorem, lemma, korollar, definisjonar og døme er nummerert i same serien. Det er nytta eigen nummerserie for figurarar.

2.5 Resultat

Niho-kodar, $h(x) = m_1(x)m_s(x)$.

d_r er funnen for $1 \le r \le l$. Gode øvre skrankar er funne for $l+1 \le r \le k$.

Kodar der $s = 2^{l+1}-1$, $m = 2l$, C = $[2^{2l}-1, 4l, 2^{2l-1} - 2^l]$:

$$\begin{aligned}
d_r &= (2^l - 2)(2^l - 2^{l-r}), && \text{om } 1 \le r \le l.\\
d_r &\le (2^l-2)(2^l-1) + (2^l - 2^{2l-r}), && \text{om } l+1 \le r \le 2l,\\
&\le (2^l-1)(2^l-1) + (2^l - 2^{3l-r}), && \text{om } 2l+1 \le r \le 3l,\\
&\le 2^{2l}(2^l-1) + (2^l - 2^{4l-r}), && \text{om } 3l+1 \le r \le 4l.
\end{aligned}$$

Kodar der $s = (2^l-1)(2^{2l}+1) + 2$, $m = 4l$, C = $[2^{4l}-1, 8l, 2^{4l-1} - 2^{3l-1}]$:

$$\begin{aligned}
d_r &= (2^{2l} - 2^l)(2^{2l} - 2^{2l-r}), && \text{om } 1 \le r \le 2l.\\
d_r &\le (2^{2l}-1)(2^{2l} - 2^l) + (2^{2l} - 2^{4l-r}), && \text{om } 2l+1 \le r \le 3l,\\
&\le 2^{2l}(2^{2l} - 2^l) + (2^{2l} - 2^{5l-r}), && \text{om } 3l+1 \le r \le 4l,\\
&\le (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 2^{5l-r}), && \text{om } 4l+1 \le r < 5l,\\
&\le (2^{2l}-1)(2^{2l}-1) + (2^{2l} - 2^{6l-r}), && \text{om } 5l \le r \le 6l,\\
&\le 2^{2l}(2^{2l}-1) + (2^{2l} - 2^{8l-r}), && \text{om } 6l+1 \le r \le 8l.
\end{aligned}$$

Irredusible sykliske ($n_1(2^l-1)$, k)-kodar.

d_r er funnen for $1 \le r \le k$.

Kodar der $k/l = 2$:

$$\begin{aligned}
d_r &= (n_1-1)(2^l - 2^{l-r}), && \text{om } 1 \le r \le l,\\
&= (n_1-1)(2^l-1) + (2^l - 2^{2l-r}), && \text{om } l+1 \le r \le k.
\end{aligned}$$

Kodar der $k/l = n_1$:

$$\begin{aligned}
d_r &= (2^l - 2^{l-r}), && \text{om } 1 \le r \le l,\\
&= t(2^l-1) + (2^l - 2^{(t+1)l-r}), && \text{om } l+1 \le r \le k,\ t = \lfloor r / l \rfloor.
\end{aligned}$$

Kodar der $k/l = n_1-1$:

$$\begin{aligned}
d_r &= 2(2^l - 2^{l-r}), && \text{om } 1 \le r \le l,\\
&= (t+1)(2^l - 1) + (2^l - 2^{(t+1)l-r}), && \text{om } l+1 \le r \le k,\ t = \lfloor r / l \rfloor.
\end{aligned}$$

Kapittel 3

Definisjonar, skrankar og viktige resultat

3.1 Definisjonar

Dette avsnittet gir formelle definsjonar for ein del omgrep brukt i oppgåva.

Hammingavstand, $d(\underline{x}, \underline{y})$. Lat $\underline{x} = (x_0, x_1,..., x_{n-1})$ og $\underline{y} = (y_0, y_1,..., y_{n-1})$ vera to vektorar i F_q^n . Hammingavstanden mellom dei er gitt av

$$d(\underline{x}, \underline{y}) = |\{1 \leq i \leq n \mid x_i \neq y_i \}|.$$

Hammingvekt, $w(\underline{x})$. Lat $\underline{x}$ vera ein vektor i F_q^n . Hammingvekta til $\underline{x}$ er gitt av

$$w(\underline{x}) = d(\underline{x}, \underline{0}).$$

Minimumsavstand, d. Lat C vera ein kode over F_q . Minimumsavstanden til C er gitt av

$$d = \min\{d(\underline{x}, \underline{y}) \mid \underline{x} \in C, \underline{y} \in C, \underline{x} \neq \underline{y}\}.$$

Feilkorrigerande kapasitet, t. Den feilkorrigerande kapasiteten til ein kode er gitt av

$$t = \lfloor (d-1)/2 \rfloor .$$

Ein t-feilkorrigerande kode rettar t feil.

Minimumsvekt. Den minste Hammingvekta (ulik 0) til eit kodeord i C.

$$= \min\{w(\underline{x}) \mid \underline{x} \in C\}.$$

Maksimumsvekt. Den største Hammingvekta til eit kodeord i C.

$$= \text{maks}\{w(\underline{x}) \mid \underline{x} \in C\}.$$

w_t Den t'te minste Hammingvekta til eit kodeord i C. w_1 er minimumsvekta.

Vektoppteljar, $A(z)$. Vektoppteljaren til ein kode spesifiserer talet på kodeord av kvar muleg vekt, 0,1,...n, og er gitt av

$$A(z) = \sum_{i=0}^{n} A_i z^i = \sum_{\underline{c} \in C} z^{w(\underline{c})} .$$

Dual kode, $C^{\perp}$. Lat C vera ein [n, k, d]- kode over F_q. Den duale koden til C er definert av

$$C^{\perp} = \{\underline{x} \in F_q^{\,n} \mid (\underline{x}, \underline{c}) = 0 \text{ for alle } \underline{c} \in C\},$$

der $(\underline{x}, \underline{c})$ er indreproduktet $\sum_{i=0}^{n-1} x_i c_i$ i $F_q^{\,n}$.

Støtte, $X(D)$. Lat C vera ein [n, k, d]- kode over F_q og D ein underkode i C. $X(D)$ er mengda av koordinatposisjonar der ikkje alle kodeord i D er "0".

Støttevekt. Støttevekta til $D \subseteq C$ er definert av

$$|X(D)|.$$

***r*'te generaliserte Hammingvekt**, $d_r(C)$, er definert av

$$d_r(C) = \min \{|X(D)| \mid D \subseteq C \text{ , } \dim(D) = r\}, \; 1 \le r \le k,$$

der $d_1 = d$ = minimumsavstanden til C.

Vekthierarki. Vekthierarkiet til ein kode er gitt av dei r'te generaliserte Hamming-vektene $\{d_1, d_2, ..., d_k\}$.

Kjedevilkåret. Ein kode, C, tilfredsstiller kjedevilkåret dersom det finns ei kjede, $D_1 \subseteq D_2 \subseteq ... \subseteq D_k$., slik at $|X(D_r)| = d_r(C)$, $\dim(D_r) = r$.

Tracefunksjonen, $Tr_e^m(x)$, $F_{q^m} \to F_{q^e}$, er definert av

$$Tr_e^m(x) = \sum_{i=0}^{m-1} x^{q^{ie}} \text{ , der } x \in GF(q^m).$$

Krysskorrelasjonsfunksjonen, $D_s(y)$, mellom to maksimale lineære rekursive sekvensar er definert av

$$D_s(y) = \sum_{x \in GF(2^m)} (-1)^{Tr(xy+x^s)} \quad \text{for ein } s, \quad \gcd(s, 2^m - 1) = 1.$$

Minimumspolynom, $m_i(x)$, Minimumspolynomet til α^i er definert av

$m_i(x) = \prod (x - \alpha^{2^i})$, der α er eit element av orden 2^m -1.

3.2 Skrankar

Griesmer-skranken. Lat C vera ein $[n, k, d]$- kode over F_q med k ≥ 1. Då er

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = g(k, d). \qquad [5]$$

Generaliserte Griesmer-skranken. Lat C vera ein $[n, k, d]$- kode over F_q.
For $1 \leq r \leq k$,

$$n \geq d_r(C) + \sum_{i=1}^{k-r} \left\lceil \frac{q-1}{q^i(q^r-1)} d_r \right\rceil.$$

For $r = 1$ vert dette den ordinære Griesmer-skranken. [7]

Singleton-skranken. Lat C vera ein $[n, k, d]$- kode over F_q. Då er

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

Generaliserte Singleton-skranken. Lat C vera ein $[n, k, d]$- kode over F_q. Då er

$d_r \leq n - k + r$.

For $r = 1$ vert dette den ordinære Singleton-skranken. [1]

3.3 Viktige resultat

Dette avsnittet gir ein oversikt over ein del viktige resultat som er nytta i oppgåva.

MacWilliams-identiteten. Lat $A(z)$ vera vektoppteljaren til ein (n, k)-kode, C, og lat $B(z)$ vera vektoppteljaren til den duale koden , $C^{\perp}$. $B(z)$ er gitt av

$$B(z) = \frac{1}{|C|} \sum_{i=0}^{n} A_i (1-z)^i (1+(q-1)z)^{n-i} . \qquad [1]$$

Dualitetsteoremet. Lat C vera ein $[n, k, d]$- kode over F_q. Relasjonen mellom vekthierarkiet til C og den duale koden, $C^{\perp}$, er gitt av

$$\{ d_r(C) \mid 1 \le r \le k\} = \{1,2,...n\} \setminus \{n+1 - d_r(C^{\perp}) \mid 1 \le r \le n-k \}. \qquad [13]$$

Lat C vera ein $[n, k, d]$- kode over F_q. For $1 \le r \le k$,

$$1 \le d_1 < d_2 < ... < d_k \le n. \qquad [13]$$

Lat C vera ein $[n, k, d]$- kode over F_q og lat U vera eit underrom i C. For $1 \le r \le k$,

$$|X(U)| = \frac{1}{2^{r-1}} \sum_{\underline{u} \in U} w(\underline{u}) . \qquad [9]$$

Lat C vera ein $[n, k, d]$- kode over F_q. For $1 \le r \le k$,

$$(q^r-1)\, d_{r-1} \le (q^r - q)\, d_r . \qquad [7]$$

Lat C vera ein $[n, k, d]$- kode over F_q . Dersom C møter Griesmer-skranken, gjeld følgjande

i) C møter den generaliserte Griesmer-skranken for $1 \le r \le k$.

ii) $$d_r = \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil = g(r, d). \qquad [7]$$

Då Simplex-koden møter Griesmer-skranken, er vekthierarkiet til Simplex-koden gitt av

$$d_r = \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil, \text{ for } 1 \le r \le k. \qquad [7]$$

Eit r-dimensjonalt underrom i ein kode kan sjåast som ein [d_r, r, d_1]-kode dersom vi fjernar alle posisjonar der alle kodeord har "0". Ved å bruka Griesmer-skranken på ein slik underkode, får vi følgjande allmene nedre skranke for d_r

$$d_r \geq \sum_{i=0}^{r-1} \left\lceil \frac{d}{q^i} \right\rceil . \qquad [7]$$

Lat C vera ein [n, k, d]- kode over F_q . Dersom C møter Singleton-skranken (dvs dersom C er ein MDS-kode), gjeld følgjande

i) C møter den generaliserte Singleton-skranken for $1 \leq r \leq k$.

ii) $d_r = n - k + r$. [1]

Lat C vera ein binær [n, k, d]- kode. Dersom $n = g(k, d)$, vil C tilfredsstilla kjede-vilkåret. [8]

Lat C vera ein binær [n, k, d]- kode. Dersom $n = g(k, d) + 1$, vil C tilfredsstilla kjedevilkåret. [8]

Lat $a \in$ GF(q^e), $x, y \in$ GF(q^m). Tracefunksjonen har då følgjande eigenskapar

$Tr_e^m(x) \in GF(q^e)$.

$Tr_e^m(x + y) = Tr_e^m(x) + Tr_e^m(y)$.

$Tr_e^m(x^{q^e}) = Tr_e^m(x)$.

$Tr_e^m(ax) = a\, Tr_e^m(x)$. [1] [11]

Kapittel 4

Niho-kodar

4.1 Introduksjon

Vi skal studera vekthierarkiet til to Niho-kodar, ei undergruppe av kodeklassen der paritetssjekkpolynomet er produktet av to primitive polynom med grad m, dvs

$$h(x) = m_1(x)m_s(x), \ \gcd(s, 2^m-1) = 1.$$

Dei to kodane kan då karakteriserast ved s, der

$$s = 2^{l+1}-1, \ m = 2l,$$

og

$$s = (2^l-1)(2^{2l}+1) + 2, \ m = 4l.$$

Å finna verdiane til krysskorrelasjonsfunksjonen mellom to maksimale lineære rekursive sekvensar er ekvivalent med å finna heile vektoppteljaren til ein kode der paritetssjekkpolynomet er produktet av rekursjonspolynoma til dei to maksimalsekvensane. Y. Niho har funne vektoppteljaren til ei rekkje av desse kodane ved å studera krysskorrelasjonsfunksjonen ved ulike verdiar for s [11].

Ein sekvens,$\{c_j\}$, er generert ved lineær rekursjon av polynomet

$$f(x) = x^m + a_1x^{m-1} + a_2x^{m-2} + \ ... + a_m \ .$$

Lat $f(x)$ vera irredusibelt. Perioden til sekvensen,$\{c_j\}$, er det minste positive heiltalet p slik at $c_{j+p} = c_j$ for alle j. p er då det minste positive heiltalet slik at $f(x)$ deler (x^p+1). Sidan $f(x)$ er irredusibelt, vil perioden til sekvensen vera ein divisor i (2^m-1). Når $p = 2^m-1$, er polynomet, $f(x)$, primitivt. Rekursjonspolynomet, $f(x)$, genererer ein maksimal lineær rekursiv sekvens viss og berre viss $f(x)$ er primitivt.

Den maksimale lineære rekursive sekvensen, $\{c_j\}$, $0 \le j \le 2^m - 2$, kan representerast ved

$$c_j = Tr_1^m(\beta\alpha^j),$$

der

$Tr_e^m(x)$, er tracefunksjonen $F_{2^m} \to F_{2^e}$,
α er ei rot i $f(x)$ og β er eit element i $GF(2^m)$.

4.2 Definisjonar og grunnleggjande resultat

Lemma 4.2.1, 4.2.2, 4.2.4 og Definisjon 4.2.5, 4.2.7, 4.2.8 er henta frå [11]. Vi tek ikkje med bevisa her.

Lemma 4.2.1. Lat $\sigma \in GF(2^m)$. Då er

$$\sum_{x \in GF(2^m)} (-1)^{Tr(x\sigma)} = \begin{cases} 2^m & om\ \sigma = 0, \\ 0 & om\ \sigma \neq 0. \end{cases}$$

Halvparten av elementa har trace = 1, den andre halvparten trace = 0.

Lemma 4.2.2. Når $m = 2l$, kan elementa i $GF(2^l)\backslash\{0\}$ representerast unikt som $x = \alpha\beta$, der $\alpha \in GF(2^l)\backslash\{0\}$, og β er ei (2^l+1)'te einingsrot i $GF(2^{2l})$.

Korollar 4.2.3. Lat $h(x) = m_1(x)m_s(x)$ og $\gcd(s, 2^m-1) = 1$. Vi får frå Lemma 4.2.2 at

$n = 2^{2l}-1 = (2^l-1)(2^l+1)$.
$x^{2^{2l}-1} = 1$, $x = \alpha\beta$.
$\alpha^{2^l-1} = 1$.
$\beta^{2^l+1} = 1$.

Lemma 4.2.4. Lat $m = 2l$, $\alpha \in GF(2^l)$ og $\beta \in GF(2^{2l})$. Då vil

$$Tr_1^{2l}(\alpha\beta) = Tr_1^l(\alpha(\beta + \beta^{2^l})).$$

Lat $m = 2l$, $\alpha \in GF(2^l)$, $\beta \in GF(2^{2l})$, $\beta^{2^l+1}=1$ og $\gcd(s, 2^l-1) = 1$. Niho syner vidare at om $s \equiv 2^k \bmod (2^l-1)$ for ein k, $0 \le k \le l-1$, og $s \equiv t \bmod (2^l+1)$, får vi følgjande

i) $Tr_1^{2l}(y\beta\beta + \alpha^s\beta^s) = Tr_1^{2l}(y\beta\beta + \alpha\beta^{t2^{-k}}) = Tr_1^{2l}(\alpha(y\beta + \beta^{t2^{-k}}))$.

ii) $$D_s(y) = 1 + \sum_{\substack{\beta \in GF(2^{2l}) \\ \beta^{2^l+1}=1}} \sum_{\alpha \in GF(2^l)} (-1)^{Tr_1^{2l}(\alpha(y\beta+\beta^{t2^{-k}}))} - (2^l+1),$$

der $Tr_1^{2l}(\alpha(y\beta + \beta^{t2^{-k}})) = Tr_1^{l}(\alpha(y\beta + \beta^{t2^{-k}} + y^{2^l}\beta^{-1} + \beta^{-t2^{-k}}))$.

Merk. $(y\beta + \beta^{t2^{-k}} + y^{2^l}\beta^{-1} + \beta^{-t2^{-k}})$
$= Tr_l^{2l}(y\beta + \beta^{t2^{-k}}) \in GF(2^l)$.

Vi går i resten av avsnitt 4.2 og i avsnitta 4.3 og 4.4 ut frå at $m = 2l$, dvs at $l = k/4$. Alle definisjonar, bevis og døme kan tilpassast koden der $m = 4l$ ved å erstatta l med $2l$.

Definisjon 4.2.5.
Lat $y \in GF(2^{2l})$. $N_\beta(y)$ er talet på distinkte løysingar β i $GF(2^{2l})$ til følgjande likningar

$$y\beta + \beta^{t2^{-k}} + y^{2^l}\beta^{-1} + \beta^{-t2^{-k}} = 0. \qquad (4.2.1)$$

$$\beta^{2^l+1} = 1. \qquad (4.2.2)$$

Definisjon 4.2.6.
Lat $B = \{v \mid v^{2^l+1} = 1\} \subseteq GF(2^{2l})$.

Definisjon 4.2.7.
Lat N_i vera talet på gonger $N_\beta(y) = i$, når y går gjennom $GF(2^{2l})$.

Definisjon 4.2.8.
Lat $h(D_s)$ vera talet på forekomstar av kvar verdi av $D_s(y)$.

Niho syner at $D_s(y) = 2^l(N_\beta(y) - 1)$. Vi kan då finna vektdistribusjonen på følgjande måte. Lat α vera ei primitiv $(2^{2l}-1)$'te rot og $a \in GF(2^{2l})$. Lat $\{c_j\}$, $0 \le j \le 2^m - 2$, vera ein sekvens der

$$c_j = Tr_1^{2l}(a\alpha^j + \alpha^{sj}) = f(\alpha^j).$$

Lat $f(x) = Tr_1^{2l}(ax + x^s)$. Då er

$$\sum_{x \in GF(2^{2l})} (-1)^{f(x)} = 2^{2l} - 2w(\{c_j\}),$$

der $w(\{c_j\})$ er Hammingvekta til sekvensen $\{c_j\}$.

i ulike vekter korresponderer til dei *i* ulike verdiane for $\Delta_s(y)$, dvs. til dei *i* ulike verdiane for $N_b(y)$. Desse kan enkelt finnast ved

$$\begin{aligned} w(\{c_j\}) &= (2^{2l} - \Delta_s(y)) / 2 \\ &= (2^{2l} - 2^l (N_b(y) - 1))/2 \\ &= 2^{2l-1} - 2^{l-1} (N_b(y) - 1). \end{aligned}$$

4.3 Vekthierarkiet, $d_1 ... d_{k/4}$.

Definisjon 4.3.1.
Lat $a \in GF(2^l)$ og lat $b \in B$. Likning (4.2.1) vil ta ulike former når *s* varierer. I dei to tilfella vi skal sjå på er uttrykket, $Tr_1^l (a \; Tr_l^{2l} (yb + b^{t2^{-k}}))$, utgangspunkt for likninga. Lat *C* vera ein Niho-kode. Ein posisjon i eit kodeord, $c(a,b)$, i *C* er gitt av

$$Tr_1^l (a \; Tr_l^{2l} (yb + b^{t2^{-k}})),$$

og koderordet vert generert ved at a går gjennom $GF(2^l)$, og b går gjennom *B*. Vi definerer då

$$f_y(b) = Tr_l^{2l} (yb + b^{t2^{-k}}).$$

$$C^* = \{ c^*(y) \mid c^*(y) = ((f_y(1), f_y(b), ..., f_y(b^{2^l}))\}.$$

C^* er ein $(2^l + 1, 4)$-kode over $GF(2^l)$. Det er 1-1-relasjon mellom eit kodeord i *C* og eit kodeord i C^*. *C* kan sjåast som "trace-koden" til C^*.

Definisjon 4.3.2
Lat C_r vera eit *r*-dimensjonalt underrom i *C* med generatormatrise $\underline{G}_r$, og C^*_r eit *r*-dimensjonalt underrom i C^* med generatormatrise $\underline{G}^*_r$, $1 \le r \le k$.

Teorem 4.3.3. Vekthierarkiet til beggje kodane er gitt av

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 = g(r,d), \text{ om } 1 \le r \le l.$$

Bevis. Vi ser på uttrykket

$Tr_1^l (a \; Tr_l^{2l} (yb + b^{t2^{-k}}))$ frå Definisjon 4.3.1.

Lat $0 \le j \le 2^l$. Om vi fikserer b^j, vil den *j*'te komponenten i eit kodeord, $c^*(y)$, i C^* vera gitt av

$$c^*_j(y) = Tr_l^{2l} (yb^j + b^{jt2^{-k}}).$$

Om vi så let α gå gjennom $GF(2^l)\backslash\{0\}$, vil

$$Tr_1^l(\alpha\, Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}))$$

føra til posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ i kodeordet, $c(y)$, i C.

Om $Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}) \neq 0$, vil halvparten av posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ få

$$Tr_1^l(\alpha\, Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}})) = 1,$$

den andre halvparten

$$Tr_1^l(\alpha\, Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}})) = 0.$$

Om $Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}) = 0$, vil *alle* posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ få

$$Tr_1^l(\alpha\, Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}})) = 0.$$

Posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ vil dermed alltid ha vekt 0 eller 2^{l-1}.

Lat $0 \leq j \leq 2^l$. Lat $c^*(y)$ vera eit kodeord i C^* . Posisjonane i kodeordet er gitt av

$$c^*_j(y) = Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}) = f_y(\beta^j).$$

Lat $\delta \in GF(2^l)$. Sidan koden er syklisk, vil det også finnast kodeord, $\delta c^*(y)$, med posisjonar gitt av

$$\delta c^*_j(y) = \delta Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}).$$

Vi ser på den j'te posisjonen i kodeorda, tilsvarande β^j. Dersom $c^*_j(y) = 0$, vil $\delta c^*_j(y) = 0$. Dersom $c^*_j(y) \neq 0$, vil $\delta c^*_j(y) \neq 0$. $\delta c^*_j(y)$ går gjennom $GF(2^l)$ når δ gjer det.

Mengda $\{\delta c^*(y) \mid \delta \in GF(2^l)\}$ vil utgjera eit l-dimensjonalt underrom i C^* sidan

$$c^*_j(y) + \delta c^*_j(y) = (1+\delta)c^*_j(y)$$

som medfører at

$$c^*(y) + \delta c^*(y) = (1+\delta)c^*(y).$$

Underrommet vil innehalda kvart (2^l+1)'te sykliske skift av $c^*(y)$.

Eit slikt underrom karakteriserast ved at

i) Kodeorda har $Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}) = 0$ i dei same posisjonane.

ii) Kodeorda vil vera ulike i posisjonar der $Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}) \neq 0$.

Dette tyder at alle kodeorda i underrommet har same vekt. Vi får då at

$$w(c(y)) = w(\delta c(y)),$$

og teoremet følgjer.

Definisjon 4.3.4.
Lat $S^*_l(y)$ vera eit l-dimensjonalt underrom i C^* slik at

$$S^*_l(y) = \{\delta\, c^*(y) \mid \delta \in GF(2^l)\},$$

og $S_l(y)$ det tilsvarande l-dimensjonale underrommet i C.

Korollar 4.3.5. Lat $0 \le j \le 2^l$. Vi ser på den j'te søyla i generatormatrisa for S^*_l. Lat søyla ha rang l over $GF(2)$. Då vert

$$c^*_j(y)_r = Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}}) \neq 0,\ 1 \le r \le l.$$

Sidan alle kodeorda er ulike i denne posisjonen, kan dei tilsvarande posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ i generatormatrisa for S_l sjåast som ei generatormatrise for ein $[2^l\text{-}1,\ l,\ 2^{l-1}]$ Simplex-kode.

Vekthierarkiet til ein $[2^l\text{-}1,\ l,\ 2^{l-1}]$ Simplex-kode er kjent

$$d_r = g(r,d) = \sum_{i=0}^{r-1}\left\lceil \frac{2^{l-1}}{2^i} \right\rceil = 2^l - 2^{l-r},$$

jfr. avsnitt 3.3.

Definisjon 4.3.6.
C^S er ein Simplex-kode med parametrane $[2^l\text{-}1,\ l,\ 2^{l-1}]$. $d_r(C^S)$ vert frå no av brukt om den r'te generaliserte Hammingvekta for denne koden.

Merk. Vektene i koden, C, vil vera ulike multippel av $d_1(C^S)$.
$d_r(C)$ kan sjåast som eit multippel av $d_r(C^S)$, om $1 \le r \le l$.

4.4 Ein metode til å finna øvre skrankar for $d_{k/4+1}...d_k$.

Vi fann i avsnitt 4.3 at

$$d_r = g(r,d), \text{ om } 1 \le r \le l.$$

Strategien vidare er å finna gode øvre skrankar for d_r, $k/4+1 \le r \le k$, og deretter evt. visa at skrankane gjeld med likskap. Dette avsnittet gjer greie for metoden som skal nyttast til dette. Metoden er basert på at det for alle vekter, w_i, finns l-dimensjonale underrom, C_l, slik at

$$w(c^*(y)) = w_i$$

for alle kodeorda i underrommet.

Definisjon 4.4.1
Lat $0 \le \mathsf{r} \le l$. Vi definerer r som rangen over $GF(2)$ til ei søyle i generatormatrisa til C^*_r. Dersom ei søyle har rang 0, vil søyla i resten av oppgåva kallast ei 0-søyle.

Talet på 0-søyler i generatormatrisa for C_r vil då vera gitt av

$$\sum_{i=0}^{2^l} (2^{l-\mathsf{r}_i} - 1), \text{ for dei } 2^l+1 \text{ søylene i } C^*_r.$$

Lat $0 \le j \le 2^l$. Vi ser på ei søyle i $\underline{G}^*_r$ svarande til posisjonen b^j. Har søyla rang r, gir ho opphav til $(2^{l-\mathsf{r}} - 1)$ 0-søyler i C_r. Vidare vil $(2^{r-\mathsf{r}} - 1)$ kodeord i C^*_r ha ein 0-komponent i denne søyla.Dei tilsvarande posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ i $\underline{G}_r$ utgjer generatormatrisa til eit r-dimensjonalt underrom i C^S.

Vi skal ta utgangspunkt i C^* sidan denne koden er enklast å handtera.

Lat $0 \le i < 4$ og $1 \le r < k$. Vi ser på intervallet $il+1 \le r \le (i+1)l$, og skal konstruera generatormatrisa til C^*_r ved å velja kodeord, $c^*(y)_r$, slik at

i) $w(c^*(y)_r) = w_{i+1}$
ii) $c^*(y)_r$ har 0-komponentar i dei *same* søylene.

Om ein vel $c^*(y)_r$ slik at $c^*(y)_r \in S^*_l(y)$, jfr. Definisjon 4.3.4, vil desse krava vera tilfredsstillt. Om muleg vel vi dessutan kodeorda slik at

iii) Alle 0-komponentane til $c^*(y)_r$ ligg innafor 0-søylene i C^*_{il}.

Lat generatormatrisa til C^*_{il} vera arrangert som synt ovanfor. Då vil C^*_{il} innehalda kodeord av vekt $\le w_i$. Om $w_i < w_{maks}$, har generatormatrisa for C^*_{il} ei eller fleire 0-søyler, og dei andre søylene har full rang.

Vi vel så $c^*(y)_{il+1}$ slik at dette kodeordet har vekt w_{i+1}. Då aukar rangen frå 0 til 1 i ei eller fleire av 0-søylene i $\underline{G}^*_{il}$. Talet på 0-søyler der rangen aukar, er avhengig av differansen mellom vektene w_i og w_{i+1}. Om differansen mellom desse to vektene er 2^{l-1}, vil kodeordet medføra eit tillegg i støttevekta på 2^{l-1}. For kvart steg vidare i intervallet $il+1 \le r \le (i+1)l$, vil rangen i søyla/søylene auka frå r til $\mathsf{r}+1$.

Å auka rangen frå 0 til l, i den j'te søyla i $\underline{G}^*$, inneber at dei tilsvarande søylene $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ i $\underline{G}$, på kvart steg kan sjåast som ei generatormatrise for eit r-dimenssjonalt underrom i (C^S), jfr Korollar 4.3.5. Dermed vil støttevekta til C_r innan dette intervallet vera gitt av

$$|X(C_{il})| + t(d_{\mathsf{r}}(C^S)), \text{ der } \mathsf{r} = r - il.$$

$|X\ (C_{il}\ )|$ vil vera eit multippel av d_l $(C^S\ )$. Variabelen t avheng av differansen mellom vektene w_i og w_{i+1}.

Uttrykket vil vera ein øvre skranke for d_r,

$$d_r \le |X\ (C_{il}\ )| + t(d_{\mathrm{r}}\ (C^S)) = d_r^{'\max}\ (C).$$

Døme 4.4.2. $s = 7$, $l = 2$ $\mathrm{d} \in GF(2^l)$,
$C^* = [\ 5, 4, 2\ ]$, $C = [\ 15, 8, 4\ ]$.

Jfr. fig. 4.4.1. $\underline{G}^*$ har $2^l + 1 = 5$ søyler svarande til posisjonane b^j, $0 \le j \le 2^2$. C^*_l er generert av $l = 2$ lineært uavhengige kodeord, $c^*(y)_r$,$1 \le r \le l$. Kodeorda har minimumsvekt w_1. Dei er frå $S^*_l(y)$. $\underline{G}^*_l$ har *tre* 0-søyler og *to* søyler der

$$c^*_j\ (y)_r = Tr_l^{2l}\ (y\mathrm{b}^j + \mathrm{b}^{jt2^{-k}}) \neq 0,\ 1 \le r \le l.\ \text{(Jfr. Definisjon 4.3.1)}$$

Sidan $c^*(y)_r \in S^*_l(y)$, vil kodeorda vera ulike desse to posisjonane,og dei to søylene har difor rang l, dvs full rang.

Vi ser så på intervallet $l+1 \le r \le 2l$. Også i dette intervallet skal l lineært uavhengige kodeord veljast slik at $c^*(y)_r \in S^*_l(y)$, men no skal kodeorda ha vekt w_2. I dømet har vi

$$w_2 - w_1 = 2^{l-1}.$$

Sidan kodeorda også kan veljast slik at dei to 0-komponentane ligg innafor 0-søylene i $\underline{G}^*_l$, er det difor tilstrekkeleg å auka rangen frå 0 til l i *ei* søyle. Ved å auka rangen frå 0 til l i *ei* søyle, vil vi oppnå eit $2l$-dimensjonalt underrom med *to* 0-søyler og *tre* søyler med rang l. Alle kodeorda i dette underrommet har vekt $\le w_2$.

I intervallet $2l+1 \le r \le 3l$ går vi fram på same måte, men brukar kodeord med vekt w_3. I intervallet $3l+1 \le r \le 4l$ nyttast kodeord med vekt w_4.

$$\underline{G}^* \quad \overset{0\ \ldots\ 2^l}{\left\{\begin{array}{ll} 000\mathrm{dd} & \\ 000\mathrm{dd} & l\ \textit{kodeord, tre}\ 0-\textit{søyler, kodeorda i}\ C^*_l\ \textit{har vekt}\ w_1. \\ 00\mathrm{ddd} & \\ 00\mathrm{ddd} & 2l\ \textit{kodeord, to}\ 0-\textit{søyler, kodeorda i}\ C^*_{2l}\ \textit{har vekt}\ w_1\ \textit{og}\ w_2. \\ 0\mathrm{dddd} & \\ 0\mathrm{dddd} & 3l\ \textit{kodeord, ei}\ 0-\textit{søyle, kodeorda i}\ C^*_{3l}\ \textit{har vekt}\ w_1,\ w_2\ \textit{og}\ w_3. \\ \mathrm{ddddd} & \\ \mathrm{ddddd} & 4l\ \textit{kodeord, ingen}\ 0-\textit{søyle, kodeorda i}\ C^*_{4l}\ \textit{har vekt}\ w_1,\ w_2, w_3\ \textit{og}\ w_4. \end{array}\right.}$$

Fig. 4.4.1. Generatormatrisa for C^* er arrangert slik at dei r første kodeorda genererer eit underrom som gir ein øvre skranke for d_r .

Vi ser så på $\underline{G}$, generatormatrisa til "trace-koden" C, jfr. fig. 4.4.2. Kodeorda, $c(y)_r$, $1 \leq r \leq k$, er delt opp i $2^l + 1 = 5$ "blokker" av lengde $2^l - 1 = 3$. Ein slik blokk tilsvarer ein komponent i $c^*(y)_r$.

Lat $0 \leq j \leq 2^l$ og lat $\alpha \in GF(2^l)$. Kvar av posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ i den j'te "blokken" i $c(y)_r$ er då gitt av

$$c_i(y) = Tr_1^l(\alpha^i\, Tr_l^{2l}(y\beta^j + \beta^{jt2^{-k}})),\ 0 \leq i \leq 2^l - 2,\ j \text{ er konstant.}$$

Posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$ har vekt 0 eller 2^{l-1}.

Fig 4.4.2. syner korleis ei søyle i $\underline{G}^*_r$ med rang r, gir opphav til ei generatormatrise for eit r-dimensjonalt underrom i C^S i posisjonane $(c_{j(2^l-1)},\ldots,c_{(2^l-2)+j(2^l-1)})$.

Vi ser også her på intervallet $l+1 \leq r \leq 2l$. Sidan alle kodeorda i C_l har minimumsvekt, vil støttevekta til C_l vera gitt av

$$|X(C_l)| = 2(d_l(C^S)).$$

Ettersom kodeordet $c^*(y)_{l+1}$ vart valt slik at dei 2 0-komponentane i kodeordet låg innafor 0-søylene i $\underline{G}^*_l$, vil det tilsvarande kodeordet, $c(y)_{l+1}$, medføra eit tillegg i støttevekta tilsvarande $w_2 - w_1 = 2^{l-1}$. Støttevekta for heile intervallet vil vera gitt av

$$|X(C_l)| + d_r(C^S), \text{ der } r = r - l.$$

$\underline{G}$

0	.	.	.	2^l
000	000	000	110	110
000	000	000	011	011
000	000	110	110	110
000	000	011	011	011
000	110	110	110	110
000	011	011	011	011
110	110	110	110	110
011	011	011	011	011

Fig. 4.4.2. Generatormatrisa for C er arrangert slik at dei r første kodeorda genererer eit underrom som gir ein øvre skranke for d_r.

For underrom "konstruert" på denne måten gjeld

$$C_1 \subseteq C_2 \subseteq \ldots \subseteq C_r.$$

Sjølv om vi på kvart steg kan visa at val av $c^*(y)_r$ er optimalt med omsyn til støttevekta, vil metoden berre gje ein øvre *skranke* for d_r sidan vi føreset at C^*_r tilfredsstiller kjedevilkåret.

Det er dessutan ikkje gitt at ein oppnår den beste skranken om $w(c^*(y)_{il+1}) = w_{i+1}$. For koden der $s = (2^l-1)(2^{2l}+1) + 2$, skal vi t.d. syna at skranken i eit intervall vert betre om $w(c^*(y)_{il+1}) = w_{i+2}$. Metoden avdekkar dessutan at denne koden ikkje tilfredsstiller kjedevilkåret.

Målet er sjølvsagt å finna vekthierarkiet med utgangspunkt i dei øvre skrankane. Vi må i så fall først og fremst prova $d_{k/4+1}$. Dette har vore den største vansken i arbeidet med oppgåva. Problemet ser ut til å vera det same for beggje kodane. Det har ikkje lukkast å fullføra dette beviset. Delresultat vert lagt fram i avsnitta 4.5.2 og 4.6.2. Vedlegga II og III inneheld meir detaljerte studiar av problemet.

Numeriske resultat for beggje kodane tilseier at dei øvre skrankane gjeld med likskap.

Frå no av skal kodane handsamast kvar for seg i avsnitta 4.5 og 4.6. Vi utviklar først likning (4.2.1) for å muleggjera ein teoretisk analyse. Deretter vert dei matematiske problema kring $d_{k/4+1}$ klargjort og nokre delresultat vert lagt fram. Deretter finn vi dei øvre skrankane for d_r.

4.5 $s = 2^{l+1}-1$

4.5.1 Introduksjon

Dette avsnittet gir ein bakgrunn for koden. Teorem 4.5.1 er henta frå [11]. Vi tek med eit samandrag av beviset, ettersom resultata herifrå skal nyttast vidare.

Teorem 4.5.1. Dersom $m \equiv 0 \bmod 4$, $m = 2l$, og $s = 2^{l+1}-1$, har $D_s(y)$ 4 verdiar. D_s og $h(D_s)$ er gitt av

D_s	$h(D_s)$
2^{l+1}	$(2^{2l-1} - 2^{l-1})/3$
2^l	2^l
0	$2^{2l-1} - 2^{l-1}$
-2^l	$(2^{2l} - 2^l)/3$

Bevis. Sidan $s \equiv 1 \bmod (2^l-1)$ og $s \equiv -3 \bmod (2^l+1)$, får likning (4.2.1) verdiane $k = 0$ og $t = -3$. Likninga vert då

$$y\beta + \beta^{-3} + y^{2^l}\beta^{-1} + \beta^3 = 0.$$

Vi multipliserer med β^3 og tek deretter rota

$$((y\beta + \beta^{-3} + y^{2^l}\beta^{-1} + \beta^3)\beta^3)^{2^{-1}} = 0$$

$$\Rightarrow \beta^3 + y^{1/2}\beta^2 + y^{2^{l-1}}\beta + 1 = 0. \qquad (4.5.1)$$

4.5 $s = 2^{l+1}-1$

4.5.1 Introduksjon

Dette avsnittet gir ein bakgrunn for koden. Teorem 4.5.1 er henta frå [11]. Vi tek med eit samandrag av beviset, ettersom resultata herifrå skal nyttast vidare.

Teorem 4.5.1. Dersom $m \equiv 0 \bmod 4$, $m = 2l$, og $s = 2^{l+1}-1$, har $D_s(y)$ 4 verdiar. D_s og $h(D_s)$ er gitt av

D_s	$h(D_s)$
2^{l+1}	$(2^{2l-1} - 2^{l-1})/3$
2^l	2^l
0	$2^{2l-1} - 2^{l-1}$
-2^l	$(2^{2l} - 2^l)/3$

Bevis. Sidan $s \equiv 1 \bmod (2^l-1)$ og $s \equiv -3 \bmod (2^l+1)$, får likning (4.2.1) verdiane $k = 0$ og $t = -3$. Likninga vert då

$$y\beta + \beta^{-3} + y^{2^l}\beta^{-1} + \beta^3 = 0.$$

Vi multipliserer med β^3 og tek deretter rota

$$((y\beta + \beta^{-3} + y^{2^l}\beta^{-1} + \beta^3)\beta^3)^{2^{-1}} = 0$$

$$\Rightarrow \beta^3 + y^{1/2}\beta^2 + y^{2^{l-1}}\beta + 1 = 0. \qquad (4.5.1)$$

For β gjeld framleis at

$$\beta^{2^l+1} = 1. \tag{4.5.2}$$

Likning(4.2.1) er no ei tredjegradslikning, og $N_\beta(y)$ vert talet på distinkte løysingar, β, til likningane (4.5.1) og (4.5.2).

Vi ser på tilfellet $y^{2^l+1}=1$ og faktoriserer likning (4.5.1)

$$\beta^3 + y^{1/2}\beta^2 + y^{2^{l-1}}\beta + 1 = (\beta + y^{1/2})(\beta + y^{2^{l-2}})^2.$$

Følgjande vert bevist:

i) (4.5.1) har 1 repetert rot med multiplisitet $3 \Leftrightarrow y = 1$,
dvs. når $y^{1/2} = y^{2^{l-2}} \Rightarrow y = y^{2^{l-1}} \Rightarrow y \in GF(2^{2^l}) \cap GF(2^{2^{l-1}}) = GF(2)$.

ii) (4.5.1) har 1 repetert rot med multiplisitet $2 \Leftrightarrow y^{2^l+1} = 1$, $y \neq 1$.
Denne rota er

$$\beta_1 = y^{2^{l-2}}. \tag{4.5.3}$$

Her vil også vera ei anna rot

$$\beta_2 = y^{1/2}. \tag{4.5.4}$$

Det vert synt at røtene tilfredsstiller likning (4.5.2).

Det vert konkludert med at

i) $N_\beta(y) = 2 \Leftrightarrow y^{2^l+1}=1$, $y \neq 1$,
ii) $N_\beta(y) = 1$, om $y = 1$,
iii) $N_\beta(y) = 3$, 1 eller 0, om $y^{2^l+1} \neq 1$.

N_i er gitt ved

$N_1 = (2^{2l-1} - 2^{l-1})/3$
$N_2 = 2^l$
$N_3 = 2^{2l-1} - 2^{l-1}$
$N_4 = (2^{2l} - 2^l)/3$.

4.5.2 Teoretisk analyse av koden

I dette avsnittet skal vi studera likningane (4.5.1) og (4.5.2). Formålet med dette er å analysera vilkåra for kodeord med vekt w_2 og w_3. Målet er i første rekkje å prova $d_{k/4+1}$. Vi treng dessutan meir kunnskap om desse kodeorda for å prova øvre skrankar for d_r, $l+1 \le r \le k$.

Dersom likningane (4.5.1) og (4.5.2) for gitt y har 3 distinkte røter, vil dette medføra at kodeordet har minimumsvekt. Minimumsvekta kan enkelt reknast ut, jfr. avsnitt 4.2. Sidan koden er lineær, vil minimumsvekta svara til minimumsavstanden, og

$$d_1 = 2^{2l-1} - 2^{l-1}(3-1) = 2^{2l-1} - 2^l$$
$$= (2^l - 2)\, 2^{l-1} = (2^l - 2)\, d_1(C^S).$$

Definisjon 4.5.2. Vi definerer koden

$$C = [2^{2l}-1,\ 4l,\ 2^{2l-1} - 2^l\,].$$

Lat $a,b \in GF(2^{2l})$. Då er $c(a,b) = (c_0(a,b),\ c_1(a,b) \ldots\ c_{n-1}(a,b))$ eit kodeord i koden. Posisjonane er gitt av

$$c_j(a,b) = Tr_1^{2l}\ (ax^j + bx^{sj}),\ 0 \le j \le 2^{2l} - 2,$$

der x er eit primitivt element i $GF(2^{2l})$.

Lat $b^{2^l+1} = 1$, (4.5.5)

og $a^{2^l-1} = 1$. Då får vi når $x = ab$

$$Tr_1^{2l}\ (ax + bx^s)$$
$$= Tr_1^{2l}\ (aab + ba^s b^s)$$
$$= Tr_1^{2l}\ (aab + bab^{-3}),\ \textit{då}\ a^s = a\ \textit{og}\ b^s = b^{-3}$$
$$= Tr_1^{l}\ (a\ Tr_l^{2l}\ (ab + bb^{-3})).$$

$$Tr_l^{2l}\ (ab + bb^{-3})$$
$$= ab + bb^{-3} + a^{2^l} b^{-1} + b^{2^l} b^{-3\cdot 2^l}$$
$$= ab + bb^{-3} + a^{2^l} b^{-1} + b^{2^l} b^{3}.$$

Vi multipliserer med b^3 og tek deretter rota

$$= ((ab + bb^{-3} + a^{2^l} b^{-1} + b^{2^l} b^3)\ b^3)^{2^{-1}}$$
$$= a^{1/2} b^2 + b^{1/2} + a^{2^{l-1}} b + b^{2^{l-1}} b^3$$
$$= b^{2^{l-1}} b^3 + a^{1/2} b^2 + a^{2^{l-1}} b + b^{1/2}.$$

Dette gir likninga

$$b^{2^l} b^3 + ab^2 + a^{2^l} b + b = 0,\ b \neq 0.$$ (4.5.6)

Teorem 4.5.3. Vekthierarkiet til C er gitt av
$d_r = (2^l - 2)(2^l - 2^{l-r})$, om $1 \le r \le l$.

Bevis. Vi har frå Teorem 4.3.2 at

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 = (2^l - 2) \sum_{i=0}^{r-1} \left\lceil \frac{2^{l-1}}{2^i} \right\rceil = (2^l - 2)(2^l - 2^{l-r}).$$

Merk. $d_r = (2^l - 2)\, d_r(C^S)$.
$d_l = (2^l - 2)(2^l - 1) = 2^{2l} - 2^{l+1} - 2^l + 2$.

Lat $\delta \in GF(2^l)$. For kodeordet $c(\delta a, \delta b)$ kan likning (4.5.6) skrivast:

$$(\delta b)^{2^l} \beta^3 + \delta a \beta^2 + (\delta a)^{2^l} \beta + \delta b = 0,\ b \neq 0,$$
$$\Rightarrow \delta^{2^l} b^{2^l} \beta^3 + \delta a \beta^2 + \delta^{2^l} a^{2^l} \beta + \delta b = 0$$

Sidan $\delta \in GF(2^l)$, gjeld

$$\delta^{2^l} = \delta,$$

og likninga vert

$$\delta (b^{2^l} \beta^3 + a\beta^2 + a^{2^l} \beta + b) = 0,\ b \neq 0.$$

Likningane (4.5.5) og (4.5.6) for kodeorda $c(a, b)$ og $c(\delta a, \delta b)$ vil då ha identiske røter (evt. ingen røter) og

$$w(c(a, b)) = w(c(\delta a, \delta b)).$$

Jfr. Definisjon 4.3.4. $S_l(a,b) = \{c(\delta a, \delta b) \mid \delta \in GF(2^l)\}$.

For alle kodeord i $S_l(a,b)$ gjeld

$$c(\delta_1 a, \delta_1 b) + c(\delta_2 a, \delta_2 b) = c((\delta_1 + \delta_2) a, (\delta_1 + \delta_2) b).$$

Teorem 4.5.1 føreset $a = y$ og $b = 1$. Lat $a,b \in GF(2^{2l})$ slik at $y = a/\sqrt[s]{b}$. Vi skal no bruka same framgangsmåten som i beviset for Teorem 4.5.1, og finna nokre grunnleggjande vilkår for at likningane (4.5.5) og (4.5.6) har *ei* eller *to* løysingar.

Lemma 4.5.4. Lat $N_\beta(a,b)$ vera talet på distinkte løysingar, β, til likningane (4.5.5) og (4.5.6), $a,b \in GF(2^{2l})$ og $y = a/\sqrt[s]{b}$. Då vil

$N_\beta(a,b) = 1$, om $y = 1$
$N_\beta(a,b) = 2$, om $y^{2^l+1} = 1$, $y \neq 1$.

Bevis. Vi ser på tilfellet $y^{2^l+1}=1$ og får då

$$(a/\sqrt[s]{b})^{2^l+1} = 1$$
$$\Leftrightarrow (a/\sqrt[s]{b})^{s(2^l+1)} = 1$$
$$\Leftrightarrow a^{s(2^l+1)} / b^{2^l+1} = 1$$
$$\Leftrightarrow a^{(2^{l+1}-1)(2^l+1)} / b^{2^l+1} = 1$$
$$\Leftrightarrow (a/b)^{2^l+1} = 1.$$

Vi faktoriserer så likning (4.5.6)

$$b^{2^l} x^3 + ax^2 + a^{2^l} x + b = (b^{2^l} x + a)(x + a^{2^l-1} / b^{2^l-1})^2,$$

sidan

$$(b^{2^l} x + a)(x + a^{2^l-1} / b^{2^l-1})^2$$
$$= (b^{2^l} x + a)(x^2 + a^{2^l} / b^{2^l})$$
$$= b^{2^l} x^3 + ax^2 + a^{2^l} x + a^{2^l+1} / b^{2^l}$$
$$= b^{2^l} x^3 + ax^2 + a^{2^l} x + b, \text{ då } (a/b)^{2^l+1} = 1 \Rightarrow a^{2^l+1} / b^{2^l} = b.$$

Vi ser ut frå dette at likningane (4.5.5) og (4.5.6) vil ha ei rot med multiplisitet 2. Denne rota er

$$x_1 = a^{2^{l-1}} / b^{2^{l-1}}.$$

Her vil også vera ei anna rot

$$b^{2^l} x_2 + a = 0$$
$$\Rightarrow x_2 = a/b^{2^l}.$$

Dersom $x_1 = x_2$, følgjer

$$a/b^{2^l} = a^{2^{l-1}} / b^{2^{l-1}}$$
$$\Leftrightarrow a / a^{2^{l-1}} = b^{2^{l-1}} / b^{2^l}$$
$$\Leftrightarrow a^{-(2^{l-1}-1)} = b^{2^{l-1}}$$
$$\Leftrightarrow a^{2^{2l}-2^{l-1}} = b^{2^{l-1}}$$
$$\Leftrightarrow a = \sqrt[2^{2l}-2^{l-1}]{b^{2^{l-1}}}$$
$$\Leftrightarrow a = \sqrt[2^{l+1}-1]{b}$$
$$\Leftrightarrow a = \sqrt[s]{b}.$$

$$a = \sqrt[s]{b} \Leftrightarrow a/\sqrt[s]{b} = 1 \Leftrightarrow y = 1.$$

Likningane (4.5.5) og (4.5.6) vil difor ha ei rot med multiplisitet 3 om $y = 1$, og vi kan konkludera med at

i) $N_x(y) = 2$, om $y^{2^l+1} = 1$, $y \neq 1$. Tilsvarande kodeord har vekt = w_2.
ii) $N_x(y) = 1$, om $y = 1$. Tilsvarande kodeord har vekt = w_3.

Alle numeriske resultat tilseier at $d_{l+1} > g(l+1, d)$, og at den minste støttevekta vi finn for eit $(l+1)$-dimensjonalt underrom er $g(l+1, d) +1$. Denne støttevekta vert oppnådd når C^*_{l+1} inneheld *eitt* kodeord med vekt w_3 *eller to* kodeord med vekt w_2, og resten av kodeorda har minimumsvekt. Denne situasjonen kan forekoma når generatormatrisa til C^*_{l+1} har *ei* eller *to* 0-søyler. Dei numeriske resultata tyder på at dersom generatormatrisa til C^*_{l+1} *ikkje* har 0-søyler, vil støttevekta til C_{l+1} alltid vera større enn $g(l+1, d) +1$.

For å prova d_{l+1} må vi ut frå dette finna eit C^*_{l+1} slik at

$$|X(C^*_{l+1})| = g(l+1, d).$$

Eller vi må prova allment at eit kodeord med vekt > minimumsvekt finns i eitkvart $(l+1)$-dimensjonalt underrom, dvs at $d_{l+1} > g(l+1, d)$.

Det er difor naudsynt å studera særleg kodeorda med vekt w_2 og w_3 meir detaljert.

Utgangspunktet er likningane (4.5.5) og (4.5.6)

$$b^{2^l+1} = 1.$$

og

$$b^{2^l} b^3 + ab^2 + a^{2^l} b + b = 0,\ b \neq 0.$$

Lemma 4.5.5. Lat $c(a,b)$ vera eit kodeord i C.
Dersom $b^{2^l} b^3 = ab^2$, $b^{2^l} b^3 \neq a^{2^l} b$, vil likningane gje eit kodeord med vekt w_2.
Dersom $b^{2^l} b^3 = a^{2^l} b$, $b^{2^l} b^3 \neq ab^2$, vil likningane gje eit kodeord med vekt w_2.
Dersom $b^{2^l} b^3 = ab^2 = a^{2^l} b$, vil likningane gje eit kodeord med vekt w_3.

Bevis. $b^{2^l} b^3 = ab^2$

$$\Rightarrow b = a/b^{2^l},$$

og likningane har *to* løysingar, jfr. beviset for Lemma 4.5.4.

$$b^{2^l} b^3 = a^{2^l} b,$$
$$\Rightarrow b^2 = a^{2^l}/b^{2^l}$$
$$\Rightarrow b = a^{2^{l-1}}/b^{2^{l-1}},$$

og likningane har *to* løysingar, jfr. beviset for Lemma 4.5.4.

$$b^{2^l} b^3 = ab^2 = a^{2^l} b$$
$$\Rightarrow b = a/b^{2^l} = a^{2^{l-1}} / b^{2^{l-1}}$$
$$\Rightarrow a/b^{2^l} = a^{2^{l-1}} / b^{2^{l-1}}$$
$$\Rightarrow a = \sqrt[5]{b},$$

og likningane har *ei* løysing, jfr. beviset for Lemma 4.5.4.

Korollar 4.5.6. Likning (4.5.6) kan skrivast

$$Tr_l^{2l}(a^2\beta + b^2\beta^{-3}) = 0.$$

β er ei rot i likninga

$$\Leftrightarrow Tr_l^{2l}(a^2\beta + b^2\beta^{-3}) = 0$$
$$\Leftrightarrow (a^2\beta + b^2\beta^{-3}) \in GF(2^l).$$

Dersom $(a^2\beta + b^2\beta^{-3}) = 0$, får vi

$$a^2\beta = b^2\beta^{-3}$$
$$\Rightarrow \beta^4 = b^2/a^2$$
$$\Rightarrow \beta^2 = b/a$$
$$\Rightarrow a/b = 1/\beta^2$$
$$\Rightarrow \beta^2 = a^{2^l}/b^{2^l}$$
$$\Rightarrow \beta = a^{2^{l-1}}/b^{2^{l-1}}.$$

Her vert då

$$(a^{2^{l-1}}/b^{2^{l-1}})^{2^l+1} = 1$$
$$\Rightarrow (a/b)^{2^l+1} = 1.$$

Likning (4.5.6) kan også skrivast

$$Tr_l^{2l}(a^2\beta + b^{2\cdot 2^l}\beta^3) = 0.$$

β er ei rot i likninga

$$\Leftrightarrow Tr_l^{2l}(a^2\beta + b^{2\cdot 2^l}\beta^3) = 0$$
$$\Leftrightarrow (a^2\beta + b^{2\cdot 2^l}\beta^3) \in GF(2^l).$$

Dersom $(a^2\beta + b^{2\cdot 2^l}\beta^3) = 0$, får vi

$$a^2\beta = b^{2\cdot 2^l}\beta^3$$
$$\Rightarrow \beta^2 = a^2/b^{2\cdot 2^l}$$
$$\Rightarrow \beta = a/b^{2^l}.$$

Her vert då

$$(a/b^{2^l})^{2^l+1} = 1$$
$$\Rightarrow (a/b)^{2^l+1} = 1.$$

Når $(a/b)^{2^l+1} = 1$, vil likningane (4.5.5) og (4.5.6) ifølgje beviset for Lemma 4.5.4 ha *to* løysingar dersom $a^{2^{l-1}}/b^{2^{l-1}} \neq a/b^{2^l}$, dvs dersom $\beta_1 \neq \beta_2$.

Dersom $a^{2^{l-1}}/b^{2^{l-1}} = a/b^{2^l}$, har likningane *ei* løysing.

Numeriske resultat tyder på at det i eitkvart (l+1)-dimensjonalt underrom i koden finns minst eitt kodeord, $c(a,b)$, slik at $(a/b^{2^l})^{2^l+1} = 1$. I Vedlegg II er tilfellet $\beta = a/b^{2^l}$ studert frå eit par andre synsvinklar.

I Lemma 4.5.4. fann vi at likningane (4.5.5) og (4.5.6) har
to løysingar om

$$(a/\sqrt[s]{b})^{2^l+1} = 1,\ a/\sqrt[s]{b} \neq 1,$$

og *ei* løysing om

$$a/\sqrt[s]{b} = 1.$$

I Lemma 4.5.7. kjem vi fram til eit meir presist utrykk.

Lemma 4.5.7. Lat β vera ei løysing til likningane (4.5.5) og (4.5.6) for eit kodeord, $c(a,b)$. Då har likningane *to* løysingar $\Leftrightarrow a/b = 1/\beta^2,\ \beta^3 \neq b^{1-2^l}$.

Bevis. Vi skriv likning (4.5.6) som

$$b^{2^l}x^3 + ax^2 + a^{2^l}x + b = 0,$$

og faktoriserer

$$\begin{aligned} & b^{2^l}x^3 + ax^2 + a^{2^l}x + b \\ &= b^{2^l}(x+\beta)^2(x+u) \\ &= b^{2^l}x^3 + b^{2^l}ux^2 + b^{2^l}\beta^2 x + b^{2^l}\beta^2 u. \end{aligned}$$

Vi ser på koeffisientane til x^2 og x og får

$$\begin{aligned} & (b^{2^l}u)^{2^l} = b^{2^l}\beta^2 \\ & \Rightarrow bu^{2^l} = b^{2^l}\beta^2 \\ & \Rightarrow u^{2^l} = b^{2^l-1}\beta^2. \end{aligned}$$

Vi ser på siste leddet i likninga og får

$$\begin{aligned} & b^{2^l}\beta^2 u = b \\ & \Rightarrow u = b^{1-2^l}/\beta^2. \end{aligned}$$

Vi set inn for u og får

$$\begin{aligned} & b^{2^l}(x+\beta)^2(x+u) = 0 \\ & \Rightarrow b^{2^l}(x+\beta)^2(x+b^{1-2^l}/\beta^2) = 0 \end{aligned}$$

Vi ser at likninga har 2 røter ; β med multiplisitet 2 og b^{1-2^l}/β^2. Dei to røtene er samanfallande om $\beta = b^{1-2^l}/\beta^2 \Rightarrow \beta^3 = b^{1-2^l}$.

Følgjande vil gjelda

$$b^{2^l}u = a \Rightarrow b^{2^l}\ b^{1-2^l}/\beta^2 = a \Rightarrow a = b/\beta^2 \Rightarrow a/b = 1/\beta^2.$$

Vi har no synt at dersom likningane har *to* røter, gjeld $a/b = 1/\beta^2$. Vi har i Korollar 4.5.6 synt at dersom $a/b = 1/\beta^2$,vil likningane ha *to* røter om røtene ikkje er samanfallande. Difor følgjer teoremet.

Lemma 4.5.8. Dersom C^*_{l+1} har 0-søyler, inneheld C^*_{l+1} minst *eitt* kodeord med vekt > w_1.

Bevis. Sidan likning (4.5.6) kan skrivast

$$Tr_l^{2l}(a^2\beta + b^2\beta^{-3}) = 0,$$

kan vi setja

$$f_{ab}(\beta) = Tr_l^{2l}(a^2\beta + b^2\beta^{-3}) = 0$$

og

$$c^*(a,b) = (f_{ab}(1), f_{ab}(\beta)....f_{ab}(\beta^{2^l})),$$ jfr. Definisjon 4.3.1.

Lat $0 \le j \le 2^l$. Vi ser på ei søyle svarande til β^j i generatormatrisa for C^*_{l+1}. Den j'te posisjonen vil for kvart kodeord i C^*_{l+1} vera gitt av

$$c^*_j(a,b) = Tr_l^{2l}(a^2\beta^j + b^2\beta^{-3j}),$$ der $a^2\beta^j + b^2\beta^{-3j} \in GF(2^{2l})$.

l+1 element i $GF(2^{2l})$ vil ha ein lineærkombinasjon i $GF(2^l)$.

Lat den j'te søyla i generatormatrisa for C^*_{l+1} vera ei 0-søyle. Då gjeld

$$c^*_j(a,b) = Tr_l^{2l}(a^2\beta^j + b^2\beta^{-3j}) = 0$$ for alle kodeord i C^*_{l+1}.

Sidan $Tr_l^{2l}(a^2\beta^j + b^2\beta^{-3j}) = 0 \Leftrightarrow a^2\beta^j + b^2\beta^{-3j} \in GF(2^l)$, vil vi no få lineærkombinasjonar av l+1 element i $GF(2^l)$.

Søyla kan illustrerast slik

$$\begin{aligned}
Tr_l^{2l}(a_1^2\beta^j + b_1^2\beta^{-3j}) &= 0\\
Tr_l^{2l}(a_2^2\beta^j + b_2^2\beta^{-3j}) &= 0\\
&\dots\\
&\dots\\
Tr_l^{2l}(a_{l+1}^2\beta^j + b_{l+1}^2\beta^{-3j}) &= 0
\end{aligned}$$

Dei l+1 elementa kan ikkje vera lineært uavhengige. Det vil i denne søyla i C^*_{l+1} forekoma minst eitt tilfelle av at

$$a^2\beta^j + b^2\beta^{-3j} = 0.$$

Sidan likning (4.5.6) og dermed $f_{ab}(\beta)$ også kan skrivast

$$f_{ab}(\beta) = Tr_l^{2l}(a^2\beta + b^{2\cdot 2^l}\beta^3),$$

vil det i den j'te søyla i C^*_{l+1} no tilsvarande vera minst eitt tilfelle av at

$$a^2\beta^j + b^{2\cdot 2^l}\beta^{3j} = 0.$$

I Korollar 4.5.6 synte vi at dersom

$$a^2\beta + b^2\beta^{-3} = 0, \text{ dvs } \beta = a^{2^{l-1}}/b^{2^{l-1}},$$

eller dersom

$$a^2\beta + b^{2\bullet 2^l}\beta^{3} = 0, \text{ dvs } \beta = a / b^{2^l},$$

vil likningane (4.5.5) og (4.5.6) medføra eit kodeord med vekt w_2 om røtene ikkje er samanfallande. Om røtene er samanfallande, gjeld

$$a^{2^{l-1}}/b^{2^{l-1}} = a / b^{2^l},$$

og kodeordet har vekt w_3.

Vi har no synt at om C^*_{l+1} har ei 0-søyle, må C^*_{l+1} innehalda minst eitt kodeord,

$c^*(a,b)_1$, slik at $\beta = a^{2^{l-1}}/b^{2^{l-1}}$

og minst eitt kodeord,

$c^*(a,b)_2$, slik at $\beta = a / b^{2^l}$.

Om $c^*(a,b)_1 = c^*(a,b)_2$, vil likningane for kodeordet ha *ei* løysing. Kodeordet har då vekt w_3. Dette medfører at C^*_{l+1} må innehalda minst *eitt* kodeord med vekt > w_1. Om $c^*(a,b)_1 \neq c^*(a,b)_2$, må C^*_{l+1} må innehalda minst *to* kodeord med vekt > w_1. Likningane har då *to* løysingar. Kodeorda har vekt w_2.

I dette avsnittet er det lagt fram nokre vilkår for at likningane (4.5.5) og (4.5.6) medfører kodeord med vekt w_2 og w_3. Vi har funne at dersom generatormatrisa for C^*_{l+1} har 0-søyler, vil C^*_{l+1} innehalda minst eitt kodeord med vekt > w_1. Derimot har vi ikkje greidd å prova at C^*_{l+1} *alltid* inneheld kodeord med vekt > w_1, slik alle numeriske resultat tilseier. Vi har dermed ikkje prova d_{l+1}. Det som er lagt fram i dette avsnittet (og også i Vedlegg II), kan vera viktige delresultat for eit slikt prov.

Alle vidare resultat vedrørande d_r, $l+1 \leq r \leq k$, vert dermed ståande som øvre skrankar.

4.5.3 Øvre skrankar for vekthierarkiet, d_{l+1} ... d_k.

Vi skal følgja metoden som vart skissert i avsnitt 4.4. Lat $0 \leq i < 4$ og $1 \leq r < k$. Vi skal konstruera generatormatrisa til C^*_r. I kvart intervall, $il+1 \leq r \leq (i+1)l$, skal vi velja kodeord, $c^*(a,b)_r$, etter følgjande retningslinjer.

i) $w(c^*(a,b)_r) = w_{i+1}$

ii) $c^*(a,b)_r$ har 0-komponentar i dei *same* søylene.

Om ein vel $c^*(a,b)_r$ slik at $c^*(a,b)_r \in S^*_l(a,b)$, vil desse krava vera tilfredsstillt. Om muleg skal vi dessutan velja kodeorda slik at

iii) Alle 0-komponentane til $c^*(a,b)_r$ ligg innafor 0-søylene i C^*_{il}.

Før vi finn skrankane, må vi undersøkja

i) differansen mellom vektene w_{i+1} og w_i, då denne gir differansen mellom $|X(C^*_{il+1})|$ og $|X(C^*_{il})|$.

ii) om det er muleg å velja $c^*(a,b)_{il+1}$ slik at alle 0-komponentane til $c^*(a,b)_{il+1}$ ligg innafor 0-søylene i C^*_{il}.

Vi reknar først ut vektene. Sidan $\mathsf{D}_s(y)$ har 4 verdiar, er C ein 4-vektskode. Vektene er gitt ved

$$\begin{aligned}
w_1 = d_1 &= 2^{2l-1} - 2^{l-1}(3-1) = 2^{2l-1} - 2^l = (2^l - 2)\,2^{l-1} = (2^l-2)d_1(C^S)\\
w_2 &= 2^{2l-1} - 2^{l-1}(2-1) = 2^{2l-1} - 2^{l-1} = (2^l - 1)\,2^{l-1} = (2^l-1)d_1(C^S)\\
w_3 &= 2^{2l-1} - 2^{l-1}(1-1) = 2^{2l-1} = (2^l)\,2^{l-1} = 2^l\, d_1(C^S)\\
w_4 &= 2^{2l-1} - 2^{l-1}(0-1) = 2^{2l-1} + 2^{l-1} = (2^l+1)\,2^{l-1} = (2^l+1)d_1(C^S).
\end{aligned}$$

Vi ser at vektene er påfølgjande multippel av $d_1(C^S)$, og differansen mellom vektene w_{i+1} og w_i er 2^{l-1}.

Merk. C^* er ein MDS-kode.

Punkt iii) kan tilfredsstillast på følgjande måte. Vi går ut frå at vi i intervallet $1 \le r \le l$ har valt kodeord med vekt w_1. Desse har 0-posisjonar tilsvarande b_1, b_2 og b_3. Vi skal så finna $c^*(a,b)_{l+1}$ med vekt w_2. Kodeordet skal om muleg ha 0-posisjonar svarande til b_1 og b_2.

Lat $M = \{\, c^*(a,b) | (a/b)^{2^l+1} = 1\}$. Vi kan ifølgje Lemma 4.5.4 velja $c^*(a,b)_{l+1}$ frå M slik at

$$a^{2^{l-1}}/b^{2^{l-1}} = \mathsf{b}_1$$

og

$$a/b^{2^l} = \mathsf{b}_2,\ a^{2^{l-1}}/b^{2^{l-1}} \neq a/b^{2^l}.$$

Dette vil vera muleg for alle kombinasjonar av to søyler.

$c^*(a,b)_{2l+1}$ med vekt w_3 , og med 0-posisjon svarande til b_1, kan også veljast frå M, men slik at $a^{2^{l-1}}/b^{2^{l-1}} = a/b^{2^l} = \mathsf{b}_1$. Dette vil vera muleg for alle søyler.

Vi kan då konkludera med at det i C finns underrom

i) med dimensjon $\leq l$, slik at likningane for alle kodeorda i C_l har *tre* felles røter, og der alle kodeord har vekt w_1.

ii) med dimensjon $\leq 2l$, slik at likningane for alle kodeorda i C_{2l} har *to* felles røter, og der alle kodeord har vekt w_1 og w_2.

iii) med dimensjon $\leq 3l$, slik at likningane for alle kodeorda i C_{3l} har *ei* felles rot, og der alle kodeord har vekt w_1, w_2 og w_3.

Eit r-dimensjonalt underrom, C_r , i C tilsvarer eit r-dimensjonalt underrom, C_r*, i C*. Dersom likningane for alle kodeorda i C_r har i felles røter, vil generatormatrisa for C_r* ha i 0-søyler.

Vi kan då konstruera følgjande generatormatrise for C^*_r.

Døme 4.5.9. $\mathrm{d} \in GF(2^l),\ l = 4.$

$$
\begin{array}{ll}
 & \quad 1\ \mathrm{b}\ \ldots \qquad\qquad\qquad\qquad \ldots\ \mathrm{b}^{2^l} \\
\underline{G}* & \left\{\begin{array}{l}
0\ 0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ 0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ 0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ 0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \qquad \mathit{tre}\ 0 - \mathit{søyler}, \mathit{kodeorda\ i}\ C*_l\ \mathit{har\ vekt}\ w_1 . \\
0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ 0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \qquad \mathit{to}\ 0 - \mathit{søyler}, \mathit{kodeorda\ i}\ C*_{2l}\ \mathit{har\ vekt}\ w_1\ \mathit{og}\ w_2 . \\
0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
0\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \qquad \mathit{ei}\ 0 - \mathit{søyle}, \mathit{kodeorda\ i}\ C*_{3l}\ \mathit{har\ vekt}\ w_1,\ w_2\ \mathit{og}\ w_3 . \\
d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \\
d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d\ d \qquad \mathit{ingen}\ 0 - \mathit{søyle}, \mathit{kodeorda\ i}\ C*_{4l}\ \mathit{har\ vekt}\ w_1,\ w_2, w_3\ \mathit{og}\ w_4 .
\end{array}\right.
\end{array}
$$

Fig.4.5.1 C = [255, 16, 112] , C* = [17, 4, 14]. Generatormatrisa er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken for d_r .

Teorem 4.5.10. Øvre skrankar for vekthierarkiet til C er gitt ved

$$\begin{aligned} d_r \le \quad & (2^l-2)(2^l-1) + (2^l - 2^{2l-r}), \quad \text{om} \quad l+1 \le r \le 2l, \\ \le \quad & (2^l-1)(2^l-1) + (2^l - 2^{3l-r}), \quad \text{om } 2l+1 \le r \le 3l, \\ \le \quad & 2^l(2^l-1) + (2^l - 2^{4l-r}), \quad \text{om } 3l+1 \le r \le 4l. \end{aligned}$$

Bevis.

***l*+1 ≤ *r* ≤ 2*l*.**

Utgangspunkt er C^*_l der 3 søyler har rang 0, og dei $(2^l+1) - 3 = 2^l - 2$ andre søylene har rang l. Vi har frå Lemma 4.5.8 at

$$c^*_j(a,b) = Tr_l^{2l}(a^2\beta^j + b^2\beta^{-3j}).$$

Sidan $c^*(a,b)_r$,$1 \le r \le l$, er valt frå $S^*_l(a,b)$, er dei ulike i alle posisjonar ≠ 0. I fig. 4.5.1. er dette posisjonane svarande til β^j, $3 \le j \le 2^l$.

Vi vel så $c^*(a,b)_{l+1}$ med vekt w_2. Vi har funne at det er muleg å velja dette slik at 0-komponentane svarar til to av 0-søylene i $\underline{G}^*_l$. Rangen må då auka frå 0 til 1 i *ei* søyle. I fig.4.5.1. er dette søyla svarande til β^2.

I heile intervallet, $l+1 \le r \le 2l$, vel vi $c^*(a,b)_r \in S^*_l(a,b)$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå 0 til l.

I dei tilsvarande kodeorda $c(a,b)_r$ i C, er kvar posisjon gitt av

$Tr_l^{2l}(\alpha \; Tr_l^{2l}(a^2\beta + b^2\beta^{-3}))$. Kodeorda vert generert ved å lata α gå gjennom $GF(2^l)$ og β gå gjennom B.), jfr også avsnitta 4.3 og 4.4.

Lat $0 \le i \le 2^l - 2$ og $0 \le j \le 2^l$. Då vil posisjonane i $c(a,b)_r$ vera gitt av

$$c_{i+j(2^l-1)}(a,b)_r = Tr_l^{2l}(\alpha^i \; Tr_l^{2l}(a^2\beta^j + b^2\beta^{-3j})).$$

Vi ser på *ei* søyle i $\underline{G}^*$. Sidan $c^*(a,b)_r \in S^*_l(a,b)$, vil alle kodeorda vera ulike i posisjon j, og

$$Tr_l^{2l}(a^2\beta^j + b^2\beta^{-3j})$$

vil vera l lineært uavhengige element i $GF(2^l)$. Då vil dei tilsvarande søylene i $\underline{G}$ vera ei generatormatrise for Simplex-koden, C^S. Dei tilsvarande søylene i $\underline{G}$ vil vera søylene $j(2^l-1) \ldots 2^l - 2 + j(2^l-1)$. Fig. 4.5.2 syner eit utdrag frå $\underline{G}$.

Døme 4.5.9, framh. Jfr. søyla tilsvarande b^2 i fig 4.5.1. Fig. 4.5.2 syner dei tilsvarande søylene i $\underline{G}$.

	Søyler tilsvarande b	Søyler tilsvarande b^2	Søyler tilsvarande b^3	.....	
$\underline{G}$	….				
	….				
	….0000000	000000000000000	10101010….		*kodeorda i* C^*_l *har vekt* w_1.
	….0000000	111111110000000	11111111….		
	….0000000	111100001111000	11110000….		
	….0000000	110011001100110	11001100….		
	….0000000	101010101010101	10101010….		*kodeorda i* C^*_{2l} *har vekt* w_1 *og* w_2.

Fig. 4.5.2 C = [255, 16, 112] , C* = [17, 4, 14]. Søylene tilsvarande b^2 utgjer ei generatormatrise for ein [2^l -1, l , 2^{l-1}] Simplex-kode.

Dette inneber at

$$d_r \le d_l + d_r\,(C^S), \text{ der } r = r - l.$$
$$= (2^l\text{-}2)(2^l\text{-}1) + (2^l - 2^{2l-r}) = d_r^{'\max}.$$

Vi samanliknar no dette resultatet med $g(r,d)$ for $l+1 \le r \le 2l$.

$\underline{r = l+1}$.

$$d_{l+1}^{'\max} - g(l+1,d)$$
$$= (2^l\text{-}1)(2^l - 2) + 2^{l-1} - \left\lceil \frac{(2^r - 1)(2^{2l-1} - 2^l)}{2^{r-1}} \right\rceil$$
$$= 2^{2l} - 2^{l+1} - 2^{l-1} + 2 - (2^{2l} - 2^{l+1} - 2^{l-1} + 1) = 1.$$

$\underline{r = 2l}$.

$$d_{2l}^{'\max} - g(2l,d)$$
$$= (2^l\text{-}1)(2^l - 2) + (2^l\text{-}1) - \left\lceil \frac{(2^r - 1)(2^{2l-1} - 2^l)}{2^{r-1}} \right\rceil$$
$$= 2^{2l} - 2^{l+1} + 1 - (2^{2l} - 2^{l+1}) = 1.$$

Ettersom $d_1 < d_2 < d_3 ... < d_k \le n$, kan vi konkludera med at

$$d_r^{'\max} = g(r,d) + 1, \text{ om } l+1 \le r \le 2l.$$

$2l+1 \le r \le 3l$.

Utgangspunkt er C^*_{2l} der 2 søyler har rang 0, og 2^l-1 søyler har rang l.

Vi vel $c^*(a,b)_{2l+1}$ med vekt w_3. Vi har funne at det er muleg å velja dette slik at 0-komponenten svarar til ei av 0-søylene i $\underline{G}^*_{2l}$. Rangen kan også no auka frå 0 til 1 i *ei* søyle. I fig.4.5.1. er dette søyla svarande til b.

I heile intervallet, $2l+1 \le r \le 3l$, vel vi $c^*(a,b)_r$ frå $S^*_l(a,b)$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r , til søyla aukar frå 0 til l.

Den øvre skranken er då gitt av

$$d_r \le d^{'\max}_{2l} + d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 2l.$$
$$= (2^l-1)(2^l-1) + (2^l - 2^{3l-r}) = d^{'\max}_r .$$

$3l+1 \le r \le 4l$.

Utgangspunkt er C^*_{3l} der 1 søyle har rang 0, og 2^l søyler har rang l.
Vi vel $c^*(a,b)_{3l+1}$ med vekt w_4.

I heile intervallet, $3l+1 \le r \le 4l$, vel vi $c^*(a,b)_r$ frå $S^*_l(a,b)$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r , til søyla aukar frå 0 til l.

Den øvre skranken er då gitt av

$$d_r \le d^{'\max}_{3l} + d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 3l.$$
$$= 2^{2l}(2^l-1) + (2^l - 2^{4l-r}) = d^{'\max}_r .$$

4.5.4 Resultat for $l \le 4$

Vi synte i Lemma 4.5.8 at dersom $\underline{G}^*_{l+1}$ har 0-søyler, kan den øvre skranken,

$$d^{'\max}_{l+1} = \mathrm{g}(l+1,d) + 1,$$

ikkje underskridast. Dette tilseier at dersom alle kodeorda i C_{l+1} har minimumsvekt slik at

$$d_{l+1} = \mathrm{g}(l+1,d),$$

kan $\underline{G}^*_{l+1}$ ikkje ha 0-søyler. Vi skal no syna at $\underline{G}^*_{l+1}$ heller ikkje kan ha søyler med rang 1. Vidare at $\underline{G}^*_{l+1}$ kan ha høgst *ei* søyle med rang 2.

Til slutt syner vi at det underrommet som $\underline{G}^*_{l+1}$ i såfall genererer, vil ha ei støttevekt som er større enn $d^{'\max}_{l+1}$, om $l \le 4$.

Vi går ut frå at $d_{l+1} = g(l+1,d)$ og at $\underline{G}^*_{l+1}$ ikkje har 0-søyler. Sidan alle kodeord i C^*_{l+1} då må ha minimumsvekt, må alle kodeord i $C^*_l \subseteq C^*_{l+1}$ også ha minimumsvekt. Kjedevilkåret vil dermed gjelda for C^*_{l+1}.

Lat C^*_{l+1} innehalda eit l-dimensjonalt underrom , C^*_l , slik at $\underline{G}^*_l$ har *ei* søyle med rang 0. Ettersom $\underline{G}^*_{l+1}$ derimot *ikkje* kan ha 0-søyler, må rangen til denne søyla vera auka til 1. Søyla representerer då eit tillegg i støttevekta på 2^{l-1}. Støttevekta til C^*_{l+1} er, dersom ingen fleire søyler bidreg, gitt av

$$d_l + 2^{l-1} = d^{'\max}_{l+1} .$$

Vi kan konkludera med at $\underline{G}^*_{l+1}$ heller ikkje kan ha søyler med rang 1 om den øvre skranken skal underskridast.

Lat C^*_{l+1} innehalda eit l-dimensjonalt underrom , C^*_l , slik at $\underline{G}^*_l$ har *to* søyler med rang 1. Ettersom $\underline{G}^*_{l+1}$ ikkje kan ha søyler med rang 1, må rangen i desse søylene vera auka til 2. Søylene representerer då eit tillegg i støttevekta på $2(2^{l-2})$. Støttevekta til C^*_{l+1} er, dersom ingen fleire søyler bidreg, gitt av

$$d_l + 2(2^{l-2}) = d^{'\max}_{l+1} .$$

Vi kan konkludera med at $\underline{G}^*_{l+1}$ kan ha høgst *ei* søyle med rang 2 om den øvre skranken skal underskridast.

Lemma 4.5.11. Dersom $l \le 4$, er vekthierarkiet til C gitt av

$$d_r = g(r,d) + 1, \text{ om } l+1 \le r \le 2l.$$

Bevis.

***l* = 2.** C = [15, 8, 4] , C* = [5, 4, 2].

Det finns følgjande alternativ for $\underline{G}^*_l$ slik at 2 kodeord har minimumsvekt.

i) <u>3 0-søyler</u>	ii) <u>2 0-søyler</u>	iii) <u>1 0-søyle</u>
$\underline{c}^*(a_1,b_1)$: 000δδ	$\underline{c}^*(a_1,b_1)$: 000δδ	$\underline{c}^*(a_1,b_1)$: 000δδ
$\underline{c}^*(a_2,b_2)$: 000δδ	$\underline{c}^*(a_2,b_2)$: 00δ0δ	$\underline{c}^*(a_2,b_2)$: 0δδ00

Dersom alle kodeord i C^*_l (og C^*_{l+1}) skal ha minimumsvekt, må alternativ i) eller ii) veljast. Dette tyder at C^*_l har minst 2 søyler med rang 0. Dermed vil C^*_{l+1} ha søyler med rang 1, og skranken kan ikkje underskridast.

***l* = 4.** C = [255, 16, 112] , C* = [17, 4, 14].

$$g(l+1,d) = \left\lceil \frac{(2^r - 1)(2^{2l-1} - 2^l)}{2^{r-1}} \right\rceil$$

$$= (31 * 112)/16$$

$$= 217.$$

Frå Teorem 4.5.10 har vi

$$d'^{\max}_{l+1} = (2^l-2)(2^l-1) + (2^l - 2^{2l-r})$$
$$= 14*15 + (16 - 8)$$
$$= 218.$$

Dersom *ei* søyle $\underline{G}^*_{l+1}$ har rang 2, og dei andre har rang 3, vil støttevekta til C^*_{l+1} verta

$$|X(C^*_{l+1})| = d_2(C^S) + 2^l\, d_3(C^S)$$
$$= (2^l - 2^{l-2}) + 2^l(2^l - 2^{l-3})$$
$$= (16 - 4) + 16(16 - 2)$$
$$= 236.$$

Berre fleire søyler med rang 2 kan minka denne summen, men då vil den øvre skranken ikkje underskridast.

Vi kan då konkludera med at den øvre skranken, $d'^{\max}_r$, vil gjelda med likskap for heile intervallet $l+1 \le r \le 2l$, sidan $d'^{\max}_r = g(r,d) +1$, og $d_{r+1} > d_r$ gjeld.

4.6 $s = (2^l-1)(2^{2l}+1) + 2$

4.6.1 Introduksjon

Dette avsnittet gir ein bakgrunn for koden. Teorem 4.6.1 er henta frå [11]. Vi tek med eit samandrag av beviset, ettersom resultata herifrå skal nyttast vidare.

Teorem 4.6.1. Dersom $m = 4l$ og $s = (2^l-1)(2^{2l}+1) + 2$, har $D_s(y)$ 4 verdiar. D_s og $h(D_s)$ er gitt av

D_s	$h(D_s)$
2^{3l}	2^l
2^{2l}	$2^{4l-1} - 2^{3l-1}$
0	$2^{3l} - 2^l$
-2^{2l}	$2^{4l-1} - 2^{3l-1}$

Bevis. Sidan $s \equiv 2 \bmod (2^{2l}+1)$ og $s \equiv 2^{l+1} \bmod (2^{2l}-1)$, får likning (4.2.1) verdiane $k = l+1$ og $t = 2$. Likninga vert då

$$y\beta + y^{2^{2l}}\beta^{-1} + \beta^{2^l} + \beta^{-2^l} = 0. \qquad (4.6.1)$$

Vi ser på tilfellet $y \in GF(2^{2l})$. Likninga kan då skrivast

$$y(\beta + \beta^{-1}) = (\beta + \beta^{-1})^{2^l}. \qquad (4.6.2)$$

4.6 $s = (2^l-1)(2^{2l}+1) + 2$

4.6.1 Introduksjon

Dette avsnittet gir ein bakgrunn for koden. Teorem 4.6.1 er henta frå [11]. Vi tek med eit samandrag av beviset, ettersom resultata herifrå skal nyttast vidare.

Teorem 4.6.1. Dersom $m = 4l$ og $s = (2^l-1)(2^{2l}+1) + 2$, har $D_s(y)$ 4 verdiar. D_s og $h(D_s)$ er gitt av

D_s	$h(D_s)$
2^{3l}	2^l
2^{2l}	$2^{4l-1} - 2^{3l-1}$
0	$2^{3l} - 2^l$
-2^{2l}	$2^{4l-1} - 2^{3l-1}$

Bevis. Sidan $s \equiv 2 \bmod (2^{2l}+1)$ og $s \equiv 2^{l+1} \bmod (2^{2l}-1)$, får likning (4.2.1) verdiane $k = l+1$ og $t = 2$. Likninga vert då

$$y\beta + y^{2^{2l}}\beta^{-1} + \beta^{2^l} + \beta^{-2^l} = 0. \qquad (4.6.1)$$

Vi ser på tilfellet $y \in GF(2^{2l})$. Likninga kan då skrivast

$$y(\beta + \beta^{-1}) = (\beta + \beta^{-1})^{2^l}. \qquad (4.6.2)$$

For β gjeld framleis at

$$\beta^{2^{2l}+1} = 1, \qquad (4.6.3)$$

og vi ser at $\beta = 1$ er ei løysing til likningane (4.6.2) og (4.6.3).

Likning (4.6.1) kan skrivast som

$$y = (\beta + \beta^{-1})^{2^l-1}. \qquad (4.6.4)$$

Følgjande vert bevist:

i) Det finns inga løysing til (4.6.3) og (4.6.4), om $y = 1$ eller om $y^{2^l+1} \neq 1$.

ii) Det finns 2^l distinkte løysingar til (4.6.3) og (4.6.4), om $y^{2^l+1} = 1$, $y \neq 1$.

Det vert konkludert med at
dersom $y \in GF(2^{2l})$,

i) $N_\beta(y) = 2^l + 1$, om $y^{2^l+1} = 1$, $y \neq 1$,

ii) $N_\beta(y) = 1$, om $y = 1$,

og dersom $y \in GF(2^{4l}) - GF(2^{2l})$,

iii) $N_\beta(y) \leq 2$.

N_i er gitt ved

$$N_1 = 2^l$$
$$N_2 = 2^{4l-1} - 2^{3l-1}$$
$$N_3 = 2^{3l} - 2^l$$
$$N_4 = 2^{4l-1} - 2^{3l-1}.$$

4.6.2 Teoretisk analyse av koden

I dette avsnittet skal vi på same vis som i avsnitt 4.5.2 studera likningane (4.6.3) og (4.6.4). Målet er også her i første rekkje å prova $d_{k/4+1}$.

Dersom likningane (4.6.3) og (4.6.4) for gitt y har $2^l + 1$ distinkte røter, vil dette medføra at kodeordet har minimumsvekt. Minimumsvekta kan enkelt reknast ut, jfr. avsnitt 4.2. Sidan koden er lineær, vil minimumsvekta svara til minimumsavstanden, og

$$d_1 = 2^{4l-1} - 2^{2l-1}((2^l+1) - 1) = 2^{4l-1} - 2^{3l-1}$$
$$= (2^{2l} - 2^l)\, 2^{2l-1} = (2^{2l} - 2^l)\, d_1(C^S).$$

Definisjon 4.6.2. Vi definerer koden
$C = [2^{4l}-1, 8l, 2^{4l-1} - 2^{3l-1}]$.

Lat $a,b \in GF(2^{4l})$. Då er $c(a,b) = (c_0(a,b), c_1(a,b) \ldots c_{n-1}(a,b))$ eit kodeord i koden. Posisjonane er gitt av

$$c_j(a,b) = Tr_1^{4l}(ax^j + bx^{sj}),\ 0 \le j \le 2^{4l} - 2,$$

der x er eit primitivt element i $GF(2^{4l})$.

Lat $b^{2^{2l}+1} = 1$, (4.6.5)

og $a^{2^{2l}-1} = 1$. Då får vi når $x = ab$

$$\begin{aligned}
&Tr_1^{4l}(ax + bx^s)\\
&= Tr_1^{4l}(aab + ba^s b^s)\\
&= Tr_1^{4l}(aab + ba^{2^{l+1}} b^2)\\
&= Tr_1^{4l}(aab + (ba^{2^{l+1}} b^2)^{2^{l-1}})\\
&= Tr_1^{4l}(aab + b^{2^{l-1}} a^{2^{2l}} b^{2^l})\\
&= Tr_1^{4l}(aab + b^{2^{l-1}} ab^{2^l})\\
&= Tr_1^{2l}(a\, Tr_{2l}^{4l}(ab + b^{2^{l-1}} b^{2^l})).
\end{aligned}$$

$$\begin{aligned}
&Tr_{2l}^{4l}(ab + b^{2^{l-1}} b^{2^l})\\
&= ab + b^{2^{l-1}} b^{2^l} + a^{2^{2l}} b^{-1} + b^{2^{-l-1}} b^{-2^l}.
\end{aligned}$$

Dette gir likninga

$$b^{2^{l-1}} b^{2^l} + ab + b^{2^{-l-1}} b^{-2^l} + a^{2^{2l}} b^{-1} = 0,\ b \neq 0. \quad (4.6.6)$$

Teorem 4.6.3. Vekthierarkiet til C er gitt av
$d_r = (2^{2l} - 2^l)(2^{2l} - 2^{2l-r})$, om $1 \le r \le 2l$.

Bevis. Vi har frå Teorem 4.3.2 at

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 = (2^{2l} - 2^l) \sum_{i=0}^{r-1} \left\lceil \frac{2^{2l-1}}{2^i} \right\rceil = (2^{2l} - 2^l)(2^{2l} - 2^{2l-r}).$$

Merk. $d_r = (2^{2l} - 2^l)\, d_r(C^S)$.
$d_l = (2^{2l} - 2^l)(2^{2l} - 1) = 2^{4l} - 2^{3l} - 2^{2l} + 2^l$.

Lat $\delta \in GF(2^{2l})$. For kodeordet $c(\delta^{2^{l-1}} a, \delta b)$ kan likning (4.6.6) skrivast:

$$(\delta b)^{2^{l-1}} \beta^{2^l} + (\delta^{2^{l-1}} a)\beta + (\delta b)^{2^{-l-1}} \beta^{-2^l} + (\delta^{2^{l-1}} a)^{2^{2l}} \beta^{-1} = 0, \quad b \neq 0,$$

$$\Rightarrow \delta^{2^{l-1}} b^{2^{l-1}} \beta^{2^l} + \delta^{2^{l-1}} a\beta + \delta^{2^{-l-1}} b^{2^{-l-1}} \beta^{-2^l} + (\delta^{2^{l-1}})^{2^{2l}} a^{2^{2l}} \beta^{-1} = 0.$$

Sidan $\delta \in GF(2^{2l})$, gjeld

$$\delta^{2^{-l-1}} = \delta^{2^{3l-1}} = \delta^{2^{l-1}},$$

og

$$(\delta^{2^{l-1}})^{2^{2l}} = \delta^{2^{l-1}}.$$

Likninga kan då vidare skrivast

$$\delta^{2^{l-1}} b^{2^{l-1}} \beta^{2^l} + \delta^{2^{l-1}} a\beta + \delta^{2^{l-1}} b^{2^{-l-1}} \beta^{-2^l} + \delta^{2^{l-1}} a^{2^{2l}} \beta^{-1} = 0$$

$$\Rightarrow \delta^{2^{l-1}} (b^{2^{l-1}} \beta^{2^l} + a\beta + b^{2^{-l-1}} \beta^{-2^l} + a^{2^{2l}} \beta^{-1}) = 0, \quad b \neq 0.$$

Likningane (4.6.5) og (4.6.6) for kodeorda $c(a, b)$ og $c(\delta^{2^{l-1}} a, \delta b)$ vil difor ha identiske røter (evt. ingen røter) og

$$w(c(a, b)) = w(c(\delta^{2^{l-1}} a, \delta b)).$$

Jfr. Definisjon 4.3.4. $S_{2l}(a,b) = \{c(\delta^{2^{l-1}} a, \delta b) \mid \delta \in GF(2^l)\}$.

For alle kodeord i $S_{2l}(a,b)$ gjeld

$$c(\delta_1^{2^{l-1}} a, \delta_1 b) + c(\delta_2^{2^{l-1}} a, \delta_2 b) = c((\delta_1^{2^{l-1}} + \delta_2^{2^{l-1}}) a, (\delta_1 + \delta_2) b).$$

Teorem 4.6.1 føreset $a = y$ og $b = 1$. Lat $a,b \in GF(2^{4l})$ slik at $y = a/\sqrt[3]{b}$. Vi skal no bruka same framgangsmåte som i beviset for Teorem 4.6.1, og finna nokre grunnleggjande vilkår for at likninga har *ei* eller 2^l+1 løysingar.

Vi ser på tilfellet $y \in GF(2^{2l})$ og ynskjer likning (4.6.6) på forma

$$y(\beta' + \beta'^{-1}) = (\beta' + \beta'^{-1})^{2^l}, \text{ jfr. likning (4.6.2).}$$

Då vi no har $b \in GF(2^{4l})$, set vi

$$\beta'^{2^l} = b^{2^{l-1}} \beta^{2^l}$$

$$\Rightarrow \beta' = (b^{2^{l-1}} \beta^{2^l})^{2^{-l}} = \sqrt{b}\beta,$$

og kan skriva likninga som

$$y(\sqrt{b}\beta + \sqrt{b}^{2^{2l}} \beta^{-1}) = (\sqrt{b}\beta + \sqrt{b}^{2^{2l}} \beta^{-1})^{2^l}.$$

Likninga har ei løysing om

$$\sqrt{b}\mathsf{b} = \sqrt{b}^{2^{2l}}\mathsf{b}^{-1}$$
$$\Rightarrow \mathsf{b} = \sqrt{b}^{2^{2l}-1}\mathsf{b}^{-1}$$
$$\Rightarrow \mathsf{b}^2 = \sqrt{b}^{2^{2l}-1}\mathsf{b}^{-1}$$
$$\Rightarrow \mathsf{b}^4 = b^{2^{2l}-1}.$$

Dette tyder at likningane for alle kodeord der $y \in GF(2^{2l})$ har ei rot, b ,slik at

$$\mathsf{b}^4 = b^{2^{2l}-1}.$$

Merk. $\sqrt{b}\mathsf{b} = \sqrt{b}^{2^{2l}}\mathsf{b}^{-1} \Rightarrow \sqrt{b}\mathsf{b} \in GF(2^{2l})$.

Vi skriv så likninga på same form som likning (4.6.4) og får

$$y = (\sqrt{b}\mathsf{b} + \sqrt{b}^{2^{2l}}\mathsf{b}^{-1})^{2^l-1}. \qquad (4.6.7)$$

Då $y \neq 0$ og $\sqrt{b}\mathsf{b} \in GF(2^{2l}) \Rightarrow \sqrt{b}\mathsf{b} = \sqrt{b}^{2^{2l}}\mathsf{b}^{-1}$,
kan $\mathsf{b}^4 = b^{2^{2l}-1}$ ikkje lenger vera ei løysing .

Vi ser på tilfellet $y^{2^l+1} = 1$ og får

$$y^{2^l+1} = (\sqrt{b}\mathsf{b} + \sqrt{b}^{2^{2l}}\mathsf{b}^{-1})^{(2^l-1)(2^l+1)} = 1.$$

Likninga kan ikkje ha løysing om $y^{2^l+1} \neq 1$.

Likning (4.6.7) er ekvivalent med likning (4.6.4), og konklusjonane frå Teorem 4.6.1. må gjelda også når $b \in GF(2^{4l})$.

Dette tilseier at om $c(a,b)$ er eit kodeord i C og $(a/\sqrt[s]{b})^{2^l+1} = 1$, vil likninga for kodeordet ha ei rot, b ,slik at $\mathsf{b}^4 = b^{2^{2l}-1}$. Dersom $(a/\sqrt[s]{b}) \neq 1$, vil likninga i tillegg ha 2^l andre løysingar. Desse løysingane er då gitt ved

$$y = (\sqrt{b}^{2^{2l}-1}\mathsf{b}^{-1} + (\sqrt{b}^{2^{2l}-1}\mathsf{b}^{-1})^{-1})$$
$$= (\sqrt{b}^{2^{2l}-1}\mathsf{b}^{-1} + \sqrt{b}^{1-2^{2l}}\mathsf{b}),$$ jfr. likningane (4.6.4 og 4.6.7).

Kodeorda der $(a/\sqrt[s]{b})^{2^l+1} = 1$ har minimumsvekt eller vekt w_3.

Definisjon 4.6.4. Lat $c(a,b)$ vera eit kodeord i C og $(a/\sqrt[s]{b})^{2^l+1} = 1$. Vi definerer

$\mathsf{b}_0 = \mathsf{b}$, slik at $\mathsf{b}^4 = b^{2^{2l}-1}$.

Definisjon 4.6.5.

$$\Gamma = \{v \mid v^{2^l+1} = 1, v \in GF(2^{4l})\}, \ g \in \Gamma$$

Vi prøver no å finna eit enklare uttrykk for relasjonen mellom a og b dersom $(a/\sqrt[s]{b})^{2^l+1} = 1$.

$$y^{2^l+1} = 1$$
$$\Rightarrow a^{2^l+1}/(\sqrt[s]{b})^{2^l+1} = 1$$
$$\Rightarrow a^{(2^l+1)s} / (\sqrt[s]{b})^{(2^l+1)s} = 1$$
$$\Rightarrow a^{(2^l+1)((2^l-1)(2^{2l}+1)+2)} / b^{2^l+1} = 1$$
$$\Rightarrow a^{2(2^l+1)} / b^{2^l+1} = 1$$
$$\Rightarrow (a^2/ b)^{2^l+1} = 1$$
$$\Rightarrow b = a^2\gamma^i, \ \gamma^i \in \Gamma$$

Dette tyder at for alle kodeord der $y^{2^l+1} = 1$, gjeld

$$b = a^2\gamma^i .$$

Alle numeriske resultat tilseier at $d_{2l+1} > g(2l+1, d)$, og at den minste støttevekta vi finn for eit $(2l+1)$-dimensjonalt underrom er $g(2l+1, d) + 2^{l-1}$. Denne støttevekta vert oppnådd når C^*_{2l+1} inneheld *eitt* kodeord med vekt w_3, og resten av kodeorda har minimumsvekt. Denne situasjonen kan forekoma når generatormatrisa til C^*_{2l+1} har *ei* 0-søyle, men *også* når generatormatrisa *ikkje* har 0-søyle.

For å prova d_{2l+1} må vi ut frå dette finna eit C^*_{2l+1} slik at

$$|X(C^*_{2l+1})| = g(2l+1, d).$$

Eller vi må prova allment at eit kodeord med vekt > minimumsvekt finns i eitkvart $(2l+1)$-dimensjonalt underrom, dvs at $d_{2l+1} > g(2l+1, d)$.

Det er difor naudsynt å studera særleg kodeord med vekt w_3 meir detaljert.

Utgangspunktet er likningane (4.6.5) og (4.6.6)

$$\gamma^{2^{2l}+1} = 1.$$

og

$$b^{2^{l-1}}\gamma^{2^l} + a\gamma + b^{2^{-l-1}}\gamma^{-2^l} + a^{2^{2l}}\gamma^{-1} = 0, \ b \neq 0.$$

Lemma 4.6.6. Lat $c(a,b)$ vera eit kodeord i C . Lat $y = a/\sqrt[s]{b}$ og $y^{2^l+1} = 1$ slik at $b = a^2\gamma^i$. Dersom $a^{(2^l-1)(2^{2l}+1)} = \gamma^i$, vil likningane gje eit kodeord med vekt w_3.

Bevis. $b = a^2\gamma^i$

$\Rightarrow b = a^2\, a^{(2^l-1)(2^{2l}+1)}$

$= a^{(2^l-1)(2^{2l}+1)+2}$

$= a^s$

$\Rightarrow y = 1.$

Lemma 4.6.7. Lat $c(a,b)$ vera eit kodeord i C . Lat $y = a/\sqrt[s]{b}$ og $y^{2^l+1} = 1$ slik at $b = a^2\gamma^i$. Dersom $(a / b^{2^{l-1}})^{2^{2l}+1} = 1$, vil likningane gje eit kodeord med vekt w_3.

Bevis. $b = a^2\gamma^i$

$\Rightarrow b^{2^{l-1}} = (a^2\gamma^i)^{2^{l-1}} = a^{2^l}\gamma^{i2^{l-1}}$

$\Rightarrow a / b^{2^{l-1}} = a^{-(2^l-1)} / \gamma^{i2^{l-1}}$.

$(a / b^{2^{l-1}})^{2^{2l}+1} = 1 \Rightarrow (a^{-(2^l-1)} / \gamma^{i2^{l-1}})^{2^{2l}+1} = 1.$

Sidan $\gamma^i \in GF(2^{2l})$ vert

$\gamma^{i(2^{l-1})(2^{2l}+1)} = \gamma^{i(2^{l-1})2} = \gamma^{i2^l}$,

og sidan $\gamma^{i(2^l+1)} = 1$ vert

$\gamma^{i2^l} = \gamma^{-i}$.

Vi får då

$a^{-(2^l-1)(2^{2l}+1)}\gamma^i = 1$

$\Leftrightarrow a^{-(2^l-1)(2^{2l}+1)} = \gamma^{-i}$

$\Leftrightarrow a^{(2^l-1)(2^{2l}+1)} = \gamma^i$,

og kodeordet har vekt w_3, jfr. Lemma 4.6.6.

Numeriske resultat tyder på at det i eit kvart $(2l+1)$-dimensjonalt underrom i koden finns minst eitt kodeord, $c(a,b)$, slik at $(a / b^{2^{l-1}})^{2^{2l}+1} = 1$.

Vi skal i Lemma 4.6.8 og 4.6.9 prova at dersom generatormatrisa til C^*_{2l+1} har ei 0-søyle, inneheld C^*_{2l+1} minst eitt kodeord med vekt > minimumsvekt.

Lemma 4.6.8. Lat $c(a,b)$ vera eit kodeord i C. Lat $y = a/\sqrt[s]{b}$. Dersom

$$b^{2^{l-1}}\beta^{2^l} = a\beta \text{ eller } a^{2^{2l}}\beta^{-1} = b^{2^{-l-1}}\beta^{-2^l},$$

vil likninga gje eit kodeord med vekt > minimumsvekt.

Bevis. Likning (4.6.6) kan skrivast

$$Tr_{2l}^{4l}(a\beta + b^{2^{l-1}}\beta^{2^l}) = 0.$$

β er ei rot i likninga

$$\Leftrightarrow Tr_{2l}^{4l}(a\beta + b^{2^{l-1}}\beta^{2^l}) = 0$$
$$\Leftrightarrow (a\beta + b^{2^{l-1}}\beta^{2^l}) \in GF(2^{2l}).$$

Dersom $(a\beta + b^{2^{l-1}}\beta^{2^l}) = 0$, får vi

$$b^{2^{l-1}}\beta^{2^l} = a\beta$$
$$\Rightarrow \beta^{2^l-1} = a / b^{2^{l-1}}$$
$$\Rightarrow \beta = \sqrt[2^l-1]{a / b^{2^{l-1}}}.$$

Sidan $\beta \in B$, tilseier dette at $(a / b^{2^{l-1}})^{2^{2l}+1} = 1$. Dersom $y^{2^l+1} = 1$, vil likninga då ha *ei* løysing i følgje Lemma 4.6.7. Sidan $y^{2^l+1} = 1$ for alle kodeord med minimumsvekt, kan β ikkje vera rot i likninga for eit minimumvekts-kodeord.

Likning (4.6.6) kan også skrivast

$$Tr_{2l}^{4l}(a^{2^{2l}}\beta^{-1} + b^{2^{-l-1}}\beta^{-2^l}) = 0.$$

β er ei rot i likninga

$$\Leftrightarrow Tr_{2l}^{4l}(a^{2^{2l}}\beta^{-1} + b^{2^{-l-1}}\beta^{-2^l}) = 0$$
$$\Leftrightarrow (a^{2^{2l}}\beta^{-1} + b^{2^{-l-1}}\beta^{-2^l}) \in GF(2^{2l}).$$

Dersom $(a^{2^{2l}}\beta^{-1} + b^{2^{-l-1}}\beta^{-2^l}) = 0$, får vi

$$a^{2^{2l}}\beta^{-1} = b^{2^{-l-1}}\beta^{-2^l}.$$
$$\Rightarrow \beta^{2^l-1} = b^{2^{-l-1}} / a^{2^{2l}}$$
$$\Rightarrow \beta = \sqrt[2^l-1]{b^{2^{-l-1}} / a^{2^{2l}}}.$$

Det kan gjerast tilsvarande utrekningar som i Lemma 4.6.7 også for dette uttrykket. Konklusjonen vert den same. Vi syner her at desse to løysingane er samanfallande dersom $y^{2^l+1} = 1$. Kodeordet vil i dette tilfellet ha vekt w_3. Om røtene er samanfallande, gjeld

$$\sqrt[2^l-1]{a / b^{2^{l-1}}} = \sqrt[2^l-1]{b^{2^{-l-1}} / a^{2^{2l}}}$$
$$\Rightarrow a / b^{2^{l-1}} = b^{2^{-l-1}} / a^{2^{2l}}.$$

Vi har no at $b = a^2\gamma^i$. Då vert

$$b^{2^{l-1}} = a^{2^l}\gamma^{i2^{l-1}},$$

og

$$b^{2^{-l-1}} = a^{2^{-l}}\gamma^{i2^{-l-1}}.$$

Vi set inn desse verdiane, og får

$$a / a^{2^l}\gamma^{i2^{l-1}} = a^{2^{-l}}\gamma^{i2^{-l-1}} / a^{2^{2l}}$$
$$\Rightarrow a^{2^{2l}+1} = a^{2^{-l}}\gamma^{i2^{-l-1}}\ a^{2^l}\gamma^{i2^{l-1}} = a^{2^l(2^{2l}+1)}\gamma^{i2^{l-1}(2^{2l}+1)}$$
$$\Rightarrow a^{-(2^l-1)(2^{2l}+1)} = \gamma^{i2^l}$$
$$\Rightarrow a^{(2^l-1)(2^{2l}+1)} = \gamma^i, \text{ jfr Lemma 4.6.7.}$$

$$\Rightarrow y = 1, \text{ jfr. Lemma 4.6.6.}$$

Lemma 4.6.9. Dersom C^*_{2l+1} har 0-søyler, inneheld C^*_{2l+1} minst *eitt* kodeord med vekt > w_1.

Bevis. Sidan likning (4.6.6) kan skrivast

$$Tr_{2l}^{4l}(a\beta + b^{2^{l-1}}\beta^{2^l}) = 0,$$

kan vi setja

$$f_{ab}(\beta) = Tr_{2l}^{4l}(a\beta + b^{2^{l-1}}\beta^{2^l}) = 0$$

og

$$c^*(a,b) = (f_{ab}(1), f_{ab}(\beta)....f_{ab}(\beta^{2^{2l}})), \text{ jfr. Definisjon 4.3.1.}$$

Jfr. også beviset for Lemma 4.5.8.

Lat $0 \le j \le 2^{2l}$. Lat den j'te søyla i generatormatrisa for C^*_{2l+1} vera ei 0-søyle. Då gjeld

$$c^*_j(a,b) = Tr_{2l}^{4l}(a\beta^j + b^{2^{l-1}}\beta^{j2^l}) = 0 \text{ for alle kodeord i } C^*_{2l+1}.$$

Sidan $Tr_{2l}^{4l}(a\beta^j + b^{2^{l-1}}\beta^{j2^l}) = 0 \Leftrightarrow a\beta^j + b^{2^{l-1}}\beta^{j2^l} \in GF(2^{2l})$, vil vi no få lineærkombinasjonar av $2l+1$ element i $GF(2^{2l})$.

Dei $2l+1$ elementa kan ikkje vera lineært uavhengige. Det vil i denne søyla i C^*_{2l+1} forekoma minst eitt tilfelle av at

$$a\beta^j + b^{2^{l-1}}\beta^{j2^l} = 0$$
$$\Rightarrow a\beta = b^{2^{l-1}}\beta^{2^l}.$$

Sidan likning (4.6.6) og dermed $f_{ab}(\beta)$ også skrivast

$$f_{ab}(\beta) = Tr_{2l}^{4l}(a^{2^{2l}}\beta^{-1} + b^{2^{-l-1}}\beta^{-2^l}) = 0,$$

vil det i den j'te søyla i C^*_{2l+1} no tilsvarande vera minst eitt tilfelle av at

$$a^{2^{2l}}\,\beta^{-1} + b^{2^{-l-1}}\,\beta^{-2^l} = 0$$
$$\Rightarrow a^{2^{2l}}\,\beta^{-1} = b^{2^{-l-1}}\,\beta^{-2^l}.$$

I Lemma 4.6.7 og 4.6.8 synte vi at dersom

$$a\beta = b^{2^{l-1}}\beta^{2^l}, \text{ dvs } \beta = \sqrt[2^l-1]{a / b^{2^{l-1}}},$$

eller

$$a^{2^{2l}}\,\beta^{-1} = b^{2^{-l-1}}\,\beta^{-2^l}, \text{ dvs } \beta = \sqrt[2^l-1]{b^{2^{-l-1}} / a^{2^{2l}}},$$

vil likningane (4.6.5) og (4.6.6) medføra eit kodeord med vekt > w_1. Om røtene er samanfallande, gjeld

$$\sqrt[2^l-1]{a / b^{2^{l-1}}} = \sqrt[2^l-1]{b^{2^{-l-1}} / a^{2^{2l}}},$$

og kodeordet har vekt w_3, om $(a/\sqrt[s]{b}\,)^{2^l+1} = 1$.

Vi kan konkludera med at om C^*_{2l+1} har ei 0-søyle, må C^*_{2l+1} innehalda minst eitt kodeord,

$c^*(a,b)_1$, slik at $a\beta = b^{2^{l-1}}\beta^{2^l}$

og minst eitt kodeord,

$c^*(a,b)_2$, slik at $a^{2^{2l}}\,\beta^{-1} = b^{2^{-l-1}}\,\beta^{-2^l}$.

Kodeorda vil i beggje tilfella ha vekt > w_1. Om $c^*(a,b)_1 = c^*(a,b)_2$, kan likningane for kodeordet ha *ei* løysing, og kodeordet har då vekt w_3. Om $c^*(a,b)_1 \neq c^*(a,b)_2$, tilseier dette at at C^*_{2l+1} må innehalda minst *to* kodeord med vekt > w_1.

I dette avsnittet er det lagt fram nokre vilkår for at likningane (4.5.5) og (4.5.6) medfører kodeord med vekt w_3. Vi har funne at dersom generatormatrisa for C^*_{2l+1} har 0-søyler, vil C^*_{2l+1} innehalda minst eitt kodeord med vekt > w_1. Derimot har vi heller ikkje for denne koden greidd å prova at C^*_{2l+1} *alltid* inneheld kodeord med vekt > w_1, slik alle numeriske resultat tilseier. Vi har dermed ikkje prova d_{2l+1}. Det som er lagt fram i dette avsnittet (og også i Vedlegg III), kan vera viktige delresultat for eit slikt prov.

Alle vidare resultat vedrørande d_r, $2l+1 \le r \le k$, vert dermed ståande som øvre skrankar.

4.6.3 Øvre skrankar for vekthierarkiet, $d_{2l+1} \ldots d_k$.

Vi skal også her følgja metoden som vart skissert i avsnitt 4.4. Lat $0 \le i < 4$ og $1 \le r < k$. Vi skal konstruera generatormatrisa til C^*_r. I kvart intervall, $i2l+1 \le r \le (i+1)2l$, skal vi velja kodeord, $c^*(a,b)_r$. Vi repeterer retningslinjene.

i) $w(c^*(a,b)_r) = w_{i+1}$
ii) $c^*(a,b)_r$ har 0-komponentar i dei *same* søylene.

Om ein vel $c^*(a,b)_r$ slik at $c^*(a,b)_r \in S^*_{2l}(a,b)$, vil desse krava vera tilfredsstillt. Om muleg skal vi dessutan velja kodeorda slik at

iii) Alle 0-komponentane til $c^*(a,b)_r$ ligg innafor 0-søylene i C^*_{i2l}.

Før vi finn skrankane, må vi undersøkja
i) differansen mellom vektene w_{i+1} og w_i, då denne gir differansen mellom $|X(C^*_{i2l+1})|$ og $|X(C^*_{i2l})|$.
ii) om det er muleg å velja $c^*(a,b)_{i2l+1}$ slik at alle 0-komponentane til $c^*(a,b)_{i2l+1}$ ligg innafor 0-søylene i C^*_{i2l}.

Vi reknar først ut vektene. Sidan $D_s(y)$ har 4 verdiar, er C ein 4-vektskode. Vektene er gitt ved

$$w_1 = 2^{4l-1} - 2^{2l-1}((2^l+1)-1) = 2^{4l-1} - 2^{3l-1} = (2^{2l} - 2^l)2^{2l-1} = (2^{2l} - 2^l)\, d_1(C^S)$$
$$w_2 = 2^{4l-1} - 2^{2l-1}(2 - 1) = 2^{4l-1} - 2^{2l-1} = (2^{2l} - 1)\, 2^{2l-1} = (2^{2l} - 1)\, d_1(C^S)$$
$$w_3 = 2^{4l-1} - 2^{2l-1}(1 - 1) = 2^{4l-1} = (2^{2l})\, 2^{2l-1} = 2^{2l}\, d_1(C^S)$$
$$w_4 = 2^{4l-1} - 2^{2l-1}(0 - 1) = 2^{4l-1} + 2^{2l-1} = (2^{2l}+1)\, 2^{2l-1} = (2^{2l}+1)\, d_1(C^S).$$

I motsetning til i forrige kode, er vektene no ikkje påfølgjande multippel av $d_1(C^S)$. Differansen mellom w_2 og w_1 er

$$(2^{2l} - 1)\, d_1(C^S) - (2^{2l} - 2^l)\, d_1(C^S)$$
$$= (2^l - 1)\, d_1(C^S).$$

Differansen mellom vektene w_{i+1} og w_i, om $i > 1$, er som i den andre koden, $d_1(C^S)$.

Merk. C^* er ikkje ein MDS-kode.

Punkt iii) kan tilfredsstillast på følgjande måte. Vi går ut frå at vi i intervallet $1 \le r \le 2l$ har valt kodeord med vekt w_1. Desse har 0-posisjonar tilsvarande b_1, $b_2 \ldots b_{2^l+1}$. Vi skal så finna $c^*(a,b)_{2l+1}$ med vekt w_2. Kodeordet skal om muleg ha 0-posisjonar svarande til b_1 og b_2.

Lat $M = \{c^*(a,b) | (a/b^{2^{l-1}})^{2^l+1} = 1\}$. Vi vel $c^*(a,b)_{2l+1}$ frå M slik at $a/b^{2^{l-1}} = 1/b_1^{2^l}$ men slik at $a/b^{2^{l-1}} \ne a^{2^{2l}} / b^{2^{-l-1}}$. Då vil kodeordet ifølgje Lemma 4.6.8 ha vekt

w_2. Sidan det er muleg å velja slike kodeord for kvar $b \in B$, tilseier dette at det vil vera muleg å finna $c^*(a,b)_{2l+1}$ slik at $a/b^{2^{l-1}} = 1/b_1^{2^l}$, og slik at den andre rota i likningane (4.6.5) og (4.6.6) for kodeordet er b_2.

$c^*(a,b)_{4l+1}$ med vekt w_3 , og med 0-posisjon svarande til b_1, kan også veljast frå M, men slik at

$a/b^{2^{l-1}} = a^{2^{2l}} / b^{2^{-l-1}} = b_1$. Dette vil vera muleg for alle søyler.

Vi kan då konkludera med at det i C finns underrom

i) med dimensjon $\leq 2l$, slik at likningane for alle kodeorda i C_{2l} har 2^l+1 felles røter, og der alle kodeord har vekt w_1.

ii) med dimensjon $\leq 4l$, slik at likningane for alle kodeorda i C_{4l} har *to* felles røter, og der alle kodeord har vekt w_1 og w_2.

iii) med dimensjon $\leq 6l$, slik at likningane for alle kodeorda i C_{6l} har *ei* felles rot, og der alle kodeord har vekt w_1, w_2 og w_3.

Desse underromma vil vera utgangspunkt for "strategi 1".

Eit r-dimensjonalt underrom, C_r , i C tilsvarer eit r-dimensjonalt underrom, C_r^*, i C^*. Dersom likningane for alle kodeorda i C_r har i felles røter, vil generatormatrisa for C_r^* ha i 0-søyler.

4.6.3.1 Strategi 1

Vi går no fram på nøyaktig same måte i forrige avsnitt, og konstruerer følgjande generatormatrise for C^*_r.

Døme 4.6.10. $d \in GF(2^{2l}),\ l = 2.$

$$
\begin{array}{l}
\quad 1\ b\ \ldots \qquad\qquad\qquad\qquad \ldots\ b^{2^{2l}} \\
\underline{G}^* \left\{
\begin{array}{ll}
0\,0\,0\,0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,0\,0\,0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,0\,0\,0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,0\,0\,0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & (2^l+1)\ 0-\textit{søyler, kodeorda i } C^*_{2l} \textit{ har vekt } w_1. \\
0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \textit{to } 0-\textit{søyler, kodeorda i } C^*_{4l} \textit{ har vekt } w_1 \textit{ og } w_2. \\
0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
0\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \textit{ei } 0-\textit{søyle, kodeorda i } C^*_{6l} \textit{ har vekt } w_1,\ w_2 \textit{ og } w_3. \\
d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \\
d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d\,d & \textit{ingen } 0-\textit{søyle, kodeorda i } C^*_{8l} \textit{ har vekt } w_1,\ w_2,\ w_3 \textit{ og } w_4.
\end{array}\right.
\end{array}
$$

Fig.4.6.1 C = [255, 16, 96] , C* = [17, 4, 12]. Generatormatrisa er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken vi finn for d_r etter strategi 1.

Lemma 4.6.11. Øvre skrankar for vekthierarkiet til C etter strategi 1 er gitt ved

$$
\begin{aligned}
d_r &\le (2^{2l}\text{-}2^l)(2^{2l}\text{-}1) + (2^l\text{-}1)(2^{2l} - 2^{4l-r}), \quad \text{om } 2l + 1 \le r \le 4l,\\
&\le (2^{2l}\text{-}1)(2^{2l}\text{-}1) + (2^{2l} - 2^{6l-r}), \quad \text{om } 4l + 1 \le r \le 6l,\\
&\le 2^{2l}\ (2^{2l}\text{-}1) + (2^{2l} - 2^{8l-r}), \quad \text{om } 6l + 1 \le r \le 8l.
\end{aligned}
$$

Bevis.

$2l+1 \le r \le 4l$.

Utgangspunkt er C^*_{2l} der (2^l+1) søyler har rang 0 og dei $(2^{2l}+1)\text{-}(2^l+1) = 2^{2l}\text{-}2^l$ andre søylene har rang $2l$. For detaljar vert det synt til gjennomgangen i forrige avsnitt.

Vi vel så $c^*(a,b)_{2l+1}$ med vekt w_2. Vi har funne at det er muleg å velja dette slik at 0-komponentane svarar til to av 0-søylene i $\underline{G}^*_{2l}$. Då

$$w_2 - w_1 = (2^l - 1)\ d_1(C^S),$$

må rangen auka i $(2^l - 1)$ søyler. I fig.4.6.1. er dette søylene svarande til b^2, b^3, b^4.

I heile intervallet $2l+1 \le r \le 4l$ vel vi $c^*(a,b)_r$ frå $S^*_{2l}(a,b)$. Då vil dei $2l$ kodeorda vera ulike i denne søyla. Rangen, r , til dei $2^l - 1$ søylene aukar frå 0 til $2l$.

Dette inneber at

$$d_r \le d_{2l} + (2^l-1)\, d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 2l.$$
$$= (2^{2l}-2^l)(2^{2l}-1) + (2^l-1)(2^{2l} - 2^{4l-r}) = d_r^{'\max}.$$

$4l+1 \le r \le 6l$.

Utgangspunkt er C^*_{4l} der 2 søyler har rang 0, og $2^{2l}-1$ søyler har rang $2l$.

Vi vel $c^*(a,b)_{4l+1}$ med vekt w_3. Vi har funne at det er muleg å velja dette slik at 0-komponenten svarar til ei av 0-søylene i $\underline{G}^*_{4l}$. Rangen kan også no auka frå 0 til 1 i *ei* søyle. I fig.4.6.1. er dette søyla svarande til b.

I heile intervallet $4l+1 \le r \le 6l$ vel vi $c^*(a,b)_r$ frå $S^*_{2l}(a,b)$. Då vil dei $2l$ kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå 0 til $2l$.

Den øvre skranken er då gitt av

$$d_r \le d_{4l}^{'\max} + d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 4l.$$
$$= (2^{2l}-1)(2^{2l}-1) + (2^{2l} - 2^{6l-r}).$$

$6l+1 \le r \le 8l$.

Utgangspunkt er C^*_{6l} der 1 søyle har rang 0, og 2^{2l} søyler har rang $2l$.
Vi vel $c^*(a,b)_{6l+1}$ med vekt w_4.

I heile intervallet $6l+1 \le r \le 8l$ vel vi $c^*(a,b)_r$ frå $S^*_{2l}(a,b)$. Då vil dei $2l$ kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå 0 til $2l$.

Den øvre skranken er då gitt av

$$d_r \le d_{6l}^{'\max} + d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 6l.$$
$$= 2^{2l}(2^{2l}-1) + (2^{2l} - 2^{8l-r}) = d_r^{'\max}.$$

Differansen mellom w_2 og w_1 medførte at kodeordet $c^*(a,b)_{2l+1}$ gav eit tillegg i støttevekta på $(2^l-1)\, d_1(C^S)$. Dette medfører at $d_{2l+1}^{'\max} > > g(2l+1, d)$. Vi skal no undersøkja om det er muleg å finna ein betre øvre skranke for intervallet $2l+1 \le r \le 4l$.

4.6.3.2 Strategi 2

Definisjon 4.6.12.

$U = \{c(a,b) \mid (a/\sqrt[s]{b})^{2^l+1} = 1\}$

$V = \{c(a,b) \mid b = a^2\gamma, \gamma \in G, \gamma$ er konstant$\}$, jfr. Definisjon 4.6.5.

Frå forrige avsnitt har vi at $V \subseteq U$ og at likningane (4.6.5) og (4.6.6) for alle kodeord i U har 2^l+1 eller *ei* rot.

$|U| = N_{2^l+1} n +$ # kodeord der $a/\sqrt[s]{b} = 1$,

$= (2^{5l} - 2^l) + (2^{4l} - 1) = 2^{5l} + 2^{4l} - 2^l - 1 = (2^l+1)(2^{4l}-1)$.

Lemma 4.6.13. Lat $\delta \in GF(2^{2l})$. Lat $c(a,b)_1$ og $c(a,b)_2$ vera to kodeord med minimumsvekt. Lat $c(a,b)_1 + c(a,b)_2 = c(a,b)_3$. Då er

$c(a,b)_3 \in U \Leftrightarrow \gamma_1 = \gamma_2 = \gamma_3$ eller $(a_1/a_2) = \delta \in GF(2^{2l})$.

Bevis. $(a_1,b_1) + (a_2,b_2) = (a_3,b_3)$

$\Rightarrow (a_1, a_1^2\gamma_1) + (a_2, a_2^2\gamma_2) = (a_3, a_3^2\gamma_3)$

$\Rightarrow (a_1, a_1^2\gamma_1) + (a_2, a_2^2\gamma_2) = ((a_1 + a_2), (a_1 + a_2)^2\gamma_3)$.

b_3 kan no skrivast som

i) $b_3 = b_1 + b_2 = (a_1 + a_2)^2\gamma_3$, og

ii) $b_3 = b_1 + b_2 = a_1^2\gamma_1 + a_2^2\gamma_2$.

Vi får då

$a_1^2\gamma_1 + a_2^2\gamma_2 = (a_1 + a_2)^2\gamma_3$

$\Rightarrow a_1^2\gamma_1 + a_2^2\gamma_2 = (a_1^2 + a_2^2)\gamma_3$

$\Rightarrow a_1^2\gamma_1 + a_2^2\gamma_2 = a_1^2\gamma_3 + a_2^2\gamma_3$

$\Rightarrow a_1^2\gamma_1 + a_1^2\gamma_3 = a_2^2\gamma_2 + a_2^2\gamma_3$

$\Rightarrow a_1^2(\gamma_1 + \gamma_3) = a_2^2(\gamma_2 + \gamma_3), \quad a_i \neq 0.$

Dette har ei løysing dersom $\gamma_1 = \gamma_2 = \gamma_3$.

Dersom $(\gamma_1 \neq \gamma_2)$ eller $(\gamma_2 \neq \gamma_3)$, får vi

$a_1^2(\gamma_1 + \gamma_3) = a_2^2(\gamma_2 + \gamma_3)$

$\Rightarrow (a_1^2 / a_2^2) = (\gamma_2 + \gamma_3) / (\gamma_1 + \gamma_3) = \delta^j / \delta^k, \delta \in GF(2^{2l})$

$\Rightarrow (a_1 / a_2) = \sqrt{\delta^{j-k}} \in GF(2^{2l})$.

Likninga

$a_1^2\gamma_1 + a_2^2\gamma_2 = (a_1 + a_2)^2\gamma_3$

har difor ei løysing $\Leftrightarrow \gamma_1 = \gamma_2 = \gamma_3$ eller $(a_1 / a_2) = \delta \in GF(2^{2l})$.

Korollar 4.6.14. Lemma 4.6.13 syner at V er eit vektorrom sidan γ er konstant for alle kodeord. Kodeorda i V har vekt w_1 eller vekt w_3.

Vi skal no finna mengda R slik at

$$R \subseteq V \text{ og } R \subseteq S_{2l}(a,b).$$

Lat $\delta \in GF(2^{2l})$. Vi har frå forrige avsnitt at for alle kodeord i $S_{2l}(a,b)$ gjeld

$$c(\delta_1^{2^{l-1}} a, \delta_1 b) + c(\delta_2^{2^{l-1}} a, \delta_2 b) = c((\delta_1^{2^{l-1}} + \delta_2^{2^{l-1}}) a, (\delta_1 + \delta_2) b).$$

Lat $\zeta \in GF(2^l)$. Vi ser på kodeord med vekt w_1 og w_3. Vi skal finna $R \subseteq S_{2l}(a,b)$ slik at

$$c(\zeta_1^{2^{l-1}} a, \zeta_1 b) + c(\zeta_2^{2^{l-1}} a, \zeta_2 b) = c((\zeta_1^{2^{l-1}} + \zeta_2^{2^{l-1}}) a, (\zeta_1 + \zeta_2) b),$$

gjeld for alle kodeord i R.

Sidan $\zeta \in GF(2^l)$, gjeld

$$(\zeta^{2^{l-1}})^2 = \zeta^{2^l} = \zeta.$$

Vi tek så utgangspunkt i beviset for Lemma 4.6.13.

b_3 kan no skrivast som

i) $b_3 = b_1 + b_2 = (\zeta_1^{2^{l-1}} a + \zeta_2^{2^{l-1}} a)^2 \gamma_3 = (\zeta_1 a^2 + \zeta_2 a^2)\gamma_3.$

ii) $b_3 = b_1 + b_2 = (\zeta_1^{2^{l-1}} a)^2 \gamma_1 + (\zeta_2^{2^{l-1}} a)^2 \gamma_2 = \zeta_1 a^2 \gamma_1 + \zeta_2 a^2 \gamma_2.$

Vi får då

$$\zeta_1 a^2 \gamma_1 + \zeta_2 a^2 \gamma_2 = (\zeta_1 a^2 + \zeta_2 a^2)\gamma_3.$$
$$\Rightarrow \zeta_1 a^2(\gamma_1 + \gamma_3) = \zeta_2 a^2(\gamma_2 + \gamma_3),\ a \neq 0.$$

Dette har ei løysing dersom $\gamma_1 = \gamma_2 = \gamma_3$.

Definisjon 4.6.15.
Lat $R^*_l(a,b)$ vera eit l-dimensjonalt underrom i C^* slik at

$$R^*_l(a,b) = \{\zeta c^*(a,b) \mid \zeta \in GF(2^l)\},$$

og $R_l(a,b)$ det tilsvarande l-dimensjonale underrommet i C.

Merk. Når γ går gjennom $\Gamma \subseteq GF(2^{2l})$, vil det for kvar verdi av γ finnast kodeord, $c^*(a,b)$, slik at

$$R^*_l(a,b) \subseteq S^*_{2l}(a,b)$$

og

$$R^*_l(a,b) \subseteq V^* \subseteq U^*.$$

Dette tilseier at

$$|V| = |U| / (2^l +1) = (2^l +1)(2^{4l} -1)/(2^l +1)$$
$$= 2^{4l} -1.$$

V er ifølgje Korollar 4.6.14 eit vektorrom. Vi får då at $\dim(V) = 4l$.

Lat $0 \le j \le 2^l$. Lat $V^*_j = \{ c^*(a,b) \mid b = a^2\gamma^j \}$.

Lat $0 \le i < 8$. Vi brukar no same metoden som ved strategi 1 til å finna øvre skrankar, men endrar følgjande i framgangsmåten

i) Vi brukar kortare intervall, dvs $il +1 \le r \le (i+1)l$.

ii) I intervallet $1 \le r \le 4l$ brukast berre kodeord frå V^*_1, og slik at
$w(c^*(a,b)_r) = w_1$, om $1 \le r \le 2l$ og
$w(c^*(a,b)_r) = w_3$, om $2l+1 \le r \le 4l$
I intervallet $4l +1 \le r \le k$ brukast berre kodeord frå V^*_1, og slik at
$w(c^*(a,b)_r) = w_1$, om $4l+1 \le r \le 6l$
$w(c^*(a,b)_r) = w_3$, om $6l+1 \le r \le k$.

Innan kvart intervall vel vi kodeord frå $R^*_l (a,b)$. Då sikrar vi at $c^*(a,b)_r$ har dei *same* 0-posisjonane, og at dei er ulike i dei andre posisjonane.

Vi undersøkjer no om det då er muleg å velja $c^*(a,b)_{il+1}$ slik at alle 0-komponentane til $c^*(a,b)_{il+1}$ ligg innafor 0-søylene i C^*_{il}.

Vi går ut frå at vi i intervallet $1 \le r \le l$ har valt kodeord med vekt w_1. Desse har 0-posisjonar, $\beta_1, \beta_2 \ldots \beta_{2^l+1}$. Vi kan då gå ut frå at for alle kodeorda i C^*_{il} gjeld

$$\beta_1{}^4 = b_r{}^{2^{2l}-1},$$ jfr. Definisjon 4.6.4.

Vi skal så finna $c^*(a,b)_{l+1}$ som også skal ha vekt w_1 , og som har 0-posisjonane β_1 og β_2. Kodeordet kan då veljast slik at $\beta_2{}^4 = b_r{}^{2^{2l}-1}$. Sidan det er muleg å velja slike kodeord for kvar $\beta \in B$, tilseier dette at det vil vera muleg å finna $c^*(a,b)_{l+1}$ slik at ei av dei 2^l andre røtene vil vera β_1, jfr. likning (4.6.7).

Generatormatrisa for C^*_{2l} vil no ha to 0-søyler. Sidan det ikkje finns kodeord med vekt w_2 i V, tyder dette at alle kodeorda i C^*_{2l} har minimumsvekt.

Vi skal så velja $c^*(a,b)_{2l+1}$ med vekt w_3. Kodeordet skal ha 0-posisjonen svarande til β_1 og kan veljast slik at

$$a/b^{2^{l-1}} = a^{2^{2l}} / b^{2^{-l-1}} = \beta_1,$$ jfr Lemma 4.6.8.

Dette vil vera muleg for alle søyler.

$c^*(a,b)_{3l+1}$ skal også ha vekt w_3. Då det i V_1 finns berre finns l lineært uavhengige kodeord med vekt w_3 slik at 0-posisjonen svarar til β_1, vel vi kodeordet slik at

$$a/b^{2^{l-1}} = a^{2^{2l}} / b^{2^{-l-1}} \neq \beta_1.$$

Vi kan då konkludera med at det i C også finns underrom

i) med dimensjon $\leq l$, slik at likningane for alle kodeorda i C_l har $2^l + 1$ felles røter, og der alle kodeord har vekt w_1.

ii) med dimensjon $\leq 2l$, slik at likningane for alle kodeorda i C_{2l} har *to* felles røter, og der alle kodeord har vekt w_1 og w_3.

iii) med dimensjon $\leq 3l$, slik at likningane for alle kodeorda i C_{3l} har *ei* felles rot, og der alle kodeord har vekt w_1 og w_3.

iv) med dimensjon $\leq 4l$, slik at likningane for alle kodeorda i C_{4l} ikkje har felles røter, der alle kodeord har vekt w_1 og w_3, og der $b = a^2$g, g$\in$ G, g er konstant, for alle kodeorda i underrommet.

Desse underromma vil vera utgangspunkt for "strategi 2".

Vi konstruerer følgjande generatormatrise for C^*_r.

Døme 4.6.16. d $\in GF(2^{2l})$, $l = 2$.

```
        1 b . . .                  . . b^(2^(2l))
       0 0 0 0 0 d d d d d d d d d d d d
       0 0 0 0 0 d d d d d d d d d d d d    (2^l + 1) 0 – søyler, kodeorda i C*_l har vekt w1.
       0 0 d d d d d d d d d d d d d d d
       0 0 d d d d d d d d d d d d d d d    to 0 – søyler, kodeorda i C*_2l har vekt w1.
       0 d d d d d d d d d d d d d d d d
       0 d d d d d d d d d d d d d d d d    ei 0 – søyle, kodeorda i C*_3l har vekt w1 og w3.
       d d d d d d d d d d d d d d d d d
G*     d d d d d d d d d d d d d d d d d    ingen 0 – søyle, kodeorda i C*_4l har vekt w1 og w3.
       d d d d d d d d d d d d d d d d d
       d d d d d d d d d d d d d d d d d
       d d d d d d d d d d d d d d d d d
       d d d d d d d d d d d d d d d d d    ingen 0 – søyle, kodeorda i C*_6l har vekt w1, w2, w3 og w4.
       d d d d d d d d d d d d d d d d d
       d d d d d d d d d d d d d d d d d
       d d d d d d d d d d d d d d d d d
       d d d d d d d d d d d d d d d d d.
```

Fig.4.6.2 C = [255, 16, 96] , C* = [17, 4, 12]. Generatormatrisa er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken vi finn for d_r etter strategi 2.

Merk. C^S har dimensjon $2l$.
$d_l\,(C^S) = 2^{2l} - 2^{2l-l} = 2^{2l} - 2^l$.

Vi ser på intervallet $il + 1 \leq r \leq (i+1)l$. Når rangen, r , til ei søyle i C^*_{il} aukar frå 0 til l, representerer dette for heile intervallet ein auke i supportvekta på

$$2^{2l} - 2^l.$$

Auken er på kvart steg gitt av

$$2^{2l} - 2^{2l - \text{r}} .$$

Dei l kodeorda, $c^*(a,b)_r$, medfører dei l første "kodeorda" i ei generatormatrise for C^S.

Når rangen til denne søyla i eit *seinare* intervall aukar frå l til $2l$, representerer dette for heile intervallet ein auke i supportvekta på

$$d_{2l}(C^S) - d_l(C^S) = 2^{2l} - 1 - (2^{2l} - 2^l) = 2^l - 1.$$

Auken er på kvart steg gitt av

$$d_{\mathsf{r}}(C^S) - d_l(C^S) = 2^{2l} - 2^{2l-\mathsf{r}} - (2^{2l} - 2^l) = 2^l - 2^{2l-\mathsf{r}}.$$

Dei l kodeorda, $c^*(a,b)_r$, medfører dei l siste "kodeorda" i generatormatrisa for C^S.

Lemma 4.6.17. Øvre skrankar for vekthierarkiet til C etter strategi 2 er gitt ved

$$\begin{aligned}
d_r &\le (2^{2l}-1)(2^{2l}-2^l) + (2^{2l}-2^{4l-r}), && \text{om } 2l+1 \le r \le 3l,\\
&\le 2^{2l}(2^{2l}-2^l) + (2^{2l}-2^{5l-r}), && \text{om } 3l+1 \le r \le 4l,\\
&\le (2^{2l}+1)(2^{2l}-2^l) + (2^{2l}-2^l)(2^l-2^{5l-r}), && \text{om } 4l+1 \le r \le 5l,\\
&\le (2^{2l}+1)(2^{2l}-2^l) + (2^{2l}-2^l)(2^l-1) + (2^l-1)(2^l-2^{6l-r}), && \text{om } 5l+1 \le r \le 6l,\\
&\le (2^{2l}+1)(2^{2l}-2^l) + (2^{2l}-1)(2^l-1) + (2^l-2^{7l-r}), && \text{om } 6l+1 \le r \le 7l,\\
&\le (2^{2l}+1)(2^{2l}-2^l) + 2^{2l}(2^l-1) + (2^l-2^{8l-r}), && \text{om } 7l+1 \le r \le 8l.
\end{aligned}$$

Bevis.

$2l+1 \le r \le 3l$.

Utgangspunkt er C^*_{2l} der 2 søyler har rang 0, og $(2^{2l}+1) - 2 = 2^{2l} - 1$ søyler har rang l. Dette tilseier at $|X(C_{2l})| = (2^{2l}-1)\, d_l(C^S) = (2^{2l}-1)(2^{2l}-2^l) = d_{2l}$, jfr Teorem 4.6.3. Vi føreset at $C^*_{2l} \subseteq V^*_1$.

Vi vel så $c^*(a,b)_{2l+1}$ med vekt w_3. Vi har funne at det er muleg å velja dette slik at 0-komponentane svarar til ei av dei to 0-søylene i $\underline{G}^*_{2l}$. Då må rangen auka i *ei* søyle. I fig.4.3.1. er dette søyla svarande til b.

I heile intervallet $2l+1 \le r \le 3l$ vel vi $c^*(a,b)_r$ frå $R^*_l(a,b) \subseteq V^*_1$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til dei $2^l - 1$ søylene aukar frå 0 til l.

Dette inneber at

$$\begin{aligned}
d_r &\le d_{2l} + d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 2l.\\
&= (2^{2l}-1)(2^{2l}-2^l) + (2^{2l} - 2^{4l-r}) = d_r^{'\max}.
\end{aligned}$$

$3l+1 \le r \le 4l$.

Utgangspunkt er C^*_{3l} der 1 søyle har rang 0, og 2^{2l} søyler har rang l.

Vi vel også $c^*(a,b)_{3l+1}$ med vekt w_3. Vi har funne at det ikkje er muleg å velja dette slik at 0-komponenten svarar til 0-søyla i $\underline{G}^*_{3l}$. Rangen må då auka frå 0 til 1 i 0-søyla. I fig.4.6.1. er dette søyla svarande til $\mathsf{b} = 1$.

I heile intervallet $3l+1 \le r \le 4l$ vel vi $c^*(a,b)_r$ frå $R^*_l(a,b) \subseteq V^*_1$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå 0 til l.

Den øvre skranken er då gitt av

$$d_r \le d^{'\max}_{3l} + d_{\mathsf{r}}(C^S), \text{ der } \mathsf{r} = r - 3l.$$
$$= 2^{2l}(2^{2l} - 2^l) + (2^{2l} - 2^{5l-r}) = d^{'\max}_r.$$

$4l+1 \le r \le 5l$.

Utgangspunkt er C^*_{4l} der alle søyler har rang l. Vi har no at $C^*_{4l} = V^*_1$.

Vi vel $c^*(a,b)_{4l+1}$ med minimumsvekt w_1. Rangen må då auka frå l til $2l$ i $(2^{2l}+1) - (2^l - 1) = 2^{2l} - 2^l$ søyler.

I heile intervallet $4l+1 \le r \le 5l$ vel vi $c^*(a,b)_r$ frå $R^*_l(a,b) \subseteq V^*_2$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til søylene aukar frå l til $2l$.

Den øvre skranken er då gitt av

$$d_r \le d^{'\max}_{4l} + (2^{2l} - 2^l)(d_{\mathsf{r}}(C^S) - d_l(C^S)), \text{ der } \mathsf{r} = r - 3l.$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 2^{2l-\mathsf{r}})$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 2^{5l-r}) = d^{'\max}_r.$$

$5l+1 \le r \le 6l$.

Utgangspunkt er C^*_{5l} der $2^l + 1$ søyler har rang l, og dei $2^{2l} - 2^l$ andre søylene har rang $2l$.

Vi vel også $c^*(a,b)_{5l+1}$ med minimumsvekt w_1. Sidan V^*_2 inneheld eit $2l$-dimensjonalt underrom der likningane (4.6.5) og (4.6.6) har *to* felles røter, vil det vera muleg finna $c^*(a,b)_{5l+1}$ slik at 2 av 0-komponentane ligg innafor søylene med rang l, dvs innafor 0-søylene til $c^*(a,b)_r$ brukt i intervallet $4l+1 \le r \le 5l$.

I heile intervallet $5l+1 \le r \le 6l$ vel vi $c^*(a,b)_r$ frå $R^*_l(a,b) \subseteq V^*_2$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå l til $2l$.

Den øvre skranken er då gitt av

$$d_r \le d^{'\max}_{5l} + (d_{\mathsf{r}}(C^S) - d_l(C^S)), \text{ der } \mathsf{r} = r - 4l.$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 1) + (2^l - 1)(2^l - 2^{2l-\mathsf{r}}).$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 1) + (2^l - 1)(2^l - 2^{6l-r}) = d^{'\max}_r.$$

$6l+1 \le r \le 7l$.

Utgangspunkt er C^*_{6l} der 2 søyler har rang l, og dei 2^{2l} -1 andre søylene har rang $2l$.

Vi vel $c^*(a,b)_{6l+1}$ med vekt w_3. Det vil vera muleg å finna $c^*(a,b)_{5l+1}$ slik at 0-komponenten ligg innafor søylene med rang l, dvs innafor 0-søylene til $c^*(a,b)_r$ brukt i intervallet $4l+1 \le r \le 6l$.

I heile intervallet $6l+1 \le r \le 7l$ vel vi $c^*(a,b)_r$ frå $R^*_l(a,b) \subseteq V^*_2$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå l til $2l$.

Den øvre skranken er då gitt av

$$\begin{aligned} d_r &\le d^{'\max}_{6l} + (d_{\mathsf{r}}(C^S) - d_l(C^S)), \text{ der } \mathsf{r} = r - 5l. \\ &= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 1)(2^l - 1) + 2^l - 2^{2l-\mathsf{r}} \\ &= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 1)(2^l - 1) + 2^l - 2^{7l-r} = d^{'\max}_r. \end{aligned}$$

$7l+1 \le r \le 8l$.

Utgangspunkt er C^*_{7l} der 1 søyle har rang l, og dei 2^{2l} andre søylene har rang $2l$.

Vi vel $c^*(a,b)_{7l+1}$ med vekt w_3. Det vil ikkje vera muleg å finna $c^*(a,b)_{5l+1}$ i V^*_2 slik at 0-komponenten svarar til søyla med rang l, dvs innafor 0-søyla til $c^*(a,b)_r$ brukt i intervallet $4l+1 \le r \le 7l$.

I heile intervallet $7l+1 \le r \le 8l$ vel vi $c^*(a,b)_r$ frå $R^*_l(a,b) \subseteq V^*_2$. Då vil dei l kodeorda vera ulike i denne søyla. Rangen, r, til søyla aukar frå l til $2l$.

Den øvre skranken er då gitt av

$$\begin{aligned} d_r &\le d^{'\max}_{7l} + (d_{\mathsf{r}}(C^S) - d_l(C^S)), \text{ der } \mathsf{r} = r - 6l. \\ &= (2^{2l}+1)(2^{2l} - 2^l) + 2^{2l}(2^l - 1) + 2^l - 2^{2l-\mathsf{r}} \\ &= (2^{2l}+1)(2^{2l} - 2^l) + 2^{2l}(2^l - 1) + 2^l - 2^{8l-r} = d^{'\max}_r. \end{aligned}$$

4.6.3.3 Samanlikning av skrankane.

Vi skal no samanlikna skrankane vi har funne etter desse to strategiane for å finna dei beste. Eit anna resultat av denne samanlikninga er at vi kan syna at koden ikkje tilfredsstiller kjedevilkåret.

Definisjon 4.6.18.
Lat $d_r^{'\max}1$ vera øvre skranke for d_r funnen etter strategi 1.
Lat $d_r^{'\max}2$ vera øvre skranke for d_r funnen etter strategi 2.

Dersom $m = 4$, vert
$s = 2^{l+1}-1$, $m = 2l$, $l = 2$,
$= (2^l-1)(2^{2l}+1) + 2$, $m = 4l$, $l = 1$.

Vi får dermed den same koden. Med $l = 1$ vil $d_r^{'\max}1$ samsvara med skrankane vi fann for den første Niho-koden, der vi då tilsvarande hadde $l = 2$. Vi ser i dette avsnittet difor berre på $l > 1$.

Teorem 4.6.19. Øvre skrankar for vekthierarkiet til C er gitt ved

$$\begin{aligned}
d_r &\le (2^{2l}-1)(2^{2l}-2^l) + (2^{2l}-2^{4l-r}), && \text{om } 2l+1 \le r \le 3l,\\
&\le 2^{2l}(2^{2l}-2^l) + (2^{2l}-2^{5l-r}), && \text{om } 3l+1 \le r \le 4l,\\
&\le (2^{2l}+1)(2^{2l}-2^l) + (2^{2l}-2^l)(2^l-2^{5l-r}), && \text{om } 4l+1 \le r < 5l,\\
&\le (2^{2l}-1)(2^{2l}-1) + (2^{2l}-2^{6l-r}), && \text{om } 5l \le r \le 6l,\\
&\le 2^{2l}(2^{2l}-1) + (2^{2l}-2^{8l-r}), && \text{om } 6l+1 \le r \le 8l.
\end{aligned}$$

Bevis.

$2l+1 \le r \le 4l$.
Vi kan her samanlikna $d_r^{'\max}1$ for eit $(2l+1)$-dimensjonale underrommet direkte med $d_r^{'\max}2$ for det $4l$-dimensjonale underrommet.

$$\begin{aligned}
&d_{2l+1}^{'\max}1 - d_{4l}^{'\max}2\\
&= (2^{2l}-2^l)(2^{2l}-1) + (2^l-1)(2^{2l}-2^{4l-r}) - (2^{2l}(2^{2l}-2^l) + (2^{2l}-2^{5l-r}))\\
&= (2^{2l}-2^l)(2^{2l}-1) + (2^l-1)(2^{2l}-2^{2l-1}) - (2^{2l}(2^{2l}-2^l) + (2^{2l}-2^l))\\
&= 2^{3l-1} - 2^{2l-1} - 2^{2l-1} + 2^{l+1}\\
&= 0 \text{ for } l = 2 \text{ og } > 0 \text{ for } l > 2.
\end{aligned}$$

Dette tyder at $d_r^{'\max}2 < d_r^{'\max}1$ for heile intervallet.

$4l+1 \le r < 5l$.
Vi samanliknar her dei to skrankane for eit $(5l-1)$- dimensjonal underrom.

$$\begin{aligned}
&d_{5l-1}^{'\max}1 - d_{5l-1}^{'\max}2\\
&= (2^{2l}-1)(2^{2l}-1) + (2^{2l}-2^{6l-r}) - ((2^{2l}+1)(2^{2l}-2^l) + (2^{2l}-2^l)(2^l-2^{5l-r}))\\
&= (2^{2l}-1)(2^{2l}-1) + (2^{2l}-2^{l+1}) - ((2^{2l}+1)(2^{2l}-2^l) + (2^{2l}-2^l)(2^l-2))\\
&= 2^{2l} - 2^{l+2} + 2^l + 1 \quad > 0 \text{ for } l \ge 2.
\end{aligned}$$

Framleis er $d_r^{'\max}2 < d_r^{'\max}1$. Dette må gjelda for heile intervallet.

***r* = 5*l*.**

Vi samanliknar her dei to skrankane for eit 5*l*- dimensjonal underrom.

$d_{5l}^{'\max} 2 - d_{5l}^{'\max} 1$

$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 2^{5l-r}) - ((2^{2l}-1)(2^{2l}-1) + (2^{2l} - 2^{6l-r}))$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l - 1) - ((2^{2l}-1)(2^{2l}-1) + (2^{2l} - 2^l))$$
$$= 2^l - 1 > 0 \text{ for } l \geq 2.$$

Tilhøvet mellom skrankane har no snudd, og $d_r^{'\max} 1 < d_r^{'\max} 2$.

$5l+1 \leq r \leq 6l$.

Vi samanliknar her dei to skrankane for eit 6*l*- dimensjonal underrom.

$d_{6l}^{'\max} 2 - d_{6l}^{'\max} 1$

$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l-1) + (2^l-1)(2^l - 2^{6l-r})$$
$$-((2^{2l}-1)(2^{2l}-1) + (2^{2l} - 2^{6l-r}))$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 2^l)(2^l-1) + (2^l-1)(2^l - 1)$$
$$-((2^{2l}-1)(2^{2l}-1) + (2^{2l} - 1))$$
$$= 2^{2l} - 2^{l+1} + 1 > 0 \text{ for } l \geq 2.$$

Framleis er $d_r^{'\max} 1 < d_r^{'\max} 2$. Dette må gjelda for heile intervallet.

$6l+1 \leq r < 7l$.

Vi samanliknar her dei to skrankane for eit (7*l*-1)- dimensjonal underrom.

$d_{7l-1}^{'\max} 2 - d_{7l-1}^{'\max} 1$

$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 1)(2^l-1) + 2^l - 2^{7l-r}$$
$$- (2^{2l} (2^{2l}-1) + (2^{2l} - 2^{8l-r}))$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 1)(2^l-1) + 2^l - 2$$
$$- (2^{2l} (2^{2l}-1) + (2^{2l} - 2^{l+1}))$$
$$= 2^l - 1 > 0 \text{ for } l \geq 2.$$

Framleis er $d_r^{'\max} 1 < d_r^{'\max} 2$. Dette må gjelda for heile intervallet

***r* = 7*l*.**

Vi samanliknar her dei to skrankane for eit 7*l*- dimensjonal underrom.

$d_{7l}^{'\max} 2 - d_{7l}^{'\max} 1$

$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 1)(2^l-1) + 2^l - 2^{7l-r}$$
$$- (2^{2l} (2^{2l}-1) + (2^{2l} - 2^{8l-r}))$$
$$= (2^{2l}+1)(2^{2l} - 2^l) + (2^{2l} - 1)(2^l-1) + 2^l - 1$$
$$- (2^{2l} (2^{2l}-1) + (2^{2l} - 2^l))$$
$$= 2^{4l} - 2^l - (2^{4l} - 2^l) = 0.$$

Skrankane er like.

$7l+1 \leq r \leq 8l$.
$d_r^{'max}$ 2 kan skrivast

$$(2^{2l}+1)(2^{2l} - 2^l) + 2^{2l}(2^l-1) + 2^l - 2^{8l-r}$$
$$= 2^{2l}(2^{2l}-1) + (2^{2l} - 2^{8l-r}) = d_r^{'max} 1.$$

Skrankane er like.

Om vi brukar dei beste skrankane for kvart intervall, følgjer teoremet.

Lemma 4.6.20. Koden tilfredsstiller ikkje kjedevilkåret.

Bevis. $d_{2l+1}^{'max}$ vart funnen etter strategi 2. Lemma 4.6.13 tilseier at dersom

$$D^*_{2l} \subseteq D^*_{2l+1},$$

må D^*_{2l} vera V^*_{2l} slik vi gjekk ut frå i Lemma 4.6.17.

$d_{4l}^{'max}$ vart også funnen etter strategi 2 og tilsvarer supportvekta til V, dvs. til eit $4l$-dimensjonalt underrom, C^*_{4l}, der generatormatrisa til C^*_{4l} har rang l i alle søyler. Vi valde på kvart steg, $2l+1 \leq r \leq 4l$, kodeord til generatormatrisa slik at tillegget til supportvekta vart minst muleg.

Dette tyder at dersom

$$D^*_{2l} \subseteq D^*_{2l+1} \subseteq ... \subseteq D^*_{4l},$$

må generatormatrisa til D_{4l} ha rang l i alle søyler.

Med V^* som utgangspunkt valde vi på kvart steg, $4l+1 \leq r \leq 5l$, kodeord slik at tillegget til supportvekta vart minst muleg. Dette syner at dersom C^*_{5l} inneheld $4l$-dimensjonalt underrom, C^*_{4l}, der generatormatrisa til C^*_{4l} har rang l i alle søyler, *må* supportvekta til C^*_{5l} vera større enn $d_{5l}^{'max}$ som vi fann etter strategi 1.

Dette tyder at dersom $D^*_{4l} \subseteq D^*_{5l}$, så kan ikkje D^*_{4l} vera V^*. Då kan heller ikkje D^*_{2l+1} vera V^*_{2l+1}, og D^*_{2l} er ikkje V^*_{2l}. Om $D^*_{2l} \subseteq D^*_{2l+1}$, vert her ei motseiing.

Dette tyder at *eitt* av følgjande to alternativ må gjelda for koden

i) $D^*_{2l} \subseteq D^*_{2l+1} \subseteq ... \subseteq D^*_{4l}$ som medfører at $D^*_{4l} \not\subseteq D^*_{5l}$

ii) $D^*_{4l} \subseteq D^*_{5l}$ som medfører at $D^*_{2l} \not\subseteq D^*_{4l}$.

4.6 Samandrag

For beggje kodar er vekthierarkiet funne for d_r ,om $1 \le r \le k/4$. I beggje tilfella er d_r i dette intervallet gitt av

$$d_r = g(r,d).$$

Det er utvikla ein metode for å finna øvre skrankar for d_r, om $k/4+1 \le r \le k$. Det er grunn til å tru at skrankane som er funne etter denne metoden, er gode. Numeriske resultat tilseier at dei gjeld med likskap. Metoden er ikkje særskilt knytt til Niho-kodar, og kan truleg nyttast på ei rekkje kodar.

Den største vansken har vore å prova at $d_{k/4+1} > g(r,d)$. Problemet ser ut til å vera det same i beggje kodane. I den første koden må ein prova at det i eit kvart $(k/4+1)$-dimensjonalt underrom må finnast eit kodeord, $c(a,b)$, slik at

$$(a/b^{2^{k/4}})^{2^{k/4}+1} = 1.$$

Det må då i alle lineærkombinasjonar av $(k/4+1)$ likningar,

$$Tr_{k/4}^{k/2}(a^2\beta^j + b^2\beta^{-3j}) = 0,\ 0 \le j \le 2^{k/4}, \beta^{2^{k/4}+1}=1,\ a,b \in GF(2^{k/2}).$$

finnast ei løysing β , slik at $\beta = a/b^{2^{k/4}}$.

I den andre koden har vi tilsvarande at det i eit kvart $(k/4+1)$-dimensjonalt underrom må vera eit kodeord der

$$(a/b^{2^{k/8-1}})^{2^{k/4}+1} = 1.$$

Det må då i alle lineærkombinasjonar av $(k/4+1)$ likningar,

$$Tr_{k/4}^{k/2}(a\beta^j + b^{2^{k/8-1}}\beta^{j2^{k/8}}) = 0,\ 0 \le j \le 2^{k/4}, \beta^{2^{k/4}+1}=1,\ a,b \in GF(2^{k/2}).$$

finnast ei løysing β , slik at $\beta = a/b^{2^{k/8-1}}$.

Det ser ut til at dette kan vera eit vanskeleg problem. Om det vert løyst, vil det truleg vera enkelt å prova d_r, om $k/4+1 \le r \le k$. Dersom $d_{k/4+1} > g(r,d)$ for den første koden, vil d_r, om $k/4+1 \le r \le k/2$, vera gitt direkte, ettersom den øvre skranken i dette intervallet er prova til å vera $g(r,d) + 1$. Vi har prova at denne skranken gjeld med likskap om $k/4 \le 4$. Om $k/4 = 2$, er kodane like.

Vi synte at den siste koden ikkje tilfredsstiller kjedevilkåret om $k/4 > 2$. For den første koden er ikkje dette studert spesielt, men alle numeriske resultat tyder på at denne koden tilfredsstiller dette vilkåret. Det er kjent at kodar der $n = g(k,d)$ og der $n = g(k,d) + 1$ tilfredsstiller kjedevilkåret [8]. Dette tilseier då at den første koden tilfredsstiller kjedevilkåret om $1 \le r \le k/2$,

Tabellane i Vedlegg V syner numeriske resultat for kodane om $k \le 32$.

Kapittel 5

Irredusible sykliske kodar

5.1 Introduksjon

Vi skal studera vekthierarkiet til tre endelege klassar av irredusible sykliske kodar over $GF(2)$. Blokklengda er $n = n_1(2^l-1)$.

Lat $h(x) \in GF(q)[x]$ vera eit irredusibelt polynom med grad k og periode n. Ein irredusibel syklisk (n, k)-kode C over $GF(q)$ er definert av

$$C = \{c(a) \mid c(a) = (Tr_1^k(a), Tr_1^k(a\beta),...,Tr_1^k(a\beta^{n-1})); a \in GF(q^k)\},$$

der β er ei rot i $h(x)$.

Dei tre klassane kan då karakteriserast ved k/l , der $k/l = 2$, $k/l = n_1$ og $k/l = n_1-1$. Vektdistribusjonen til desse kodane er funnen av Helleseth, Kløve og Mykkeltveit [6]. Ettersom bevisa for vektdistribusjonen er svært viktige for å finna vekthierarkiet, er dei tekne med i oppgåva.

5.2 Definisjonar og grunnleggjande resultat

Lemma 5.2.1, 5.2.4, 5.2.5, Korollar 5.2.2 og Definisjon 5.2.3 er henta frå [6].

Lemma 5.2.1. Lat $n = n_1n_2$, der $n_2 \mid q^l-1$. Då kan komponentane i $c(a)$ arrangerast som ei n_1 x n_2 matrise $(u_{j_1j_2})$ slik at $u_{j_1j_2} = Tr_1^l(\beta^{j_2n_1} Tr_l^k(a\beta^{j_1}))$.

Bevis. Lat $0 \le j < n$. Då kan j skrivast unikt som $j = j_2 n_1 + j_1$ med $0 \le j_1 < n_1$ og $0 \le j_2 < n_2$. Lat $c_j(a)$ vera den j'te komponenten i $c(a)$. Vi får då

$$\begin{aligned} c_j(a) &= Tr_1^k(a\beta^j) \\ &= Tr_1^k(a\beta^{j_2n_1+j_1}) \\ &= Tr_1^k(\beta^{j_2n_1} a\beta^{j_1}). \end{aligned}$$

$\beta^{j_2 n_1} \in GF(q^l)$ sidan $\beta^{n_1 n_2} = 1$. Dette inneber at

$$c_j(a) = Tr_1^l(\beta^{j_2 n_1} Tr_l^k(a\beta^{j_1})) = u_{j_1 j_2}.$$

Korollar 5.2.2. Dersom $n = n_1 n_2$, $n_2 \mid q^l-1$ og l vert valt så liten som muleg, vil kvar rekkjevektor tilhøyra ein irredusibel (n_2, l)-kode. Dersom $n_2 = q^l-1$, får vi $k = ml$, og kvar rekkjevektor høyrer til ein maksimal skiftregister-kode.

Frå no av går vi ut frå at $n_2 = q^l - 1$ og definerer følgjande kodar

Definisjon 5.2.3.

$$C = \{c(a) \mid c(a) = (Tr_1^k(a), Tr_1^k(a\beta),...,Tr_1^k(a\beta^{n-1})); a \in GF(q^k)\},$$
$$C^* = \{c^*(a) \mid c^*(a) = (Tr_l^k(a), Tr_l^k(a\beta),...,Tr_l^k(a\beta^{n_1-1})); a \in GF(q^k)\},$$
$$C^{*+} = \{c^{*+}(a) \mid c^{*+}(a) = (Tr_l^k(a), Tr_l^k(a\beta),...,Tr_l^k(a\beta^{n-1})); a \in GF(q^k)\}.$$

C er ein irredusibel syklisk (n, k)-kode over $GF(q)$,
C^* er ein lineær $(n_1, k/l)$-kode over $GF(q^l)$,
C^{*+} er ein irredusibel syklisk $(n_1(q^l-1), k/l)$-kode over $GF(q^l)$.

Lemma 5.2.4. Lat $c^{*+}(a) = (c_0, c_1,..., c_{n-1}) \in C^{*+}$. Då får vi $c^{*+}_{sn_1+t} = \beta^{sn_1} c_t$.

Bevis. Frå definisjonen av C^{*+} får vi

$$c^{*+}_{sn_1+t} = Tr_l^k(a\beta^{sn_1+t}) = \beta^{sn_1} Tr_l^k(a\beta^t) = \beta^{sn_1} c_t$$

sidan $\beta^{n_1} \in GF(q^l)$.

Lemma 5.2.5. Lat $A(z)$, $A^*(z)$, $A^{*+}(z)$ vera vektoppteljarane til C, C^* og C^{*+}. Då gjeld følgjande relasjon mellom vektoppteljarane

$$A(z) = A^*(z^{q^{l-1}(q-1)}) = A^{*+}(z^{q^{l-1}(q-1)/(q^l-1)})$$

Bevis. Lat $A^*(z) = \sum_{i=0}^{n_1} A^*_i z^i$. Det er ein-til-ein-relasjon mellom C^* og C gitt av $c^*(a) \leftrightarrow c(a)$. Lat i vera vekta av $c^*(a)$. I følgje Korollar 5.2.2 vil vekta av $c(a)$ vera $(q^{l-1}(q-1)i)$ sidan vi har i ikkje-null-rekkjer, og $(q^{l-1}(q-1))$ er vekta til eit kode-ord, $c(a) \neq \underline{0}$, i ein maksimal skiftregisterkode. Vi får då

$$A(z) = \sum_{i=0}^{n_1} A^*_i \, z^{q^{l-1}(q-1)i} . = A^*(z^{q^{l-1}(q-1)}) = A^{*+}(z^{q^{l-1}(q-1)/(q^l-1)})$$

sidan $A^{*+}(z) = A^*(z^{q^{l-1}})$.
$1 \le k/l \le n_1$ vil alltid gjelda.

I avsnitta 5.3 og 5.4 går vi ut frå at q = 2.

5.3 Vekthierarkiet, $d_1 ... d_l$.

Teorem 5.3.1. Vekthierarkiet til alle kodeklassana er gitt av

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 \text{ , om } 1 \le r \le l.$$

Bevis. Vi set $q = 2$. Frå Lemma 5.2.1 har vi

$$c_j(a) = Tr^l_1(\beta^{j_2 n_1} Tr^k_l(a\beta^{j_1})) \text{ og } \beta^{j_2 n_1} \in GF(2^l).$$

Vi deler opp eit kodeord i n_1 blokker med lengde n_2 og ser på dei n_2 posisjonane $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1})$. Ein slik blokk tilsvarar ein rekkjevektor i matrisa $(u_{j_1 j_2})$, jfr. Korollar 5.2.2. Posisjonane i blokken får vi ved å la $\beta^{j_2 n_1}$ gå gjennom $GF(2^l)$ - {0}, medan leddet $Tr^k_l(a\beta^{j_1})$ er konstant.

Om $Tr^k_l(a\beta^{j_1}) \neq 0$, vil halvparten av posisjonane $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1})$ få

$$Tr^l_1(\beta^{j_2 n_1} Tr^k_l(a\beta^{j_1})) = 1,$$

den andre halvparten

$$Tr^l_1(\beta^{j_2 n_1} Tr^k_l(a\beta^{j_1})) = 0.$$

Om $Tr^k_l(a\beta^{j_1}) = 0$, vil *alle* posisjonane $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1})$ få

$$Tr^l_1(\beta^{j_2 n_1} Tr^k_l(a\beta^{j_1})) = 0.$$

Posisjonane $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1})$ vil dermed alltid ha vekt 0 eller 2^{l-1}.

Lat $0 \le j_1 \le n_1$-1. Lat $c^*(a)$ vera eit kodeord i C^* . Posisjonane i kodeordet er gitt av

$$c^*_{j_1}(a) = Tr^k_l(a\beta^{j_1}).$$

Lat $\delta \in GF(2^l)$. Sidan koden er syklisk, vil det også finnast kodeord, $\delta c(a)$, med posisjonar gitt av

$$\delta c^*_{j_1}(a) = \delta Tr^k_l(a\beta^{j_1}).$$

Vi ser på den j_1'te posisjonen i kodeorda tilsvarande β^{j_1}. Dersom $c^*_j(a) = 0$, vil $\delta\, c^*_j(a) = 0$. Dersom $c^*_j(a) \neq 0$, vil $\delta\, c^*_j(a) \neq 0$. $\delta\, c^*_j(a)$ går gjennom $GF(2^l)$ når δ gjer det.

Mengda $\{\delta\, c^*(a) \mid \delta \in GF(2^l)\}$ vil utgjera eit l-dimensjonalt underrom i C^* sidan

$$c^*_j(a) + \delta\, c^*_j(a) = (1+\delta)c^*_j(a)$$

som medfører at

$$c^*(a) + \delta\, c^*(a) = (1+\delta)c^*(a).$$

Underrommet vil innehalda kvart (2^l+1)'te sykliske skift av $c^*(a)$.

Eit slikt underrom karakteriserast ved at

i) Kodeorda har $Tr_l^k(a\beta^{j_1}) = 0$ i dei same posisjonane.

ii) Kodeorda vil vera ulike i posisjonar der $Tr_l^k(a\beta^{j_1}) \neq 0$.

Dette tyder at alle kodeorda i underrommet har same vekt. Vi får då at

$$w(c(a)) = w(\delta\, c(a)),$$

og teoremet følgjer.

Korollar 5.3.2. Ettersom blokken $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1})$ har vekt 0 eller 2^{l-1} for alle kodeord i C, vil skiftregister-koden som denne blokken/rekkjevektoren inngår i, vera ein $[2^l-1, l, 2^{l-1}]$ Simplex-kode.

Vi ser at vi også for desse kodane kan bruka Definisjon 4.3.4 vedrørande underrommet, S_l, og Definisjon 4.3.6 vedrørande Simplex-koden, C^S.

Merk. Også i desse kodane vil vektene vera ulike multippel av $d_1(C^S)$.
$d_r(C)$ kan sjåast som eit multippel av $d_r(C^S)$, om $1 \leq r \leq l$.

5.4 Ein metode til å finna nedre skrankar for $d_{l+1} ... d_k$

Resultata frå forrige avsnitt tilseier at vi kan nytta same metoden som for Niho-kodane når vi skal finna øvre skrankar for d_r, om $l+1 \leq r \leq k$. Skilnaden vert at vi no handsamar *blokker* i generatormatrisa for C direkte, medan vi for Niho-kodane brukte *søylene* i generatormatrisa for C^* som utgangspunkt.

Lat $0 \leq i < k/l$ og $1 \leq r < k$. Vi ser på intervallet $il+1 \leq r \leq (i+1)l$, og skal konstruera generatormatrisa til koden ved å velja kodeord, $c(a)_r$, slik at

i) $w(c\,(a)_r) = w_{i+1}$

ii) $c\,(a)_r$ har 0-komponentar i dei *same* søylene.

Om ein vel $c\,(a)_r$ slik at $c\,(a)_r \in S_l(a)$, jfr. Definisjon 4.3.4, vil desse krava vera tilfredsstillt. Om muleg vel vi dessutan kodeorda slik at

iii) Alle 0-komponentane til $c(a)_r$ ligg innafor 0-søylene i C^*_{il}.

Lat generatormatrisa til C_{il} vera arrangert som synt ovanfor. Då vil C_{il} innehalda kodeord av vekt $\leq w_i$. Generatormatrisa er synt i fig. 5.4.1.

Døme 5.4.1. $l = 3$, $w_1 = 2(2^{l-1})$.

$$\underline{G} \quad \begin{matrix} \leftarrow n_2 \rightarrow \leftarrow n_2 \rightarrow \leftarrow n_2 \rightarrow \leftarrow n_2 \rightarrow \leftarrow .. \\ \left\{ \begin{matrix} 1111000\ 1111000\ 0000000\ 0000000\ \ldots. \\ 1100110\ 1100110\ 0000000\ 0000000\ \ldots. \\ 1010101\ 1010101\ 0000000\ 0000000\ \ldots. \\ 1111000\ 1111000\ 1111000\ 0000000\ \ldots. \\ 1100110\ 1100110\ 1100110\ 0000000\ \ldots. \\ 1010101\ 1010101\ 1010101\ 0000000\ldots. \\ 1111000\ 1111000\ 1111000\ 1111000\ \ldots. \\ 1100110\ 1100110\ 1100110\ 1100110\ \ldots. \\ 1010101\ 1010101\ 1010101\ 1010101\ \ldots. \\ \ldots. \quad \ldots. \quad \ldots. \quad \ldots. \\ \ldots. \quad \ldots. \quad \ldots. \quad \ldots. \end{matrix} \right. \end{matrix} \begin{matrix} \\ \\ l \text{ kodeord. Kodeorda i } C_l \text{ har vekt } w_1. \\ \\ \\ 2l \text{ kodeord. Kodeorda i } C_{2l} \text{ har vekt } w_1 \text{ og } w_2. \\ \\ \\ 3l \text{ kodeord. Kodeorda i } C_{3l} \text{ har vekt } w_1, w_2 \text{ og } w_3. \\ \\ \end{matrix}$$

Fig. 5.4.1. Utsnitt av generatormatrisa som er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken for d_r.

Ved å konstruera generatormatriser på denne måten, vil vi for alle kodar enkelt kunna finna øvre skrankar for d_r ,om $l+1 \leq r \leq k$.

Vi ser så på ein metode for å finna nedre skrankar. Vi har funne at alle vekter er multippel av $d_1(C^S) = 2^{l-1}$. I kodane finns k/l ulike vekter [6]. Frå forrige avsnitt har vi

$w(c(a)) = w(\mathsf{d}\, c(a))$.

Då må følgjande gjelda

$(w(c(a)) = w(\mathsf{d}\, c(a)) = w_i$, for $1 \leq i \leq k/l$.

Dette tyder at vektene er påfølgjande multippel av $d_1(C^S) = 2^{l-1}$. Då må det i kodane finnast l-dimensjonale underrom, W_l, generert av

r uavhengige kodeord med vekt w_{i+1},

og

$(l\text{-}\mathsf{r})$ uavhengige kodeord med vekt w_i.

Definisjon 5.4.1. Lat $1 \leq r, r \leq l$. Vi definerer følgjande underrom i C.

$U_r = \{ u(a) \mid w(u(a)) = w_i \}$.

$V_r = \{ v(a) \mid w(v(a)) = w_{i+1} \}$.

$W_l = \{$ l-dimensjonalt underrom generert av r lineært uavhengige kodeord frå V og $(l\text{-}r)$ lineært uavhengige kodeord frå U $\}$.

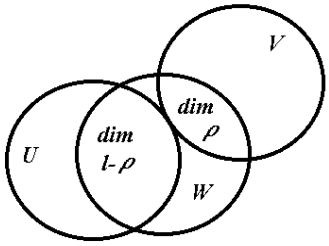

Fig. 5.4.2. Figuren syner dei tre l-dimensjonale underromma U_l , V_l og W_l .

Vi skal no finna $|X(W_l)|$. Vi ser først på $S_l(a) = \{ c\,(a) \mid \in GF(2^l) \}$, som også finns i desse kodane ifølgje forrige avsnitt. Om kodeorda i $S_l(a)$ har vekt w_i , gjeld

$$d_r\,(S(a)\,) = \frac{1}{2^{r-1}} \sum_{c \in S} w_i \ .$$

Vi kan gå ut frå at $w_1 = t2^{l-1}$ og $w_2 = (t+1)2^{l-1}$.

Då får vi

$$| X\,(U_r\,)| \ = t\, d_r\,(C^S\,) = t(2^l - 2^{l-r}\,),$$

og

$$| X\,(U_l\,)| \ = \ t\, d_l\,(C^S\,) = t\,(2^l - 1).$$

$$\begin{aligned} | X\,(V_r\,)| \ &= \ (t+1)(2^l - 2^{l-r}\,) \\ &= t(2^l - 2^{l-r}\,) + (2^l - 2^{l-r}\,) \\ &= | X\,(U_r\,)| + (2^l - 2^{l-r}\,) \end{aligned}$$

og

$$| X\,(V_l\,)| = \ | X\,(U_l\,)| + (2^l - 1\,)$$

Lat T_l vera eit l-dimensjonalt underrom i C slik at $T_l = V_l \cap U_l$. Då er

$$| X\,(T_r\,)| = \ d_r\,(C^S\,) = 2^l - 2^{l-r}\ ,$$

og

$$| X\,(T_l\,)| = d_l\,(C^S\,) = 2^l - 1\ .$$

Då vert

$$|X(W_l)| = (|X(V_r)| + |X(U_l)|) - (|X(V_r) \cap X(U_l)|)$$
$$= (|X(U_r)| + |X(T_r)| + |X(U_l)|) - (|(X(U_r) \cup X(T_r)) \cap X(U_l)|).$$

Sidan

$$X(U_r) \cap X(U_l) = X(U_r),$$

og

$$X(T_r) \cap X(U_l) = 0,$$

får vi vidare

$$|X(W_l)| = (|X(U_r)| + |X(T_r)| + |X(U_l)|) - (|X(U_r)|)$$
$$= |X(U_l)| + |X(T_r)|$$
$$= t(2^l - 1) + (2^l - 2^{l-r}).$$

Lat $1 \le i < k/l$. Lat W_l vera generert av r lineært uavhengige kodeord med vekt w_{i+1}, og $(l-r)$ lineært uavhengige kodeord med vekt w_i. Om vi kan påvisa at eitkvart underrom med dimensjon $(il+r)$ inneheld W_l, vil $|X(W_l)|$ vera ein nedre skranke for d_{il+r}.

5.5 $k/l = 2$

Teorem 5.5.1. Lat C vera ein irredusibel $(n_1(q^l-1), k)$-kode over $GF(q)$. Dersom $k/l = 2$, vil vektoppteljaren vera

$$A(z) = 1 + (q^l-1)n_1 z^{q^{l-1}(q-1)(n_1-1)} + (q^{2l}-1-(q^l-1)n_1) z^{q^{l-1}(q-1)n_1}.$$

Bevis. I følgje Lemma 5.2.5 er det nok å syna at $C^* - \{\underline{0}\}$ ikkje inneheld kodeord med vekt $< n_1-1$ og å finna talet på kodeord med vekt $n_1 - 1$. (Vi utelet her den delen av beviset som vedrører *talet* på kodeord med vekt n_1-1.)
Vi går ut frå at $c^*(a) = (c_0,\ldots, c_{n_1-1})$ har $c_j = 0$ og $c_{j+s} = 0$ for ein $s > 0$. Dette fører til ei motseiing. Lat $c^{*+}(a) = (c_0,\ldots, c_{n_1-1})$. Velg t slik at $\beta^{n_1 t} = c_{j+1}^{-1} c_{j+s+1}$ og $0 < t \le q^l-1$. Dette er muleg sidan β^{n_1} er eit primitivt element i $GF(q^l)$. Frå Lemma 5.2.4 får vi

$$(c_{j+n_1t}, c_{j+n_1t+1}) = (\beta^{n_1t} c_j, \beta^{n_1t} c_{j+1})$$
$$= (0, c_{j+s+1})$$
$$= (c_{j+s}, c_{j+s+1}).$$

Sidan dimensjonen til C^{*+} er $k/l = 2$, tyder dette at $c^{*+}(a)$ har periode e, der $e \le n_1t - s < n_1t \le n_1(q^l-1)$. Dette er umuleg sidan C^{*+} er ein irredusibel syklisk $(n_1(q^l-1), 2)$-kode.

[6]

5.5 $k/l = 2$

Teorem 5.5.1. Lat C vera ein irredusibel $(n_1(q^l\text{-}1), k)$-kode over $GF(q)$. Dersom $k/l = 2$, vil vektoppteljaren vera

$$A(z) = 1 + (q^l\text{-}1)n_1 z^{q^{l-1}(q-1)(n_1-1)} + (q^{2l}\text{-}1\text{-}(q^l\text{-}1)n_1) z^{q^{l-1}(q-1)n_1}.$$

Bevis. I følgje Lemma 5.2.5 er det nok å syna at $C^* - \{\underline{0}\}$ ikkje inneheld kodeord med vekt $< n_1\text{-}1$ og å finna talet på kodeord med vekt n_1 -1. (Vi utelet her den delen av beviset som vedrører *talet* på kodeord med vekt n_1-1.)
Vi går ut frå at $c^*(a) = (c_0,..., c_{n_1-1})$ har $c_j = 0$ og $c_{j+s} = 0$ for ein $s > 0$. Dette fører til ei motseiing. Lat $c^{*+}(a) = (c_0,..., c_{n_1-1})$. Velg t slik at $\beta^{n_1 t} = c_{j+1}^{-1} c_{j+s+1}$ og $0 < t \le q^l\text{-}1$. Dette er muleg sidan β^{n_1} er eit primitivt element i $GF(q^l)$. Frå Lemma 5.2.4 får vi

$$\begin{aligned}(c_{j+n_1t}, c_{j+n_1t+1}) &= (\beta^{n_1 t} c_j, \beta^{n_1 t} c_{j+1}) \\ &= (0, c_{j+s+1}) \\ &= (c_{j+s}, c_{j+s+1}).\end{aligned}$$

Sidan dimensjonen til C^{*+} er $k/l = 2$, tyder dette at $c^{*+}(a)$ har periode ε, der $\varepsilon \le n_1 t - s < n_1 t \le n_1(q^l\text{-}1)$. Dette er umuleg sidan C^{*+} er ein irredusibel syklisk $(n_1(q^l\text{-}1), 2)$-kode.

[6]

Teorem 5.5.1 syner at C er ein 2-vektskode og at $w_2 = (n_1/(n_1\text{-}1))w_1$.

Frå Lemma 5.2.5 og Teorem 5.5.1 får vi

$$A(z) = A^*(z^{q^{l-1}(q-1)})$$
$$\Rightarrow A^*(z) = 1 + (q^l\text{-}1)n_1 z^{n_1-1} + (q^{2l}\text{-}1\text{-}(q^l\text{-}1)n_1) z^{n_1}.$$

Ettersom C^* ikkje innheld kodeord med vekt $< n_1$-1, vil eit kodeord med minimumsvekt innehalda $(n_1\text{-}1)$ komponentar, $c^*_{j_1}(a)$, der $Tr_l^k(ab^{j_1}) \neq 0$, medan eit kodeord med maksimumsvekt inneheld n_1 slike komponentar, jfr.avsnitt 5.2. Eit kodeord med minimumsvekt i C^* tilsvarer eit kodeord i C der $(n_1\text{-}1)$ blokker, $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1}) \neq$ "0,...,0".

Vi går frå no av ut frå at $q = 2$.Vektene vert $w_1 = d_1 = (n_1\text{-}1)2^{l-1}$ og $w_2 = n_1 2^{l-1}$.

Merk. C^* er ein MDS-kode sidan $k = n - d + 1 = n_1 - (n_1\text{-}1) + 1 = 2$.

Teorem 5.5.2. Vekthierarkiet til C er gitt av

$$d_r = (n_1\text{-}1)(2^l - 2^{l-r}), \text{ om } 1 \le r \le l,$$
$$= (n_1\text{-}1)(2^l\text{-}1) + (2^l - 2^{2l-r}), \text{ om } l+1 \le r \le k.$$

Bevis.

$1 \le r \le l$.

Vi har frå Teorem 5.3.1, Korollar 5.3.2 og Teorem 5.5.1 at

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 = (n_1\text{-}1) \sum_{i=0}^{r-1} \left\lceil \frac{2^{l-1}}{2^i} \right\rceil = (n_1\text{-}1)(2^l - 2^{l-r}).$$

$l+1 \le r \le k$.

Vi finn først ein øvre skranke etter metoden skissert i avsnitt 5.4, og konstruerer følgjande generatormatrise for C.

Døme 5.5.3. $n_1 = 3$, $l = 3$, $w_1 = (n_1\text{-}1)2^{l-1}$.

$$\underline{G} \quad \begin{cases} \overset{\leftarrow n_2 \rightarrow}{1111000} \; \overset{\leftarrow n_2 \rightarrow}{1111000} \; \overset{\leftarrow n_2 \rightarrow}{0000000} \\ 1100110 \; 1100110 \; 0000000 \\ 1010101 \; 1010101 \; 0000000 & l \text{ kodeord. Kodeorda i } C_l \text{ har vekt } w_1. \\ 1111000 \; 1111000 \; 1111000 \\ 1100110 \; 1100110 \; 1100110 \\ 1010101 \; 1010101 \; 1010101 & 2l \text{ kodeord. Kodeorda i } C_{2l} \text{ har vekt } w_1 \text{ og } w_2. \end{cases}$$

Fig. 5.5.1. $C = [\,21, 6, 8\,]$. Generatormatrisa er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken for d_r.

Lat $0 \le i < k/l$. For kvart intervall, $il + 1 \le r \le (i+1)l$, skal vi velja kodeord $c\,(a)_r$ slik at $w(c\,(a)_r) = w_{i+1}$ og $c\,(a)_r \in S_l(a)$. Sidan koden er syklisk og vektene er påfølgjande multippel av 2^{l-1}, vil det vera muleg å velja kodeorda slik at alle 0-komponentane til $c(a)_r$ ligg innafor 0-søylene i C^*_{il}. Dette vil medføra ei generatormatrise for C^S.

Vi får då følgjande øvre øvre skranke for d_r i dette intervallet.

$$d_r \le d_l + d_{\mathsf{r}}\,(C^S), \text{ der } \mathsf{r} = r - l.$$
$$= (n_1\text{-}1)(2^l\text{-}1) + (2^l - 2^{2l-r}) = d_r^{'\max}.$$

Ettersom $k = 2l$, må eit l-dimensjonalt underrom av kodeord med vekt w_2, V_l, skjera eitkvart $(l+1)$-dimensjonalt underrom i C. Vi kan difor finna ein nedre skranke etter metoden frå avsnitt 5.4.

Lat $r > l$ og $\mathsf{r} = r - l$. Då vil det i eitkvart underrom $C_r \subseteq C$ finnast eit l-dimensjonalt underrom, W_l, generert av r lineært uavhengige kodeord med vekt w_2 og $(l\text{-}\mathsf{r})$ lineært uavhengige kodeord med vekt w_1, jfr. Definisjon 5.4.1.

Når $w_i = t\,2^{l-1}$ og $w_2 = (t+1)2^{l-1}$, vil støttevekta til W_l ifølgje avsnitt 5.4 vera gitt av

$$|\,X(W_l)\,| = t\,(2^l - 1) + (2^l - 2^{l-\mathsf{r}}).$$

$|\,X(W_l)\,|$ vil i intervallet $l+1 \le r \le k$ vera ein nedre skranke for $d_{l+\mathsf{r}} = d_r$.

Sidan $t = n_1\text{-}1$, vert

$$d_r \ge |\,X(W_l)\,|$$
$$= (n_1\text{-}1)(2^l - 1) + (2^l - 2^{l-(r-l)})$$
$$= (n_1\text{-}1)(2^l\text{-}1) + (2^l - 2^{2l-r}) = d_r^{'\min} = d_r^{'\max}.$$

For denne koden, der $k/l = 2$, er vekthierarkiet tidlegare funne [10]. Resultata samsvarer.

5.6 $k/l = n_1$

Teorem 5.6.1. Lat C vera ein irredusibel $(n_1(q^l\text{-}1), k)$-kode over $GF(q)$. Dersom $k/l = n_1$, vil vektoppteljaren vera

$$A(z) = (1 + (q^l\text{-}1)\, z^{q^{l-1}(q-1)})^{n_1}.$$

Bevis. Sidan k/l = n_1, vil C^* vera ein (n_1, n_1)-kode med vektoppteljar

$$A^*(z) = \sum_{i=0}^{n_1} \binom{n_1}{i} (q^l - 1)^i z^i = (1 + (q^l\text{-}1)\, z)^{n_1}.$$

Teoremet følgjer av Lemma 5.2.5.

[6]

Teorem 5.6.1 syner at C har n_1 ulike vekter, $w \neq 0$, og at $w_i = iw_1$, $1 \leq i \leq n_1$. Vidare er vektene uavhengige av n_1.

Ettersom C^* har minimumsvekt 1, vil eit kodeord med minimumsvekt innehalda *ein* komponent, $c^*_{j_1}(a)$, der $Tr_l^k(a\beta^{j_1}) \neq 0$. Eit kodeord med vekt $t\,2^{l-1}$ vil ha t slike komponentar, jfr. avsnitt 5.2. Eit kodeord med minimumsvekt i C^* tilsvarer då eit kodeord i C der *ein* blokk, $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1}) \neq$ "0,...,0".

Vi går frå no av ut frå at $q = 2$. Vektene vert $w_t = t\,2^{l-1}$, $1 \leq t \leq n_1$.

Merk. C^* er ein MDS-kode sidan $k = n - d + 1 = n_1 - 1 + 1 = n_1$.

Teorem 5.6.2. Vekthierarkiet til C er gitt av

$$\begin{aligned} d_r &= (2^l - 2^{l-r}), \text{ om } \quad 1 \leq r \leq l, \\ &= t(2^l\text{-}1) + (2^l - 2^{(t+1)l-r}), \text{ om } l+1 \leq r \leq k, \ t = \lfloor r / l \rfloor. \end{aligned}$$

Bevis.

1 ≤ r ≤ l.

Vi har frå Teorem 5.3.1, Korollar 5.3.2 og Teorem 5.6.1 at

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 = \sum_{i=0}^{r-1} \left\lceil \frac{2^{l-1}}{2^i} \right\rceil = (2^l - 2^{l-r}).$$

l+1 ≤ r ≤ k.

Vi finn først ein øvre skranke etter metoden skissert i avsnitt 5.4, og konstruerer følgjande generatormatrise for C.

Døme 5.6.3. $n_1 = 3$, $l = 4$, $w_1 = 2^{l-1}$.

$\underline{G}$

$\leftarrow n_2 \rightarrow$	$\leftarrow n_2 \rightarrow$	$\leftarrow n_2 \rightarrow$	
111111110000000	000000000000000	000000000000000	
111100001111000	000000000000000	000000000000000	
110011001100110	000000000000000	000000000000000	
101010101010101	000000000000000	000000000000000	l *kodeord. Kodeorda i* C_l *har vekt* w_1.
111111110000000	111111110000000	000000000000000	
111100001111000	111100001111000	000000000000000	
110011001100110	110011001100110	000000000000000	
101010101010101	101010101010101	000000000000000	$2l$ *kodeord. Kodeorda i* C_{2l} *har vekt* w_1 *og* w_2.
111111110000000	111111110000000	111111110000000	
111100001111000	111100001111000	111100001111000	
110011001100110	110011001100110	110011001100110	
101010101010101	101010101010101	101010101010101	$3l$ *kodeord. Kodeorda i* C_{3l} *har vekt* w_1, w_2 *og*

Fig. 5.6.1. $C = [\,45, 12, 8\,]$. Generatormatrisa er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken for d_r.

Lat $0 \le i < k/l$. For kvart intervall, $il + 1 \le r \le (i+1)l$, skal vi velja kodeord $c\,(a)_r$ slik at $w(c\,(a)_r) = w_{i+1}$ og $c\,(a)_r \in S_l(a)$. Sidan koden er syklisk og vektene er påfølgjande multippel av 2^{l-1}, vil det vera muleg å velja kodeorda slik at alle 0-komponentane til $c(a)_r$ ligg innafor 0-søylene i C^*_{il}. Dette vil medføra ei generatormatrise for C^S.

Vi får då følgjande øvre øvre skranke for d_r i dette intervallet.

$$d_r \le d_{il} + d_{\mathsf{r}}\,(C^S), \text{ der } \mathsf{r} = r - il.$$
$$= i(2^l-1) + (2^l - 2^{(i+1)l - r}).$$

Lat $t = \lfloor r / l \rfloor$. Den øvre skranken for d_r ,om $l + 1 \le r \le k$, vert

$$d_r \le t(2^l - 1) + (2^l - 2^{(t+1)l-r}) = d_r^{'\max}.$$

Lat $1 \le \mathrm{t} < k/l$. Lat $tl + 1 \le r \le (t+1)l$ og $\mathsf{r} = r - tl$. Om resultatet frå avsnitt 5.4. skal kunna nyttast, må vi syna at eitkvart $C_r \subseteq C$ inneheld eit l-dimensjonalt underrom, W_l , generert av r lineært uavhengige kodeord med vekt $(t+1)2^{l-1}$ og $(l-\mathsf{r})$ lineært uavhengige kodeord med vekt $t\,2^{l-1}$.

Då vi fann den øvre skranken, føresette vi at C_r inneheld kodeord som har alle sine '1'-posisjonar innafor dei same $(t+1)$ blokkene. I dette tilfellet må W_l finnast. Generatormatrisa for C_r var då arrangert slik at det var '1'-posisjonar i til saman $(t+1)$ blokker. Då har alle kodeorda i C_r vekt $\le (t+1)2^{l-1}$.

Allment har vi at om generatormatrisa til C_{tl} har '1'-posisjonar i t' blokker vil C_{tl} innehalda kodeord med vekt $\le t'\,2^{l-1}$.

Lat $tl+1 \le r \le (t+1)l$ og $\rho = r - tl$ som over. Lat $t' > t$ og $\rho' < \rho$. Vi går no ut frå at generatormatrisa til C_r har '1'-posisjonar i $(t'+1)$ blokker, og at det i C_r berre finns ρ' lineært uavhengige kodeord med vekt $(t+1)2^{l-1}$. Dette tilseier då at det må finnast $(\rho - \rho')$ uavhengige kodeord med vekt $> (t+1)2^{l-1}$. Likeeins må det finnast $l - ((\rho - \rho') + \rho') = (l-\rho)$ uavhengige kodeord med vekt $\ge t\,2^{l-1}$.

Dette må medføra at C_r inneheld eit l-dimensjonalt underrom, W'_l, generert av ρ kodeord med vekt $\ge (t+1)2^{l-1}$ og $(l-\rho)$ kodeord med vekt $\ge t\,2^{l-1}$. Då vert

$$|X(W'_l)| \ge |X(W_l)| .$$

Når $w_i = t\,2^{l-1}$ og $w_{i+1} = (t+1)2^{l-1}$, vil støttevekta til W_l ifølgje avsnitt 5.4 vera gitt av

$$|X(W_l)| = t(2^l - 1) + (2^l - 2^{l-\rho}).$$

$|X(W_l)|$ vil i intervallet $tl+1 \le r \le (t+1)l$ vera ein nedre skranke for $d_{tl+\rho} = d_r$.

Lat $t = \lfloor r/l \rfloor$. Vektene $w_t = t\,2^{l-1}$, $1 \le t \le k/l$.
Den nedre skranken for d_r, om $l+1 \le r \le k$, vert

$$\begin{aligned} d_r &\ge |X(W_l)| \\ &= t(2^l - 1) + (2^l - 2^{l-(\rho-l)}) \\ &= t(2^l - 1) + (2^l - 2^{(t+1)l-r}) = d_r^{'\min} = d_r^{'\max}. \end{aligned}$$

5.7 $k/l = n_1 - 1$

Teorem 5.7.1. Lat C vera ein irredusibel $(n_1 (q^l-1), k)$-kode over $GF(q)$. Dersom $k/l = n_1 - 1$, vil vektoppteljaren vera

$$A(z) = \sum_{i=0}^{n_1} \binom{n_1}{i} \frac{(q^l-1)^i + (q^l-1)(-1)^i}{q^l} z^{q^{l-1}(q-1)i} .$$

Bevis. Sidan $k/l = n_1 - 1$, vil C^* vera ein lineær (n_1, n_1-1)- kode. I følgje Lemma 5.2.4 må paritets-sjekkpolynomet $h(x)$ til C^{*+} dela $x^{n_1} - \beta^{n_1}$. Vi har

$$x^{n_1} - \beta^{n_1} = \prod_{i=0}^{n_1-1} (x - \alpha^i \beta),$$ der α er ei primitiv n_1'te einingsrot. Sidan $h(x)$ har grad $n_1 - 1$, får vi

$h(x) = (x^{n_1} - \beta^{n_1})/(x - \alpha^a\beta)$ for ein a slik at $\alpha^a\beta \in GF(2^l)$.
Difor vert

$$h(x) = (x^{n_1} - \delta^{n_1})/(x - \delta) = x^{n_1-1} + \delta x^{n_1-2} + \ldots + \delta^{n_1-1} \text{ for } \delta = \alpha^a\beta.$$

Sidan C^* utgjer det første n_1 - tuppelet av kodeorda i C^{*+}, som har $h(x)$ som paritetssjekkpolynom, må C^* vera ein (n_1, n_1-1)-kode.

Den duale koden, $C^{*\perp}$, til C^* er ein $(n_1, 1)$-kode, og $(\delta^{n_1-1}, ..., \delta, 1)$ er eit kodeord i den duale koden. Difor vert

$$C^{*\perp} = (\gamma(\delta^{n_1-1}, ..., \delta, 1) \mid \gamma \in GF(2^l)).$$

Lat $B^*(z)$ vera vektoppteljaren til $C^{*\perp}$. Vi får $B^*(z) = 1 + (q^l - 1)z^{n_1}$. Ved hjelp av MacWilliams-identiteten og Lemma 5.2.5 får vi det ønska resultatet.

[6]

Teorem 5.7.1 syner at C har n_1-1 ulike vekter, $w \neq 0$, sidan ingen kodeord har vekt $(q^{l-1})(q-1)$. Vidare er vektene uavhengige av n_1.

Frå Lemma 5.2.5 og Teorem 5.7.1 ser vi at C^* har minimumsvekt 2. Eit kodeord med minumumsvekt vil innehalda 2 komponentar, $c^*_{j_1}(a)$, der $Tr_l^k(a\beta^{j_1}) \neq 0$. Eit kodeord med vekt $t2^{l-1}$ vil ha t slike komponentar, jfr. avsnitt 5.2. Eit kodeord med minimumsvekt i C^* tilsvarer då eit kodeord i C der *to* blokker, $(c_{j_1 n_2}, ..., c_{(j_1+1)n_2-1}) \neq$ "0,...,0" for *to* ulike verdiar for j_1.

Vi går frå no av ut frå at $q = 2$. Vektene vert $w_t = (t+1)(2^{l-1})$, $1 \leq t \leq n_1 - 1$.

Merk. C^* er ein MDS-kode sidan $k = n - d + 1 = n_1 - 2 + 1 = n_1 - 1$.

Teorem 5.7.2. Vekthierarkiet til C er gitt av

$$d_r = 2(2^l - 2^{l-r}), \text{ om } 1 \leq r \leq l,$$
$$= (t+1)(2^l - 1) + (2^l - 2^{(t+1)l-r}), \text{ om } l+1 \leq r \leq k,\ t = \lfloor r/l \rfloor.$$

Bevis.

1 ≤ r ≤ l.

Vi har frå Teorem 5.3.1, Korollar 5.3.2 og Teorem 5.7.1 at

$$d_r = \frac{1}{2^{r-1}} \sum_{\underline{c} \in C_r} w_1 = 2 \sum_{i=0}^{r-1} \left\lceil \frac{2^{l-1}}{2^i} \right\rceil = 2(2^l - 2^{l-r}).$$

l+1 ≤ r ≤ k.

Vi finn først ein øvre skranke etter metoden skissert i avsnitt 5.4, og konstruerer følgjande generatormatrise for C.

Døme 5.7.3. $n_1 = 5$, $l = 3$, $w_1 = 2(2^{l-1})$.

$\underline{G}$

$\leftarrow n_2 \rightarrow$	$\leftarrow n_2 \rightarrow$	$\leftarrow n_2 \rightarrow$	$\leftarrow n_2 \rightarrow$	$\leftarrow n_2 \rightarrow$	
1111000	1111000	0000000	0000000	0000000	
1100110	1100110	0000000	0000000	0000000	
1010101	1010101	0000000	0000000	0000000	l kodeord. Kodeorda i C_l har vekt w_1.
1111000	1111000	1111000	0000000	0000000	
1100110	1100110	1100110	0000000	0000000	
1010101	1010101	1010101	0000000	0000000	$2l$ kodeord. Kodeorda i C_{2l} har vekt w_1 og w_2
1111000	1111000	1111000	1111000	0000000	
1100110	1100110	1100110	1100110	0000000	
1010101	1010101	1010101	1010101	0000000	$3l$ kodeord. Kodeorda i C_{3l} har vekt w_1, w_2 og w_3.
1111000	1111000	1111000	1111000	1111000	
1100110	1100110	1100110	1100110	1100110	
1010101	1010101	1010101	1010101	1010101	$4l$ kodeord. Kodeorda i C_{4l} har vekt w_1, w_2, w_3 og w_4.

Fig. 5.7.1. $C = [\,35, 12, 8\,]$. Generatormatrisa er arrangert slik at dei r første kodeorda genererer eit underrom som held den øvre skranken for d_r.

Lat $0 \le i < k/l$. For kvart intervall, $il + 1 \le r \le (i+1)l$, skal vi velja kodeord $c\,(a)_r$ slik at $w(c\,(a)_r) = w_{i+1}$ og $c\,(a)_r \in S_l(a)$. Sidan koden er syklisk og vektene er påfølgjande multippel av 2^{l-1}, vil det vera muleg å velja kodeorda slik at alle 0-komponentane til $c(a)_r$ ligg innafor 0-søylene i C^*_{il}. Dette vil medføra ei generatormatrise for C^S.

Vi får då følgjande øvre øvre skranke for d_r i dette intervallet.

$$d_r \le d_{il} + d_{\mathsf{r}}\,(C^S), \text{ der } \mathsf{r} = r - il.$$
$$= (i+1)(2^l - 1) + (2^l - 2^{(i+1)l - r}).$$

Lat $t = \lfloor r / l \rfloor$. Den øvre skranken for d_r ,om $l + 1 \le r \le k$, vert

$$d_r \le (t+1)(2^l - 1) + (2^l - 2^{(t+1)l - r}) = d_r^{'\max}.$$

Lat $1 \le \mathrm{t} < k/l$. Lat $tl + 1 \le r \le (t+1)l$ og $\mathsf{r} = r - tl$. Med same argumentasjon som for koden der $k/l = n_1$, kan det påvisast at C_r inneheld eit l-dimensjonalt underrom, W'_l, generert av r lineært uavhnegige kodeord med vekt $\ge (t+2)2^{l-1}$ og $(l - \mathsf{r})$ kodeord med vekt $\ge (t+1)2^{l-1}$. Då vert

$$|X(W'_l)| \ge |X(W_l)|.$$

Når $w_i = (t+1)\,2^{l-1}$ og $w_{i+1} = (\mathrm{t}+2)2^{\mathrm{l}-1}$, vil støttevekta til W_l ifølgje avsnitt 5.4 vera gitt av

$$|X(W_l)| = (t+1)(2^l - 1) + (2^l - 2^{l - \mathrm{r}}).$$

$|X(W_l)|$ vil i intervallet $tl + 1 \le r \le (t+1)l$ vera ein nedre skranke for $d_{tl+\mathsf{r}} = d_r$.

Lat $t = \lfloor r / l \rfloor$. Vektene $w_t = (t+1)2^{l-1}$, $1 \le t \le k/l$.
Den nedre skranken for d_r, om $l + 1 \le r \le k$, vert

$$d_r \ge |X(W_l)|$$
$$= (t+1)(2^l - 1) + (2^l - 2^{l-(r-l)})$$
$$= (t+1)(2^l - 1) + (2^l - 2^{(t+1)l-r}) = d_r^{'\min} = d_r^{'\max}.$$

5.8 Samandrag

Vi har funne vekthierkiet til kodane ved å analysera vektdistribusjonen. Vi har først og fremst utnytta at

i) kodeorda har k/l ulike vekter,
ii) det finns l-dimensjonale underrom der alle kodeord har same vekt,
iii) dei ulike vektene for kodeorda er påfølgjande multippel av 2^{l-1},
iv) rekkjevektorane i matrisa $(u_{j_1 j_2})$ inngår i $[2^l-1, l, 2^{l-1}]$ Simplex-kodar.

Resultata gjeld for $q = 2$, men kan truleg enkelt generaliserast for alle q.

For alle kodeklassane har vi sett at $D_1 \subseteq D_2 \subseteq ... \subseteq D_k$.. Dette inneber at dei tilfredsstiller kjedevilkåret.

Vi har vidare sett at C^* er ein MDS-kode for alle kodeklassane. Vekthierarkiet til C^* er gitt av

$d_r = n - k + r$, jfr. avsnitt 3.2.

Tabellane i Vedlegg VI syner nokre numeriske resultat for kodane.

Kapittel 6

Samandrag og konklusjon

Vi har studert vekthierarkiet til undergrupper av to ulike klassar av binære, lineære, sykliske kodar.

Kodane i klassen der $h(x)$ er produktet av to primitive polynom av grad m, har dimensjon $2m = k$. Undergruppa vi studerte kan karakteriserast ved

$$h(x) = m_1(x)\, m_s(x).$$

Vi tok føre oss to ulike verdiar for s og fann d_r for $1 \le r \le k/4$.

Lat $a, b \in GF(2^{k/2})$, $\delta \in GF(2^{k/4})$ og $c(a,b)$ vera eit kodeord i C. For beggje desse 4-vektskodane fann vi at

$$w(c(a,b)) = w(c(\delta^i a, \delta^j b)) = w_i,\ 1 \le i \le 4.$$

Det finns difor $k/4$-dimensjonale underrom der alle kodeord har minimumsvekt. d_r er difor gitt av

$$d_r = g(r,d), \text{ om } 1 \le r \le k/4.$$

Det er vidare funne gode øvre skrankar for d_r, om $k/4+1 \le r \le k$. Det har ikkje lukkast å finna $d_{k/4+1}$. Dette er det viktigaste uløyste problemet i oppgåva. Ein del grunnleggjande resultat for eit slikt prov vart lagt fram i avsnitta 4.5.2 og 4.6.2. Ytterlegare delresultat som kan vera nyttige, er lagt fram i vedlegga II og III.

For dei tre undergruppene av dei irredusible sykliske kodane fann vi heile vekthierarkiet. Sidan $h(x)$ her har grad $k = \dim(C)$, var dette ei enklare oppgåve.

Lat $a \in GF(2^k)$, $\delta \in GF(2^l)$ og $c(a)$ vera eit kodeord i C. Vi fann her at

$$w(c(a)) = w(c(\delta a)) = w_i,\ 1 \le i \le k/l.$$

Det finns dermed l-dimensjonale underrom der alle kodeord har same vekt. Dette var kjerna i provet for heile vekthierarkiet.

Lat C^* vera ein lineær, syklisk (n, k)- kode over $GF(2^l)$. Alle kodane vi har studert kan sjåast som ein binær ($n(2^l-1)$, kl)-"trace-kode", C, til C^* . Ein kan dela kodeorda i C opp i n blokker av lengd (2^l-1) slik at ein blokk i kodeorda i C tilsvarer ein komponent i tilhøyrande kodeord i C^*. Ein r-dimensjonal blokk i ei generatormatrise for C tilsvarer då ei r-dimensjonal søyle i generatormatrisa for C^*.

Vektene i C er multippel av 2^{l-1} sidan kvar blokk har vekt 0 eller 2^{l-1}. Dersom her for alle vekter finns l-dimensjonale underrom av kodeord med same vekt, vil kvar blokk i generatormatrisa for C_r høyra til ein $[2^l-1, l, 2^{l-1}]$ Simplex-kode, C^S.

På grunnlag av dette er det utvikla ein metode der vi konstruerer ei generatormatrise for C slik at støttevekta for eit r-dimensjonalt underrom, er gitt av

$$|X(C_{il})| + t(d_{\mathsf{r}}(C^S)), \text{ der } \mathsf{r} = r - il,\ 0 \le i < k/l.$$

$|X(C_{il})|$ vert eit multippel av $d_l(C^S)$. Variabelen t avheng av differansen mellom vektene i koden.

Å finna klassen av kodar der vekthierarkiet har ein slik eigenskap, kunne vera ei interessant vidareføring av denne oppgåva.

Sjølv om dei øvre skrankane for Niho-koden der $s = (2^l-1)(2^{2l}+1) + 2$ også har tilsvarande eigenskap, framstår resultata likevel som meir ustrukturerte enn dei vi fann for dei andre kodane. Årsaka til dette er først og fremst at koden ikkje held kjedevilkåret. Denne koden skil seg ut ved at C^* ikkje er ein MDS-kode, og at vektene i C ikkje er påfølgjande multippel av 2^{l-1}. Det kunne også vera interessant å sjå om desse faktorane har noko å seia for kor vidt ein kode tilfredsstiller kjedevilkåret.

Det er i arbeidet med oppgåva utført ei rekkje søk etter underrom med minst muleg støttevekt. Programmet genererer underrom med utgangspunkt miminimumvektskodeorda. Eit fellestrekk ved dei beste underromma som er funne på denne måten, er at generatormatrisa kan organiserast etter metoden skissert ovanfor for $r > l$. For $r \le l$ varierer løysingane.

For dei irredusible kodane vart det også utarbeidd ein metode som gir ein nedre skranke for d_r. For alle desse kodane var det samsvar mellom øvre og nedre skranke.

Vedlegg I

Notasjonar og ordliste

Notasjonar

Avsnittet gir ein oversikt over notasjonane som er brukt i oppgåva. Formelle definisjonar for omgrep hovudsakleg vedrørande avstand, vekt og vekthierarki er gitt i avsnitt 3.1. Andre definisjonar kan ein finna i allmene lærebøker i kodeteori og talteori.

$A(z)$	Vektoppteljaren til ein kode. A_i gir talet på kodeord med vekt i i koden. I oppgåva vert vektoppteljar og vektdistribusjon brukt synonymt.
$\{c_j\}$	Ein sekvens generert av eit polynom.
C	Ein kode. Om ikkje anna er sagt, vil C i denne oppgåva vera ein [n, k, d]-kode.
C_r	Eit vilkårleg r-dimensjonalt underrom i C.
$C_r \subseteq C$	C_r er eit underrom i C.
$C^{\perp}$	Den duale koden til C.
$\underline{c}$	Eit kodeord i koden C slik at $\underline{c} = (c_0, c_1, ..., c_{n-1})$, der c_j gir koordinatposisjonane i kodeordet. Sjå også $c(a)$.
$\underline{c}_i$	Det i'te kodeordet i koden C.
c_j	Den j'te koordinatposisjonen i kodeordet $\underline{c}$.
$c(a)$	Eit kodeord i koden, C, over GF(q). Kodeorda i ein Simplex-kode kan genererast av tracefunksjonen s.a dei vert på forma $c(a) = (Tr_e^m(a), Tr_e^m(a\alpha), ..., Tr_e^m(a\alpha^{n-1}))$, der α^i er rot i $h(x)$ og $a \in GF(q^m)$. Ettersom ein liknande teknikk vert brukt for alle kodar som vert handsama i oppgåva, vert $\underline{c}$ og $c(a)$ brukt synonymt om kodeord.
$c(a)_i$	Det i'te kodeordet i koden C. $c(a)_i = \underline{c}_i$.
$c_j(a)$	Den j'te koordinatposisjonen i kodeordet $c(a)$. $c_j(a) = Tr_e^m(a\alpha^j) = c_j$.
$\Delta_s(y)$	Krysskorrelasjonsfunksjonen mellom to maksimale lineære rekursive sekvensar.
D_r	Eit r-dimensjonalt underrom i koden C slik at $\lvert X(D)\rvert = d_r(C)$ for gitt r.
d	Minimumsavstanden til koden.

$d(\underline{x}, \underline{y})$ Hammingavstanden mellom to vektorar,
$\underline{x} = (x_0, x_1,..., x_{n-1})$ og $\underline{y} = (y_0, y_1,..., y_{n-1})$.

$d_r(C)$ Den r'te generaliserte Hammingvekta til koden C. Vekthierarkiet til koden er gitt ved settet av generaliserte Hammingvekter, $\{d_1, d_2,..., d_k\}$. I oppgåva vert d_r og $d_r(C)$ brukt synonymt. For å uttykkja den r'te generaliserte Hammingvekta til eit vilkårleg underrom, U, i C nyttast $d_r(U)$.

$d_r^{'max}(C)$ øvre skranke for $d_r(C)$

$d_r^{'min}(C)$ nedre skranke for $d_r(C)$

F_q Ein endeleg kropp av orden q, der q er ein potens av eit primtal.

F_q^n Det n-dimensjonale vektorrommet over F_q.

F_q^* Ikkje-null-elementa i F_q, dvs $F_q - \{0\}$.

$F_q[x]$ Ringen av polynom i x med koeffisientar i F_q.

$\underline{G}$ Generatormatrise.

$GF(q)$ Galois-kropp av orden q.

$g(k,d)$ Griesmerskranken for ein kode med dimensjon k og minimumsavstand d. I oppgåva vert også $g(r, d)$ nytta dersom eit r-dimensjonalt underrom i C held Griesmerskranken, dvs dersom $d_r(C)$ = Griesmerskranken for gitt r.

$g(x)$ Generatorpolynom..

$\underline{H}$ Paritetssjekkmatrise.

$h(x)$ Paritetssjekkpolynom

$m_i(x)$ Minimumspolynomet til α^i.

(n, k)- kode. Gir parametrane til ein kode; lengde n og dimensjon k.

$[n, k, d]$-kode. Gir parametrane til ein lineær kode; lengde n, dimensjon k og minimumsavstand d.

$Tr_e^m(x)$ Tracefunksjonen.

$w(\underline{x})$ Hammingvekta til vektoren $\underline{x}$.

w_t den t'te minste Hammingvekta til eit kodeord i koden.

$X(D)$ Støtta til D er settet av koordinatposisjonar der ikkje alle kodeord i D $\subseteq C$ er "0".

$\underline{x}$ Ein vektor, $\underline{x} = (x_0, x_1,..., x_{n-1})$

Ordliste

Avsnittet syner til notasjonar og/eller definisjonar av ein del ord og uttrykk som er brukt i oppgåva.

Dual kode	$C^\perp$	definert i avsnitt 3.1
Dualitetsteoremet		definert i avsnitt 3.3
Einingsrot		root of unity
Generaliserte Griesmer-skranken		definert i avsnitt 3.2
Generaliserte Singleton-skranken		definert i avsnitt 3.2
Generatormatrise	$\underline{G}$	
Generatorpolynom	$g(x)$	

Griesmer-skranken	$g(k,d)$	definert i avsnitt 3.2
Hammingavstand	$d(\underline{x}, \underline{y})$	definert i avsnitt 3.1
Hammingvekt	$w(\underline{x})$	definert i avsnitt 3.1
Kjedevilkåret		definert i avsnitt 3.1
Krysskorrelasjonsfunksjonen	$\mathsf{D}_s(y)$	definert i avsnitt 3.1
MacWilliams-identiteten		definert i avsnitt 3.3
Minimumsdistanse	d	definert i avsnitt 3.1
Minimumspolynom	$m_i(x)$	definert i avsnitt 3.1
Maksimumsvekt		definert i avsnitt 3.1
Minimumsvekt		definert i avsnitt 3.1
r'te generaliserte Hammingvekt	$d_r(C)$	definert i avsnitt 3.1
Singleton-skranken		definert i avsnitt 3.2
Paritetssjekkmatrise	$\underline{H}$	
Paritetssjekkpolynom	$h(x)$	
Sekvens	$\{c_j\}$	
Støtte	$X(D)$	definert i avsnitt 3.1
Støttevekt	$\lvert X(D)\rvert$	definert i avsnitt 3.1
Tracefunksjonen	$Tr_e^m(x)$	definert i avsnitt 3.1
Vektdistribusjon		(jfr. vektoppteljar)
Vekthierarki	$\{d_1, d_2,..., d_k\}$	definert i avsnitt 3.1
Vektoppteljar	$A(z)$	definert i avsnitt 3.1

Vedlegg II

Resultat vedrørande $d_{k/4+1}$ for Niho-koden der $s = 2^{l+1} - 1$

Lat $b \in B$. Vi skal i dette vedlegget sjå nærare på tilfellet $b = a/b^{2^l}$.

Utgangspunktet er likningane (4.5.5) og (4.5.6)

$$b^{2^l+1} = 1.$$

og

$$b^{2^l} b^3 + ab^2 + a^{2^l} b + b = 0,\ b \neq 0.$$

Lemma 1. Lat $f \in F_{2^l}^*$.

Dersom $Tr_1^l(1/b^{2^l+1} f^2) = 0$, vil likninga gje eit kodeord med vekt w_3.

Dersom $Tr_1^l(1/b^{2^l+1} f^2) = 1$, vil likninga gje eit kodeord med vekt w_2 eller w_1.

Bevis. Vi skriv likning (4.5.6) som

$$b^{2^l} x^3 + ax^2 + a^{2^l} x + b = 0.$$

Vi ser så på likninga

$$(b^{2^l} x + b^{2^l} b)(x^2 + ux + b/b^{2^l} b) = 0$$

$$\Rightarrow b^{2^l} x^3 + (b^{2^l} b + ub^{2^l})x^2 + (b^{2^l} b/b^{2^l} b + b^{2^l} bu)x + b = 0$$

$$\Rightarrow b^{2^l} x^3 + b^{2^l}(b + u)x^2 + (bb^{-1} + b^{2^l} bu)x + b = 0.$$

Vi får

$$(b^{2^l}(b + u))^{2^l} = bb^{-1} + b^{2^l} bu$$

$$\Rightarrow bb^{-1} + bu^{2^l} = bb^{-1} + b^{2^l} bu$$

$$\Rightarrow bu^{2^l} = b^{2^l} bu$$

$$\Rightarrow u^{2^l-1} = b^{2^l-1} b$$

$$\Rightarrow u = \sqrt[2^l-1]{b^{2^l-1} b} = b^{2^{l-1}} bf.$$

Vi ser så på tilfellet der $x^2 + ux + b/b^{2^l} b = 0$. Lat $x = uz$.

$$(uz)^2 + uuz + b/b^{2^l} b = 0$$

$$\Rightarrow z^2 + z + b^{1-2^l}/bu^2 = 0.$$

Vi set inn for u og får

$$b^{1-2^l} / \mathrm{b} u^2 = b^{1-2^l} / \mathrm{b} b^{2^l} b^2 f^2 = b^{-1-2^l} / f^2 = 1/b^{2^l+1} f^2 \in F_{2^l}^* .$$

$$\Rightarrow z^2 + z + 1/b^{2^l+1} f^2 = 0$$

$$\Rightarrow \sum_{i=0}^{l-1} (z^2 + z)^{2^i} = \sum_{i=0}^{l-1} (1/b^{2^l+1} f^2)^{2^i}$$

$$\Rightarrow z^{2^l} + z = Tr_1^l (1/b^{2^l+1} f^2) .$$

Vi ser på dei to ulike tilfella for $Tr_1^l (1/b^{2^l+1} f^2)$.

Dersom $Tr_1^l (1/b^{2^l+1} f^2) = 0$, får vi

$$z^{2^l} + z = (u^{-1}x)^{2^l} + u^{-1}x = Tr_1^l (1/b^{2^l+1} f^2) = 0$$

$$\Rightarrow x^{2^l} = u^{2^l-1} x$$

$$\Rightarrow x^{2^l+1} = 1 \Leftrightarrow u^{2^l-1} x^2 = 1$$

$$\Leftrightarrow x^2 = 1/u^{2^l-1} = 1/b^{2^l-1} \mathrm{b}$$

Dette gir

$$x^2 + ux + b/b^{2^l} \mathrm{b} = 1/b^{2^l-1} \mathrm{b} + ux + b/b^{2^l} \mathrm{b}$$

$$= 1/b^{2^l-1} \mathrm{b} + ux + 1/b^{2^l-1} \mathrm{b} = ux$$

Sidan $x^2 + ux + b/b^{2^l} \mathrm{b} = 0$ og $ux \neq 0$, følgjer det at $x^2 + ux + b/b^{2^l} \mathrm{b} = 0$ ikkje har noko løysing i $F_{2^{2l}}$. Dette inneber at likning (4.5.6) har *ei* løysing når $Tr_1^l (1/b^{2^l+1} f^2) = 0$ og vil medføra eit kodeord med vekt = w_3. For uttrykket a/b^{2^l} får vi

$$a/b^{2^l} = b^{2^l} (\mathrm{b} + u)/b^{2^l} = \mathrm{b} + u = \mathrm{b} + \mathrm{b}^{2^{l-1}} bf.$$

Dersom $Tr_1^l (1/b^{2^l+1} f^2) = 1$, får vi

$$z^{2^l} + z = (u^{-1}x)^{2^l} + u^{-1}x = Tr_1^l (1/b^{2^l+1} f^2) = 1$$

$$\Rightarrow x^{2^l} = u^{2^l-1} x + u^{2^l} .$$

Likninga $x^2 + ux + b/b^{2^l} \mathrm{b} = 0$ har to løysingar i $F_{2^{2l}}$ sidan

$$Tr_1^{2l} ((b/b^{2^l} \mathrm{b})/u^2) = Tr_1^{2l} (1/b^{2^l+1} f^2) = 0.$$

Dette inneber at likning (4.5.6) har tre løysingar når $Tr_1^l (1/b^{2^l+1} f^2) = 1$, men då løysingane kan ha multiplisitet 2, vil likninga føra til eit kodeord med vekt w_1 eller vekt w_2.

Vi sjekkar til slutt om desse løysingane tilfredsstiller $x^{2^l+1} = 1$.

$$x^{2^l+1} = 1 \Leftrightarrow u^{2^l-1}x^2 + u^{2^l}x = 1$$
$$\Leftrightarrow x^2 + ux + 1/u^{2^l-1} = 0$$
$$\Leftrightarrow x^2 + ux + 1/b^{2^l-1}\beta = x^2 + ux + b/b^{2^l}\beta = 0.$$

Korollar 2. Vi har frå Lemma 1 at

$$a/b^{2^l} = \beta + u = \beta + \beta^{2^{l-1}} bf .$$

og

$$x^2 + ux + b/b^{2^l}\beta = 0.$$

Kodeord med vekt = w_1

Følgjande gjeld

$$(x - \beta_1)(x - \beta_2)(x - \beta_3) = 0$$
$$\Rightarrow (x - \beta_1)(x^2 + (\beta_2 + \beta_3)x + \beta_2\beta_3) = 0$$

Vi set $u = \beta_2 + \beta_3$, og $b/b^{2^l}\beta = \beta_2\beta_3 = b^{1-2^l}/\beta$

Sidan $\beta_1\beta_2\beta_3 = b^{1-2^l}$, får vi no

$$b/b^{2^l}\beta_1 = b^{2^l}/\beta_1 = \beta_1\beta_2\beta_3 /\beta_1 = \beta_2\beta_3,$$

og

$$a/b^{2^l} = \beta + u = \beta_1 + u = \beta_1 + \beta_2 + \beta_3 .$$

Kodeord med vekt = w_2

Vi set $\beta' = \beta_2 = \beta_3$, då denne løysinga har multiplisitet 2. Vi får då

$$a/b^{2^l} = \beta + u = \beta_1 + u = \beta_1 + \beta_2 + \beta_3. = \beta_1 + \beta' + \beta' = \beta_1$$
$$\Rightarrow (\beta')^2 = \beta_1\beta_2\beta_3 /\beta_1 = b^{1-2^l}/a / b^{2^l} = b/a.$$
$$\Rightarrow \beta' = \sqrt{b/a} .$$

Løysinga, β' , med multiplisitet 2, finn vi slik

$$a/b^{2^l} = \beta_1 \Rightarrow (a/b^{2^l})^{2^l+1} = 1$$
$$\Rightarrow a^{2^l+1} / b^{2^{2l}+2^l} = 1$$
$$\Rightarrow a^{2^l+1} / b^{2^l+1} = 1$$
$$\Rightarrow a^{2^l+1} / b^{2^l} = b$$
$$\Rightarrow b/a = a^{2^l} / b^{2^l}$$
$$\Rightarrow \sqrt{b/a} = a^{2^{l-1}} / b^{2^{l-1}}$$, jfr også Lemma 4.5.4.

Kodeord med vekt = w_3

Vi fann i Lemma 1 at likninga $x^2 + ux + b/b^{2^l} \beta = 0$ ikkje har løysing i $F_{2^{2l}}$.

Lat β_1 vera einaste rot i likningane (4.5.5) og (4.5.6) for kodeorda. Dersom β_1 har multiplisitet 3, kan vi setja $\beta' = \beta_1 = \beta_2 = \beta_3$. Vi får då

$$a/b^{2^l} = \beta + u = \beta_1 + u = \beta_1 + \beta_2 + \beta_3 = \beta' + \beta' + \beta' = \beta'$$
$$= a^{2^{l-1}} / b^{2^{l-1}}$$, jfr også Lemma 4.5.4.

Dersom β_1 ikkje har har multiplisitet 3, må likevel følgjande gjelda

$$a/b^{2^l} = \beta + u = \beta_1 + u = \beta_1 + \beta_2 + \beta_3 .$$

No har vi at $\beta_1 \neq \beta_2 \neq \beta_3$. $\beta_1, \beta_2, \beta_3 \in B$ og er røter i likninga 4.5.5. Men berre β_1 er rot i likningsset*tet* (4.5.5) og (4.5.6).

Vedlegg III

Resultat vedrørande $d_{k/4+1}$ for Niho-koden der $s = (2^l - 1)(2^{2l} + 1) + 2$

Vi skal i dette vedlegget sjå nærare på eigenskapar ved kodeorda i C. Utgangspunkt er likningane (4.6.5) og (4.6.6)

$$\beta^{2^{2l}+1} = 1.$$

og

$$b^{2^{l-1}} \beta^{2^l} + a\beta + b^{2^{-l-1}} \beta^{-2^l} + a^{2^{2l}} \beta^{-1} = 0,\ b \neq 0.$$

Likning (4.6.6) kan skrivast

$$Tr_{2l}^{4l} (a\beta + b^{2^{l-1}} \beta^{2^l}) = 0.$$

β vil då vera ei rot i likninga $\Leftrightarrow (a\beta + b^{2^{l-1}} \beta^{2^l}) \in GF(2^{2l})$, jfr Lemma 4.6.8.

I avsnitt 4.6.2 fann vi at dersom $(a/\sqrt[s]{b})^{2^l+1} = 1$,

i) likningane (4.6.5) og (4.6.6) har ei løysing, β_0, slik at $\sqrt{b}\beta_0 \in GF(2^{2l})$.

ii) $b = a^2\gamma^i$.

Då vert

$$\sqrt{b}\,\beta_0 = a\sqrt{\gamma^i}\,\beta_0$$
$$\Rightarrow a\sqrt{\gamma^i}\,\beta_0 \in GF(2^{2l}).$$
$$\Rightarrow a\beta_0 \in GF(2^{2l}), \text{ sidan } \sqrt{\gamma^i} \in GF(2^{2l}).$$

Lemma 1. Lat $c^*(a,b)$ vera eit kodeord i C^*. Lat $(a/\sqrt[s]{b})^{2^l+1} = 1$. Lat $\beta_0 = \beta^e$. Då vil posisjonane i kodeordet vera "symmetriske" rundt $f_{ab}(\beta^e)$, slik at

$$f_{ab}(\beta^{e+i}) = f_{ab}(\beta^{e-i}).$$

Bevis. Lat $0 \le j \le 2^{2l}$. Komponentane i $c^*(a,b)$ er gitt av $f_{ab}(\beta^j)$

$$c^*_j(a,b) = Tr_{2l}^{4l} (a\beta^j + b^{2^{l-1}} \beta^{j2^l}),$$

og

$$f_{ab}(\beta^e) = Tr_{2l}^{4l} (a\beta^e + b^{2^{l-1}} \beta^{e2^l}) = 0.$$

Vi får då

$$a\beta^e \in GF(2^{2l})$$
$$\Rightarrow b^{2^{l-1}} \beta^{e2^l} \in GF(2^{2l}).$$

Lat $a\beta^e = \alpha^j$ og $b^{2^{l-1}} \beta^{e2^l} = \alpha^k$, $0 \le e \le 2^{2l}$, $0 \le j, k \le 2^{2l}-2$, $0 \le i \le 2^{2l}-1$.
Vi får då

$$a\beta^e = \alpha^j \Rightarrow a\beta^{e+i} = \alpha^{j+i(2^{2l}-1)} \text{ og } a\beta^{e-i} = \alpha^{j-i(2^{2l}-1)},$$

og

$$b^{2^{l-1}} \beta^{e2^l} = \alpha^k \Rightarrow b^{2^{l-1}} \beta^{(e+k)2^l} = \alpha^{k+i(2^{2l}-1)} \text{ og } b^{2^{l-1}} \beta^{(e-k)2^l} = \alpha^{k-i(2^{2l}-1)}.$$

$f_{ab}(\beta^e)$ kan også skrivast som

$$f_{ab}(\beta^e) = Tr_{2l}^{4l}(a\beta^e) + Tr_{2l}^{4l}(b^{2^{l-1}} \beta^{e2^l}) = 0.$$

Då vert

$$f_{ab}(\beta^{e+i}) = Tr_{2l}^{4l}(\alpha^{j+i(2^{2l}-1)}) + Tr_{2l}^{4l}(\alpha^{k+i(2^{2l}-1)}),$$

og

$$f_{ab}(\beta^{e-i}) = Tr_{2l}^{4l}(\alpha^{j-i(2^{2l}-1)}) + Tr_{2l}^{4l}(\alpha^{k-i(2^{2l}-1)}).$$

Ettersom $(\alpha^j)^{2^{2l}} = \alpha^j$ og $(\alpha^{i(2^{2l}-1)})^{2^{2l}} = \alpha^{i(2^{2l}-1)}$, får vi

$$Tr_{2l}^{4l}(\alpha^{j+i(2^{2l}-1)}) = Tr_{2l}^{4l}(\alpha^{j-i(2^{2l}-1)}),$$

og

$$Tr_{2l}^{4l}(\alpha^{k+i(2^{2l}-1)}) = Tr_{2l}^{4l}(\alpha^{k-i(2^{2l}-1)}).$$

Dette må då medføra at $f_{ab}(\beta^{e+i}) = f_{ab}(\beta^{e-i})$.

Lemma 2. Lat $c^*(a,b)$ vera eit kodeord i C^*. Lat $(a/\sqrt[3]{b})^{2^l+1} = 1$. Då vil komponentane i kodeordet ha høgst 2^l ulike vediar.

Bevis. Lat $0 \le j \le 2^{2l}$. Komponentane i $c^*(a,b)$ er gitt av $f_{ab}(\beta^j)$

$$c^*_j(a,b) = Tr_{2l}^{4l}(a\beta^j + b^{2^{l-1}} \beta^{j2^l}).$$

Sidan $b = a^2\gamma^i$, kan likning (4.6.6) skrivast

$$(a^2)^{2^{l-1}} \gamma^{i2^{l-1}} \beta^{2^l} + a\beta + (a^2)^{2^{-l-1}} \gamma^{i2^{-l-1}} \beta^{-2^l} + a^{2^{2l}} \beta^{-1} = 0$$
$$\Rightarrow \gamma^{i2^{l-1}} (a\beta)^{2^l} + a\beta + \gamma^{i2^{-l-1}} a^{2^{-l}} \beta^{-2^l} + a^{2^{2l}} \beta^{-1} = 0.$$

Sidan $\gamma^i \in GF(2^{2l})$, får vi

$$\gamma^{i2^{-l-1}} = \gamma^{i2^{3l-1}} = \gamma^{i2^{l-1}}.$$

Likninga kan då vidare skrivast

$$\alpha\beta + \alpha^{2^{2l}}\beta^{-1} + \gamma^{i2^{l-1}}(\alpha^{2^l}\beta^{2^l} + \alpha^{2^{-l}}\beta^{-2^l}) = 0.$$

Vi får då

$$(\alpha\beta + \alpha^{2^{2l}}\beta^{-1}) = Tr_{2l}^{4l}(\alpha\beta).$$

og

$$(\alpha^{2^l}\beta^{2^l} + \alpha^{2^{-l}}\beta^{-2^l}) = Tr_{2l}^{4l}((\alpha\beta)^{2^l}).$$

Likninga kan dermed skrivast

$$Tr_{2l}^{4l}(\alpha\beta) + \gamma^{i2^{l-1}} Tr_{2l}^{4l}((\alpha\beta)^{2^l}) = f_{ab}(\beta) = Tr_{2l}^{4l}(\alpha\beta + b^{2^{l-1}}\beta^{2^l}).$$

Lat $Tr_{2l}^{4l}(\alpha\beta) = \delta \in GF(2^{2l})$. Då kan likninga skrivast

$$\delta + \gamma^{i2^{l-1}}\delta^{2^l} = 0.$$

For $\delta \in GF(2^{2l})$ gjeld

i) $(\delta + \delta^{2^l})^{2^l} = (\delta^{2^l} + \delta) \Rightarrow (\delta + \delta^{2^l}) = \zeta \in GF(2^l)$.

ii) $\delta = \delta^{2^l} \Leftrightarrow \delta = \zeta \in GF(2^l)$.

γ^i er konstant for alle komponentar i $c^*(a,b)$. Når $(\delta + \delta^{2^l})$ går gjennom $GF(2^l)$ vil også $(\delta + \gamma^{i2^{l-1}}\delta^{2^l})$ gjera det. Dette tilseier at posisjonane gitt av $f_{ab}(\beta^j)$, kan ha høgst 2^l ulike vediar.

Jfr. definisjon 4.6.12.

Korollar 3. Søylene i generatormatrisa for V^* har rang $\leq l$.

Bevis. Lat $0 \leq j \leq 2^{2l}$. Sidan $V^* \subseteq U^*$, kan $f_{ab}(\beta^j)$ skrivast

$$f_{ab}(\beta^j) = Tr_{2l}^{4l}(\alpha\beta) + \gamma^{i2^{l-1}} Tr_{2l}^{4l}((\alpha\beta)^{2^l})$$
$$= \delta + \gamma^{i2^{l-1}}\delta^{2^l} = 0,\ \delta \in GF(2^{2l}).$$

Ettersom γ er konstant for alle kodeord i V^*, kan ei kvar søyle i V^* sjåast som lineærkombinasjonar av $(\delta + \delta^{2^l})$, $\delta \in GF(2^{2l})$. Sidan $(\delta + \delta^{2^l}) \in GF(2^l)$, vil $f_{ab}(\beta^j)$ ha høgst 2^l ulike vediar, og søyla har rang $\leq l$.

Vedlegg IV

Numeriske data for kodar der $h(x) = m_1(x)m_s(x)$, $n = 2^m-1$, gcd(n, s) = 1.

d'_r og vektoppteljar ved søk.

m = 4, **s = 7.** $A(z) = 1 + 30\,z^4 + 60\,z^6 + 105\,z^8 + 60\,z^{10}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	4	4	4	0
2	6	6	2	0
3	7	8	2	1
4	8	9	1	1
5	9	11	2	2
6	10	12	1	2
7	11	14	2	3
8	12	15	1	3

m = 4, **s = 7. Den duale koden.** $A(z) = 1 + 5\,z^3 + 806\,z^6 + 2635\,z^7$

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	3	3	3	0
2	5	6	3	1
3	6	9	3	3
4	7	11	2	4
5	8	13	2	5
6	9	14	1	5
7	10	15	1	5

***m* = 5, *s* = 3, 5, 7, 11.** $A(z) = 1 + 310\, z^{12} + 527z^{16} + 186\, z^{20}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	12	12	12	0
2	18	18	+ 6	0
3	21	21	+ 3	0
4	23	23	+ 2	0
5	24	25	+ 2	1
6	25	26	+ 1	1
7	26	28	+ 2	2
8	27	29	+ 1	2
9	28	30	+ 1	2
10	29	31	+ 1	2

***m* = 5, *s* = 3, 5, 7, 11. Dei duale kodane.** $A(z) = 1 + 186\, z^5 + 806\, z^6 + 2635\, z^7 + 7905\, z^8 + 18910\, z^9 + 41602\, z^{10} + 85560\, z^{11} + 142600\, z^{12} + 195300\, z^{13} + 251100\, z^{14} + 301971\, z^{15} + 301971\, z^{16} + 251100\, z^{17} + 195300\, z^{18} + 142600\, z^{19} + 85560\, z^{20} + 41602\, z^{21} + 18910\, z^{22} + 7905\, z^{23} + 2635\, z^{24} + 806\, z^{25} + 186z^{26} + z^{31}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	5	5	5	0
2	8	8	+ 3	0
3	10	10	+ 2	0
4	11	12	+ 2	1
5	12	13	+ 1	1
6	13	15	+ 2	2
7	14	16	+ 1	2
8	15	17	+ 1	2
9	16	18	+ 1	2
10	17	19	+ 1	2
11	18	21	+ 2	3
12	19	22	+ 1	3
13	20	23	+ 1	3
14	21	24	+ 1	3
15	22	25	+ 1	3
16	23	26	+ 1	3
17	24	27	+ 1	3
18	25	28	+ 1	3
19	26	29	+ 1	3
20	27	30	+ 1	3
21	28	31	+ 1	3

$m = 5$, $s = 15$. $A(z) = 1 + 31\,z^{10} + 155\,z^{12} + 310\,z^{14} + 217\,z^{16} + 155\,z^{18} + 155\,z^{20}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	10	10	10	0
2	15	16	+ 6	1
3	18	20	+ 4	2
4	20	23	+ 3	3
5	21	25	+ 2	4
6	22	26	+ 1	4
7	23	28	+ 2	5
8	24	29	+ 1	5
9	25	30	+ 1	5
10	26	31	+ 1	5

$m = 5$, $s = 15$. Den duale koden. $A(z) = 1 + 217\,z^5 + 837\,z^6 + 2325\,z^7 + 7595\,z^8 + 20305\,z^9 + 42997\,z^{10} + 81840\,z^{11} + 138880\,z^{12} + 201810\,z^{13} + 257610\,z^{14} + 294159\,z^{15} + 294159\,z^{16} + 257610\,z^{17} + 201810\,z^{18} + 138880\,z^{19} + 81840\,z^{20} + 42997\,z^{21} + 20305\,z^{22} + 7595\,z^{23} + 2325\,z^{24} + 837\,z^{25} + 217\,z^{26} + z^{31}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	5	5	5	0
2	8	8	+ 3	0
3	10	10	+ 2	0
4	11	11	+ 1	0
5	12	13	+ 2	1
6	13	14	+ 1	1
7	14	15	+ 1	1
8	15	17	+ 2	2
9	16	18	+ 1	2
10	17	19	+ 1	2
11	18	20	+ 1	2
12	19	21	+ 1	2
13	20	23	+ 2	3
14	21	24	+ 1	3
15	22	25	+ 1	3
16	23	26	+ 1	3
17	24	27	+ 1	3
18	25	28	+ 1	3
19	26	29	+ 1	3
20	27	30	+ 1	3
21	28	31	+ 1	3

$m = 6$, $s = 5, 13$. $A(z) = 1 + 630\, z^{24} + 3087\, z^{32} + 378\, z^{40}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	24	24	24	0
2	36	36	12	0
3	42	42	6	0
4	45	45	3	0
5	47	47	2	0
6	48	48	1	0
7	49	54	6	5
8	50	57	3	7
9	51	59	2	8
10	52	60	1	8
11	53	62	2	9
12	54	63	1	9

$m = 6$, $s = 31$. $A(z) = 1 + 189\, z^{24} + 504\, z^{26} + 567\, z^{28} + 378\, z^{30} + 882\, z^{32} + 756 z^{34} + 441 z^{36} + 378 z^{38}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	24	24	24	0
2	36	36	12	0
3	42	43	7	1
4	45	47	4	2
5	47	51	4	4
6	48	54	3	6
7	49	56	2	7
8	50	57	1	7
9	51	59	2	8
10	52	60	1	8
11	53	62	2	9
12	54	63	1	9

$m = 6$, $s = 11, 23$. $A(z) = 1 + 126\, z^{20} + 252\, z^{24} + 756\, z^{28} + 1827\, z^{32} + 1134\, z^{36}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	20	20	20	0
2	30	30	10	0
3	35	35	5	0
4	38	39	4	1
5	40	41	2	1
6	41	42	1	1
7	42	50	8	8
8	43	54	4	11
9	44	56	2	12
10	45	60	4	15
11	46	62	2	16
12	47	63	1	16

$m = 7$, $s = 3, 9, 13, 15, 23, 43.$ $A(z) = 1 + 4572\, z^{56} + 8255\, z^{64} + 3556\, z^{72}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	56	56	56	0
2	84	84	28	0
3	98	98	14	0
4	105	105	7	0
5	109	110	5	1
6	111	114	4	3
7	112	117	3	5
8	113	119	2	6
9	114	121	2	7
10	115	122	1	7
11	116	124	2	8
12	117	125	1	8
13	118	126	1	8
14	119	127	1	8

$m = 7$, $s = 5, 27.$ $A(z) = 1 + 4572\, z^{56} + 8255\, z^{64} + 3556\, z^{72}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	56	56	56	0
2	84	84	28	0
3	98	98	14	0
4	105	105	7	0
5	109	110	5	1
6	111	113	3	2
7	112	116	3	4
8	113	119	3	6
9	114	121	2	7
10	115	122	1	7
11	116	124	2	8
12	117	125	1	8
13	118	126	1	8
14	119	127	1	8

***m* = 7, *s* = 11.** $A(z) = 1 + 4572\, z^{56} + 8255\, z^{64} + 3556\, z^{72}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	56	56	56	0
2	84	84	28	0
3	98	98	14	0
4	105	105	7	0
5	109	109	4	0
6	111	113	4	2
7	112	116	3	4
8	113	119	3	6
9	114	121	2	7
10	115	122	1	7
11	116	124	2	8
12	117	125	1	8
13	118	126	1	8
14	119	127	1	8

***m* = 7, *s* = 29.** $A(z) = 1 + 4572\, z^{56} + 8255\, z^{64} + 3556\, z^{72}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	56	56	56	0
2	84	84	28	0
3	98	98	14	0
4	105	105	7	0
5	109	110	5	1
6	111	114	4	3
7	112	116	2	4
8	113	119	3	6
9	114	121	2	7
10	115	122	1	7
11	116	124	2	8
12	117	125	1	8
13	118	126	1	8
14	119	127	1	8

$m = 7$, $s = 63$. $A(z) = 1 + 889\,z^{54} + 1778\,z^{56} + 1778\,z^{58} + 889\,z^{60} + 2667\,z^{62} + 2032\,z^{64} + 889\,z^{66} + 2667\,z^{68} + 1016\,z^{70} + 889\,z^{72} + 889\,z^{74}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	54	54	54	0
2	81	81	27	0
3	95	95	14	0
4	102	103	8	1
5	106	109	6	3
6	108	113	4	5
7	109	116	3	7
8	110	119	3	9
9	111	121	2	10
10	112	122	1	10
11	113	124	2	11
12	114	125	1	11
13	115	126	1	11
14	116	127	1	11

$m = 7$, $s = 7, 21, 31, 55$. $A(z) = 1 + 889\,z^{52} + 1778\,z^{56} + 3556\,z^{60} + 4699\,z^{64} + 3556\,z^{68} + 1778\,z^{72} + 127\,z^{84}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	52	52	52	0
2	78	78	26	0
3	91	91	13	0
4	98	99	8	1
5	102	105	6	3
6	104	110	5	6
7	105	114	4	9
8	106	117	3	11
9	107	119	2	12
10	108	120	1	12
11	109	123	3	14
12	110	125	2	15
13	111	126	1	15
14	112	127	1	15

***m* = 7, *s* = 19, 47.** $A(z) = 1 + 889\,z^{52} + 1778\,z^{56} + 3556\,z^{60} + 4699\,z^{64} + 3556\,z^{68} + 1778\,z^{72} + 127\,z^{84}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	52	52	52	0
2	78	78	26	0
3	91	91	13	0
4	98	99	8	1
5	102	107	8	5
6	104	111	4	7
7	105	113	2	8
8	106	117	4	11
9	107	120	3	13
10	108	122	2	14
11	109	123	1	14
12	110	125	2	15
13	111	126	1	15
14	112	127	1	15

***m* = 8, *s* = 31, 91.** Sjå Vedlegg V.

***m* = 8, *s* = 127.** $A(z) = 1 + 1275\,z^{112} + 2040\,z^{114} + 5100\,z^{116} + 4080\,z^{118} + 4080\,z^{120} + 4080\,z^{122} + 5100\,z^{124} + 4080\,z^{126} + 4590\,z^{128} + 8160\,z^{130} + 4080\,z^{132} + 6120\,z^{134} + 4590\,z^{136} + 2040\,z^{138} + 4080\,z^{140} + 2040\,z^{142}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	112	112	112	0
2	168	168	56	0
3	196	196	28	0
4	210	212	16	2
5	217	223	11	6
6	221	230	7	9
7	223	236	6	13
8	224	238	2	14
9	225	244	6	19
10	226	246	2	20
11	227	248	2	21
12	228	250	2	22
13	229	251	1	22
14	230	252	1	22
15	231	254	2	23
16	232	555	1	23

***m* = 8, *s* = 11, 29.** $A(z) = 1 + 1020\, z^{104} + 2550\, z^{112} + 17340\, z^{120} + 26010\, z^{128} + 16320\, z^{136} + 2040\, z^{144} + 255\, z^{160}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	104	104	104	0
2	156	156	52	0
3	182	182	26	0
4	195	202	20	7
5	202	214	12	12
6	206	223	9	17
7	208	230	7	22
8	209	234	4	25
9	210	239	5	29
10	211	243	4	32
11	212	246	3	34
12	213	249	3	36
13	214	251	2	37
14	215	253	2	38
15	216	254	1	38
16	217	255	1	38

***m* = 8, *s* = 19, 47.** $A(z) = 1 + 2040\, z^{104} + 2040\, z^{112} + 16320\, z^{120} + 22695\, z^{128} + 22440\, z^{136}$.

r	*g*(*r*, *d*)	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	104	104	104	0
2	156	156	52	0
3	182	182	26	0
4	195	198	16	3
5	202	211	13	9
6	206	219	8	13
7	208	223	4	15
8	209	225	2	16
9	210	233	8	23
10	211	237	4	26
11	212	239	2	27
12	213	240	1	27
13	214	248	8	34
14	215	252	4	37
15	216	254	2	38
16	217	255	1	38

$m = 8$, $s = 7, 37$. $A(z) = 1 + 255\, z^{96} + 3570\, z^{112} + 17340\, z^{120} + 27030\, z^{128} + 13260\, z^{136} + 3570\, z^{144}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	96	96	96	0
2	144	144	48	0
3	168	180	36	12
4	180	198	18	18
5	186	214	16	28
6	189	222	8	33
7	191	230	8	39
8	192	234	4	42
9	193	240	6	47
10	194	243	3	49
11	195	247	4	52
12	196	249	2	53
13	197	251	2	54
14	198	252	1	54
15	199	254	2	55
16	200	255	1	55

$m = 8$, $s = 13, 59$. $A(z) = 1 + 255\, z^{96} + 1020\, z^{104} + 21420\, z^{120} + 26010\, z^{128} + 12240\, z^{136} + 4590\, z^{144}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d')$
1	96	96	96	0
2	144	144	48	0
3	168	174	30	6
4	180	189	15	9
5	186	197	8	11
6	189	201	4	12
7	191	203	2	12
8	192	204	1	12
9	193	228	24	35
10	194	240	12	46
11	195	246	6	51
12	196	249	3	53
13	197	251	2	54
14	198	252	1	54
15	199	254	2	55
16	200	255	1	55

$m = 8$, $s = 23, 61$. $A(z) = 1 + 510\, z^{96} + 5100\, z^{112} + 14280\, z^{120} + 23205\, z^{128} + 22440\, z^{136}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	96	96	96	0
2	144	144	48	0
3	168	168	24	0
4	180	180	12	0
5	186	204	24	18
6	189	216	12	27
7	191	222	6	31
8	192	225	3	33
9	193	233	8	40
10	194	237	4	43
11	195	239	2	44
12	196	240	1	44
13	197	248	8	51
14	198	252	4	54
15	199	254	2	55
16	200	255	1	55

$m = 8$, $s = 53$. Sjå Vedlegg V.

$m = 8$, $s = 43$. $A(z) = 1 + 510\, z^{80} + 255\, z^{96} + 19380\, z^{120} + 28050\, z^{128} + 15300\, z^{136} + 2040\, z^{144}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	80	80	80	0
2	120	120	40	0
3	140	140	20	0
4	150	150	10	0
5	155	158	8	3
6	158	164	6	6
7	160	168	4	8
8	161	170	2	9
9	162	210	40	48
10	163	230	20	67
11	164	240	10	76
12	165	245	8	80
13	166	249	4	83
14	167	252	3	85
15	168	254	2	86
16	169	255	1	86

Vedlegg V

Numeriske data for Niho-kodar.
$h(x) = m_1(x)m_s(x)$,
$n = 2^m-1$, gcd(n, s) = 1.

$s = 2^{l+1}-1$, $m = 2l$.

$l = 4$, **$s = 7$.** $A(z) = 1 + 30\,z^4 + 60\,z^6 + 105\,z^8 + 60\,z^{10}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	4	4	4	0
2	6	6	2	0
3	7	8	2	1
4	8	9	1	1
5	9	11	2	2
6	10	12	1	2
7	11	14	2	3
8	12	15	1	3

$l = 4$, **$s = 31$.** $A(z) = 1 + 10200\,z^{112} + 4080\,z^{120} + 30855\,z^{128} + 20400\,z^{136}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	112	112	112	0
2	168	168	56	0
3	196	196	28	0
4	210	210	14	0
5	217	218	8	1
6	221	222	4	1
7	223	224	2	1
8	224	225	1	1
9	225	233	8	8
10	226	237	4	11
11	227	239	2	12
12	228	240	1	12
13	229	248	8	19
14	230	252	4	22
15	231	254	2	23
16	232	255	1	23

$l = 8$, $s = 511$. $A(z) = 1 + 713\,020\,800\, z^{32512} + 16\,776\,960\, z^{32640} + 2\,139\,127\,935\, z^{32768} + 1\,426\,041\,600\, z^{32896}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	32512	32512	32512	0
2	48768	48768	16256	0
3	56896	56896	8128	0
4	60960	60960	4064	0
5	62992	62992	2032	0
6	64008	64008	1016	0
7	64516	64516	508	0
8	64770	64770	254	0
9	64897	64898	128	1
10	64961	64962	64	1
11	64993	64994	32	1
12	65009	65010	16	1
13	65017	65018	8	1
14	65021	65022	4	1
15	65023	65024	2	1
16	65024	65025	1	1
17	65025	65153	128	128
18	65026	65217	64	191
19	65027	65249	32	222
20	65028	65265	16	237
21	65029	65273	8	244
22	65030	65277	4	247
23	65031	65279	2	248
24	65032	65280	1	248
25	65033	65408	128	375
26	65034	65472	64	438
27	65035	65504	32	469
28	65036	65520	16	484
29	65037	65528	8	491
30	65038	65532	4	494
31	65039	65534	2	495
32	65040	65535	1	495

$s = (2^l-1)(2^{2l}+1) + 2,\ m = 4l.$

$l = 2,$ $s = 53.$ Tabellen syner resultat frå to ulike framgangsmåtar.

$$A(z) = 1 + 1020\, z^{96} + 24480\, z^{120} + 15555\, z^{128} + 24480\, z^{136}.$$

		STRATEGI 1			***STRATEGI 2***		
r	***g*(r, d)**	***d'r***	***tillegg frå d'r-1 til d'r***	***differanse d'r - g(r, d)***	***d'r***	***tillegg frå d'r-1 til d'r***	***differanse d'r - g(r, d)***
1	96	96	96	0	96	96	0
2	144	144	48	0	144	48	0
3	168	168	24	0	168	24	0
4	180	180	12	0	180	12	0
5	186	204	24	18	**188**	**8**	**2**
6	189	216	12	27	**192**	**4**	**3**
7	191	222	6	31	**200**	**8**	**9**
8	192	225	3	33	**204**	**4**	**12**
9	193	233	8	40	**228**	**24**	**35**
10	194	**237**	**4**	**43**	240	12	46
11	195	**239**	**2**	**44**	246	6	51
12	196	**240**	**1**	**44**	249	3	53
13	197	**248**	**8**	**51**	251	2	54
14	198	252	4	54	252	1	54
15	199	254	2	55	254	2	55
16	200	255	1	55	255	1	55

***l* = 4,** ***s* = 3857.** Tabellen syner resultat frå to ulike framgangsmåtar.

$$A(z) = 1 + 1\,048\,560\, z^{30720} + 2\,013\,235\,200\, z^{32640} + 267\,448\,335\, z^{32768} + 2\,013\,235\,200\, z^{32896}.$$

		STRATEGI 1			***STRATEGI 2***		
r	***g*(*r*, *d*)**	***d'*$_r$**	***tillegg frå d'*$_{r-1}$ *til d'*$_r$**	***differanse d'*$_r$ - *g*(*r*, *d*)**	***d'*$_r$**	***tillegg frå d'*$_{r-1}$ *til d'*$_r$**	***differanse d'*$_r$ - *g*(*r*, *d*)**
1	30720	30720	30720	0	30720	30720	0
2	46080	46080	15360	0	46080	15360	0
3	53760	53760	7680	0	53760	7680	0
4	57600	57600	3840	0	57600	3840	0
5	59520	59520	1920	0	59520	1920	0
6	60480	60480	960	0	60480	960	0
7	60960	60960	480	0	60960	480	0
8	61200	61200	240	0	61200	240	0
9	61320	63120	1920	1800	**61328**	**128**	**8**
10	61380	64080	960	2700	**61392**	**64**	**12**
11	61410	64560	480	3150	**61424**	**32**	**14**
12	61425	64800	240	3375	**61440**	**16**	**15**
13	61433	64920	120	3487	**61568**	**128**	**135**
14	61437	64980	60	3543	**61632**	**64**	**195**
15	61439	65010	30	3571	**61664**	**32**	**225**
16	61440	65025	15	3585	**61680**	**16**	**240**
17	61441	65153	128	3712	**63600**	**1920**	**2159**
18	61442	65217	64	3775	**64560**	**960**	**3118**
19	61443	65249	32	3806	**65040**	**480**	**3597**
20	61444	**65265**	**16**	**3821**	65280	240	3836
21	61445	**65273**	**8**	**3828**	65400	120	3955
22	61446	**65277**	**4**	**3831**	65460	60	4014
23	61447	**65279**	**2**	**3832**	65490	30	4043
24	61448	**65280**	**1**	**3832**	65505	15	4057
25	61449	**65408**	**128**	**3959**	65513	8	4064
26	61450	**65472**	**64**	**4022**	65517	4	4067
27	61451	**65504**	**32**	**4053**	65519	2	4068
28	61452	65520	16	4068	65520	1	4068
29	61453	65528	8	4075	65528	8	4075
30	61454	65532	4	4078	65532	4	4078
31	61455	65534	2	4079	65534	2	4079
32	61456	65535	1	4079	65535	1	4079

Vedlegg VI

Numeriske data for irredusible sykliske kodar.

$k/l = 2$.

$n_1 = 3$, $l = 3$. $A(z) = 1 + 21\, z^8 + 42\, z^{12}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	8	8	8	0
2	12	12	4	0
3	14	14	2	0
4	15	18	4	3
5	16	20	2	4
6	17	21	1	4

$n_1 = 3$, $l = 7$. $A(z) = 1 + 381\, z^{128} + 16002\, z^{192}$.

r	$g(r, d)$	d'_r	*tillegg frå* d'_{r-1} *til* d'_r	*differanse* $d'_r - g(r, d)$
1	128	128	128	0
2	192	192	64	0
3	224	224	32	0
4	240	240	16	0
5	248	248	8	0
6	252	252	4	0
7	254	254	2	0
8	255	318	64	63
9	256	350	32	94
10	257	366	16	109
11	258	374	8	116
12	259	378	4	119
13	260	380	2	120
14	261	381	1	120

$k/l = n_1$.

$n_1 = 3$, $l = 2$. $A(z) = 1 + 9\,z^2 + 27\,z^4 + 27\,z^6$.

r	$g(r, d)$	d'_r	tillegg frå d'_{r-1} til d'_r	differanse $d'_r - g(r, d)$
1	2	2	2	0
2	3	3	1	0
3	4	5	2	1
4	5	6	1	1
5	6	8	2	2
6	7	9	1	2

$n_1 = 3$, $l = 4$. $A(z) = 1 + 45\,z^8 + 675\,z^{16} + 3375\,z^{24}$.

r	$g(r, d)$	d'_r	tillegg frå d'_{r-1} til d'_r	differanse $d'_r - g(r, d)$
1	8	8	8	0
2	12	12	4	0
3	14	14	2	0
4	15	15	1	0
5	16	23	8	8
6	17	27	4	10
7	18	29	2	11
8	19	30	1	11
9	20	38	8	18
10	21	42	4	21
11	22	44	2	22
12	23	45	1	22

$k/l = n_1 - 1$.

$n_1 = 5$, $l = 3$. $A(z) = 1 + 70\,z^8 + 420\,z^{12} + 1505\,z^{16} + 2100\,z^{24}$.

r	$g(r, d)$	d'_r	tillegg frå d'_{r-1} til d'_r	differanse $d'_r - g(r, d)$
1	8	8	8	0
2	12	12	4	0
3	14	14	2	0
4	15	18	4	3
5	16	20	2	4
6	17	21	1	4
7	18	25	4	7
8	19	27	2	8
9	20	28	1	8
10	21	32	4	11
11	22	34	2	12
12	23	35	1	12

Kjelder:

[1] R. Brualdi, W. C. Huffman, V.S. Pless, *An Introduction to Algebraic Codes*, Chapter in Handbook of Coding Theory, boka er under arbeid.

[2] G. Cohen, L. Huguet, G. Zemor, *Bounds on generalized Weights*, French-Israeli Workshop on Algebraic Coding. Springer L. N. Comp. Sci., vil verta publisert.

[3] G. van der Geer and M. van der Vlugt, *Generalized Hamming Weights of BCH(3) Revisited*, IEEE Trans. Info. Theory, vol 41, s.300-301, 1995.

[4] G. van der Geer and M. van der Vlugt, *The second generalized Hamming weights of the dual codes of double-error correcting binary BCH-codes*, Bull. London Math. Soc., vil verta publisert.

[5] J. H. Griesmer, *A bound for error-correcting codes*, IBM J. Res. Develop., vol. 4, s. 532-542, 1960.

[6] T. Helleseth, T. Kløve, J. Mykkeltveit,*The weight distribution of irreducible cyclic codes with block lengths* $n_1((q^l-1)/N)$, Discrete Math., vol. 18, s. 179-211, 1977.

[7] T. Helleseth, T. Kløve, Ø. Ytrehus, *Generalized Hamming weights of Linear Codes*, IEEE Trans. Info. Theory, vol 38, s. 1133-1140, 1992.

[8] T. Helleseth, T. Kløve, Ø. Ytrehus, *Codes and the chain condition*, International Workshop on Algebraic and Combinatorial Coding Theory, Bulgaria, 1992.

[9] T. Helleseth and P.V. Kumar, *The weight hierarchy of the Kasami Codes*, Discrete Math., vol. 145, s. 133-143, 1995.

[10] T. Helleseth and P.V. Kumar, *On the weight hierarchy of the semiprimitive codes*, Discrete Math., vil verta publisert.

[11] Y. Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph.D. Dissertation, University of Southern California, Los Angeles, CA, 1972.

[12] M.A. Tsfasman and S.G. Vladut, *Geometric Approach to Higher Weights*, Laboratoire de Mathematiques discrete, Centre National de la Recherches Scientifique, 1995.

[13] V. K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Info. Theory, vol 37, s. 1412-1418, 1991.

Allmen bakgrunnslitteratur har vore:

S. Lin and D. J. Costello, Jr., *Error control Coding; fundamentals and applications*, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1983.

W.W. Peterson and E.J. Weldon, *Error-Correcting Codes*, MIT Press, Cambridge, MASS, 1972

H. van Tilborg, *Error-Correcting Codes - a first course*, ISBN 91-44-38501-3 Studentlitteratur, Lund, 1993.