Sekvenser og anvendelser i mobilkommunikasjon

Tor Helleseth
Institutt for Informatikk
Universitetet of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
Email: torh@ii.uib.no

1 Introduksjon

I moderne kommunikasjonssystemer er det et utstrakt behov for binære (dvs $\{0, 1\}$) sekvenser. Sekvenser har mange praktiske anvendelser som inkluderer radarsystemer, synkronisering av data, generering av tilfeldige tall, konstruksjon av kryptosystemer, posisjonsbestemmelser i Global Positioning System (GPS), samt multippel-aksess-kommunikasjon. Sekvenser med gitte egenskaper kan konstrueres ved hjelp av matematiske metoder som benytter algebra over Galoiskropper eller Galoisringer. Sekvenser kan også genereres enkelt og effektivt i maskinvare ved å benytte skiftregistre. Konstruksjon og anvendelser av sekvenser er derfor et fagområde hvor teori og praksis møtes.

Hovedmålsettingen er å beskrive sekvenser med anvendelser i tredje generasjons mobile kommunikasjons systemer. Slike systemer benytter Code Division Multiple Access (CDMA) der de enkelte brukerne får tildelt forskjellige sekvenser (signatursekvenser). Når en bruker skal sende en databit sender han hele sekvensen sin multiplisert med databiten. Dette kan virke lite effektivt, ihvertfall når brukerne kan ha lange signatursekvenser. Fordelen er at mange brukere kan sende samtidig. CDMA krever store familier av sekvenser med spesielle egenskaper for å forenkle synkronisering samt å minimalisere interferens mellom brukerne. Konstruksjon av optimale sekvensfamilier med ønskede egenskaper og som er enkle å generere er derfor et viktig forskningsområde.

Først beskrives maksimalsekvenser (eller m-sekvenser) som er de mest vanlige sekvensene, og som er byggestener i mange konstruksjoner av gode sekvensfamilier. Deretter beskrives noen tradisjonelt viktige familier av sekvenser konstruert fra m-sekvenser, nemlig Kasami- og Gold-sekvenser. Begge sekvensfamiliene har hatt tallrike anvendelser de siste 30 år.

Den store økningen av antall brukere som kommuniserer har skapt et behov for større familier av sekvenser enn tidligere. I løpet av de siste ti år er enda bedre sekvensfamilier blitt konstruert. Disse sekvensene har symboler fra $Z_4 = \{0, 1, 2, 3\}$, ringen av heltall modulo 4. Tredje generasjons mobilkommunikasjonsstandard (3G IMT-2000) benytter en familie av sekvenser, S(2), funnet av Kumar, Helleseth, Calderbank og Hammons [6]. Vi vil beskrive familien S(2) som er konstruert fra sekvenser med symboler i Z_4, og som inneholder Gold sekvenser som en undermengde.

Første del vil hovedsakelig gi en elementær konstruksjon av sekvensfamilier, illustrert med enkle eksempler, og en forenklet skisse av anvendelsene. Til slutt beskrives kort noen av de matematiske problemene som konstruksjoner av gode sekvensfamilier gir opphav til.

2 Maksimalsekvenser og skiftregistre

En enkel og effektiv metode for å generere binære sekvenser er ved hjelp av lineære rekursjoner. For eksempel vil rekursjonen

$$s(t+3) = s(t+1) + s(t) \pmod 2$$

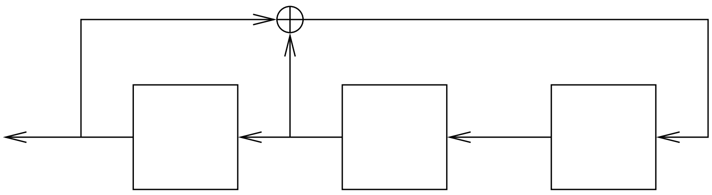
med starttilstand $(s(0), s(1), s(2)) = (001)$ generere den periodiske sekvensen

$$0010111 \;\; 0010111 \;\; 0010111 \;\; 0010111 \;\; \ldots$$

som har periode $e = 7$. Forskjellige starttilstander gir forskjellige sekvenser (som kan være sykliske skift av hverandre).

Binære sekvenser kan lett genereres i maskinvare ved hjelp av skiftregistre. Et eksempel på et skiftregister er vist i Figur 1. Registeret består av "flip-flops" som hver inneholder en 0 eller en 1. Registeret er styrt av en ekstern klokke (som ikke er vist på figuren) som ved hvert tidspunkt skifter hver bit et trinn til venstre og erstatter biten til høyre med summen (mod 2) av de to bitene til venstre. Registeret implementerer rekursjonen $s(t+3) = s(t+1) + s(t) \pmod 2$ som med startinnhold $(s(0), s(1), s(2)) = (001)$ gir den periodiske sekvensen 0010111... ovenfor. Tabell 1 viser innholdet av skiftregisteret ved hver tidsenhet.

Figur 1: Skiftregister for $s(t+3) = s(t+1) + s(t) \pmod 2$



Tabell 1: Skiftregisterinnhold i Figur 1 for generering av m-sekvens

t	$S0$	$S1$	$S2$
0	0	0	1
1	0	1	0
2	1	0	1
3	0	1	1
4	1	1	1
5	1	1	0
6	1	0	0
7	0	0	1
.	.	.	.

En lineær rekursjon av grad n er gitt ved

$$\sum_{i=0}^{n} f_i \, s(t+i) = 0 \tag{1}$$

der koeffisientene $f_i \in GF(2)$ for $0 < i < n$ og $f_0 = f_n = 1$. Det *karakteristiske polynomet* til rekursjonen er definert ved

$$f(x) = \sum_{i=0}^{n} f_i x^i.$$

Starttilstanden og den gitte rekursjonen bestemmer entydig sekvensen som genereres. Et lineært skiftregister med karakteristisk polynom av grad n genererer derfor 2^n forskjellige sekvenser svarende til de 2^n forskjellige starttilstandene, og disse utgjør et vektorrom over $GF(2)$.

Et n-bit lineært skiftregister kan anta høyst 2^n forskjellige tilstander. Siden nulltilstanden alltid etterfølges av nulltilstanden, vil alle sekvenser generert av skiftregisteret ha periode høyst $2^n - 1$. En *maksimalsekvens* (m-sekvens) er en periodisk sekvens av maksimal periode $2^n - 1$ generert av et linært skiftregister av grad n. *Perioden til et polynom* $f(x)$ er definert som det minste positive heltall e slik at $f(x) \mid x^e - 1$. La $f(x)$ være et irredusibelt polynom av grad n og periode $e = 2^n - 1$. Slike polynomer kalles primitive polynomer. Det tilsvarende skiftregister genererer en m-sekvens når starttilstanden er forskjellig fra nulltilstanden. Alle m-sekvenser har et primitivt polynom som sitt karakteristiske polynom.

Binære m-sekvenser er kanskje den best kjente familien av sekvenser. Tabell 2 viser noen m-sekvenser og tilhørende karakteristiske polynomer. Figur 1 viser et skiftregister som har $f(x) = x^3 + x + 1$ som karakteristisk polynom og som genererer en m-sekvens med periode $e = 7$ når starttilstanden er ulik nulltilstanden. Viktige egenskaper for en binær m-sekvens $\{s(t)\}$ med periode $2^n - 1$ er:

- (Balansert) I løpet av en periode av m-sekvensen finnes 2^{n-1} enere og $2^{n-1} - 1$ nullere.

- (Multigram) Når t gjennomløper $0, 1, \ldots, 2^n - 2$, vil n-tuplet

  $$(s(t), s(t+1), \cdots, s(t+n-1))$$

  gjennomløpe alle elementer i $GF(2)^n$ en gang med unntak av n-tuplet (0,0,...,0) som ikke opptrer.

Tabell 2: Karakteristiske polynomer og m-sekvenser

Grad	$f(x)$	m-sekvens	Periode
2	x^2+x+1	011	3
3	x^3+x+1	0010111	7
3	x^3+x^2+1	0011101	7
4	x^4+x+1	000100110101111	15
4	x^4+x^3+1	000111101011001	15

- (Skift-og-addér) For enhver verdi av τ, $0 < \tau \leq 2^n - 2$, finnes en verdi av δ, som avhenger av τ, slik at

$$s(t+\tau) + s(t) = s(t+\delta), \text{ for alle } t.$$

Gitt en m-sekvens $\{s(t)\}$ med periode $2^n - 1$ og la d være primisk til $2^n - 1$. Sekvensen $\{s(dt)\}$ definert ved å velge hvert d-te ledd i $\{s(t)\}$ viser seg å være en m-sekvens og alle m-sekvenser av samme periode kan fås på denne måten. Det viser seg at m-sekvenser av samme lengde generert av forskjellige primitive karakteristiske polynomer er syklisk forskjellige. Antall binære primitive polynomer av grad n er $\phi(2^n - 1)/n$ der $\phi(x)$ er antall positive heltall mindre enn x som er relativt primisk med x. Dette medfører at det er $\phi(2^n - 1)/n$ syklisk forskjellige m-sekvenser av periode $2^n - 1$. Eksemplet nedenfor viser de to $\phi(7)/3 = 2$ syklisk forskjellige m-sekvenser av periode $e = 7$.

Eksempel. Det primitive polynomet $f_1(x) = x^3 + x + 1$, vil generere m-sekvensene $\{a(t)\} = 0010111...$ med periode $e = 2^3 - 1 = 7$. Det primitive polynomet $f_2(x) = x^3 + x^2 + 1$ vil generere m-sekvensen $\{b(t)\} = 0011101...$ med periode $e = 2^3 - 1 = 7$. Bemerk at $\{b(t)\} = \{a(3t)\}$ er sekvensen som fås ved å velge hvert tredje element i $\{a(t)\}$, med indeks beregnet modulo e.

Gitt en sekvens $\{s(t)\}$ med periode e. Da er det i mange anvendelser som krever synkronisering viktig å sammenligne sekvensen med et syklisk skift av seg selv. Derfor er det nyttig å definere *autokorrelasjonen* til den binære sekvensen $\{s(t)\}$, med skift τ, ved

$$\theta_s(\tau) = \sum_{t=0}^{e-1} (-1)^{s(t+\tau)-s(t)}.$$

Spesielt vil $\theta_s(\tau)$ angi antall overenstemmelser minus antall uoverenstemmelser mellom $\{s(t+\tau)\}$ og $\{s(t)\}$. I anvendelser er det ønskelig at et skift av sekvensen ser ut som en "random" sekvens sammenlignet med seg selv, dvs at $|\theta_s(\tau)|$ er liten for alle $\tau \not\equiv 0 \pmod{e}$. En meget viktig egenskap for en m-sekvens er at den har en lavest mulig maksimal verdi (ideéll verdi) av autokorrelasjonen når $\tau \not\equiv 0 \pmod{e}$.

Lemma 1 *Autokorrelasjonen til en m-sekvens $\{s(t)\}$ av periode $e = 2^n - 1$ er gitt ved:*

$$\theta_s(\tau) = \begin{cases} -1 & \textit{for} \quad \tau \not\equiv 0 \ (\textit{mod}\ 2^n - 1), \\ 2^n - 1 & \textit{for} \quad \tau \equiv 0 \ (\textit{mod}\ 2^n - 1). \end{cases}$$

Bevis. Definer $u(t) = s(t+\tau) - s(t)$ og bemerk at $\{u(t)\}$ oppfyller den samme lineære rekursjonen som $\{s(t)\}$. Dette medfører at $\{u(t)\}$ er en m-sekvens når $\tau \not\equiv 0 \pmod{2^n - 1}$ og balanseegenskapen til m-sekvenser gir

$$\theta_s(\tau) = \sum_{t=0}^{e-1} (-1)^{s(t+\tau)-s(t)} = \sum_{t=0}^{e-1} (-1)^{u(t)} = -1.$$

I mange praktiske anvendelser legger en inn kopier av m-sekvensen i dataene som overføres slik at mottaker kan bruke den ideelle autokorrelasjonen til m-sekvensen til synkronisering. Balanse, multigram og autokorrelasjons egenskapene til m-sekvenser er egenskaper en kan forvente av tilfeldige binære sekvenser. Denne pseudo-tilfeldige oppførselen til m-sekvenser har gjort den til en populær byggesten i mange systemer og har ledet til tallrike praktiske anvendelser i mange omåder, inkludert synkronisering, posisjonsbestemmelse, generering av tilfeldige tall og multippel-aksess-kommunikasjon.

3 Krysskorrelasjonen mellom m-sekvenser

I et CDMA system vil hver bruker anvende en fast tildelt $\{-1, +1\}$ sekvens. La $\{p_i(t)\}$ være sekvensen for den i-te bruker. Vi vil illustrere med et lite eksempel hvorledes en benytter sekvenser ved kommunikasjonen. Anta systemet har 8 brukere som vi tilordner hver sin av de følgende sekvenser av lengde $e = 8$.

$$\begin{array}{rcl}
p_1(t) & = & (+1+1+1+1+1+1+1+1) \\
p_2(t) & = & (+1+1+1-1+1-1-1-1) \\
p_3(t) & = & (+1-1+1+1-1+1-1-1) \\
p_4(t) & = & (+1-1-1+1+1-1+1-1) \\
p_5(t) & = & (+1-1-1-1+1+1-1+1) \\
p_6(t) & = & (+1+1-1-1-1+1+1-1) \\
p_7(t) & = & (+1-1+1-1-1-1+1+1) \\
p_8(t) & = & (+1+1-1+1-1-1-1+1)
\end{array}$$

Dette er en Hadamard-matrise av orden 8 (dvs en 8x8 ortogonal matrise der indreproduktet av to ulike rekker er 0). Det er også verdt å bemerke at matrisen som fås ved å stryke første rekke og første søyle i matrisen består av en maksimalsekvens av lengde 7 og alle sykliske skift (når +1 erstattes med 0 og -1 med 1).

Hvorledes sender den j-te bruker en databit d_j? For eksempel er det ofte vanlig å velge $d_j \in \{-1, +1\}$, eller $d_i \in \{1, \omega, \omega^2, \omega^3\}$, avhengig av hvilken modulasjonsmetode som benyttes, der ω er en kompleks primitiv fjerde enhetsrot. Bruker sender hele sekvensen $\{d_j p_j(t)\}$ for $t = 0, 1, \ldots, e-1$. Dersom flere brukere (for eksempel bruker i og j) sender samtidig gir dette opphav til sekvensen

$$q(t) = \{d_i p_i(t)\} + \{d_j p_j(t)\}.$$

Når sekvensen $\{q(t)\}$ mottas, og brukerne sender data synkront, kan vi enkelt beregne dataene til enhver bruker. For å finne d_j beregnes indreproduktet,

$$\begin{array}{rcl}
T & = & \sum_{t=0}^{e-1} q(t) p_j(t) \\
& = & d_i \sum_{t=0}^{e-1} p_i(t) p_j(t) + d_j \sum_{t=0}^{e-1} p_j(t) p_j(t) \\
& = & 8 d_j
\end{array}$$

siden sekvensene $\{p_i(t)\}$ er ortogonale når $i \neq j$.

I mange anvendelser er brukerne ikke synkroniserte, eller det er så mange brukere at det er upraktisk å finne et tilstrekkelig antall ortogonale sekvenser uten at disse blir for lange. Når brukerne ikke er synkroniserte vil signalet (når i og j sender) være av formen $q(t) = \{d_i p_i(t+\tau)\} + \{d_j p_j(t)\}$. Ved rekonstruksjon av d_j vil da indreproduktet mellom $p_i(t+\tau)$ og $p_j(t)$ representere interferensen fra bruker i. Vi ønsker derfor at den maksimale absoluttverdien av indreproduktet er minimal for alle i, j, τ (unntatt for $\tau = 0$ når $i = j$). Denne diskusjonen motiverer definisjonen av krysskorrelasjonen mellom sekvenser.

La $\{u(t)\}$ og $\{v(t)\}$ være to sekvenser med samme periode e og med symboler fra et alfabet med q elementer. Da er krysskorrelasjonen, med skift τ, til sekvensene definert som

$$\theta_{u,v}(\tau) = \sum_{t=0}^{e-1} \omega^{u(t+\tau)-v(t)},$$

der ω er en kompleks primitiv q-te enhetsrot. For binære sekvenser brukes derfor $\omega = -1$. For å forenkle synkronisering og redusere interferensen mellom brukerne ønsker en at denne absoluttverdien er liten.

Et viktig problem i mange anvendelser er derfor å finne store familier av sekvenser med lav maksimal korrelasjon. La

$$\mathcal{F} = \{\{s_i(t)\} \mid 1 \leq i \leq M\}$$

være en familie med M sekvenser med (minste) periode e. La $\theta_{i,j}(\tau)$ være krysskorrelasjonen mellom den i-te and j-te sekvensen med skift τ,

$$\theta_{i,j}(\tau) = \sum_{t=0}^{e-1} \omega^{s_i(t+\tau)-s_j(t)}, \quad 0 \leq \tau \leq e-1.$$

Konstruksjon av sekvenser for CDMA systemer prøver å minimalisere parameteren

$$\theta_{max} = \max\{|\theta_{i,j}(\tau)| \mid \text{ enten } i \neq j \text{ eller } \tau \neq 0\}$$

for fast e and M.

Det er også nyttig å observere at alle sekvensene i en sekvensfamilie antas å være syklisk forskjellige, og ha e som minste periode. Hvis ikke vil en sekvens med minste periode $\epsilon < e$ gi en autokorrelasjon med skift ϵ som medfører $\theta_{max} = e$, noe som er katastrofalt dårlig.

I de neste avsnittene vil vi beskrive familier av gode CDMA sekvenser, inkludert de binære familiene Gold, Kasami og Kerdock, samt sekvensene i Familie $\mathcal{A}$ og $S(2)$ som har symboler i Z_4.

4 Goldsekvenser

Siden m-sekvenser har ideell autokorrelasjon, er det naturlig å studere kryss-korrelasjonen mellom par av m-sekvenser. Mange familier av sekvenser er konstruert fra par av m-sekvenser med lav maksimal krysskorrelasjon.

Krysskorrelasjonen mellom to binære m-sekvenser $\{s(t)\}$ og $\{s(dt)\}$ begge med periode $e = 2^n - 1$ kan utrykkes ved:

$$C_d(\tau) = \sum_{t=0}^{2^n-2} (-1)^{s(t+\tau)-s(dt)}.$$

En kan vise at krysskorrelasjonen mellom to m-sekvenser generert av forskjellige primitive karakteristiske polynomer antar minst tre forskjellige verdier. I 1968 viste Gold [1] det første eksemplet på par av m-sekvenser med tre-nivås krysskorrelasjon.

Teorem 1 *Definer $f = gcd(n,k)$ og la n/f være odde. Hvis $d = 2^k + 1$, har $C_d(\tau)$ de tre følgende verdier når τ gjennomløper $0, 1, \ldots, 2^n - 2$,*

$$\begin{array}{llll} -1 + 2^{\frac{n+f}{2}} & \textit{opptrer} & 2^{n-f-1} + 2^{\frac{n-f-2}{2}} & \textit{ganger} \\ -1 & \textit{opptrer} & 2^n - 2^{n-f} - 1 & \textit{ganger} \\ -1 - 2^{\frac{n+f}{2}} & \textit{opptrer} & 2^{n-f-1} - 2^{\frac{n-f-2}{2}} & \textit{ganger.} \end{array}$$

Basert på dette resultatet konstrueres familien av Goldsekvenser. Familien består av to m-sekvenser som adskiller seg med en desimering d samt alle summer av den ene m-sekvensen med alle sykliske skift av den andre. La $\{a(t)\}$ være en binær m-sekvens med periode $e = 2^n - 1$ der n er odde. La $\{b(t)\} = \{a(dt)\}$, der $d = 2^k + 1$ og $f = gcd(n,k) = 1$. Gold familien er definert ved

$$\mathcal{G} = \{a(t)\} \cup \{b(t)\} \cup \{\{a(t) + b(t+\tau)\} \mid 0 \leq \tau \leq 2^n - 2\}.$$

Parametrene til Gold familien er

$$M = |\mathcal{G}| = e + 2,\ e = 2^n - 1,\ n \text{ odde },\ \theta_{max} = 1 + \sqrt{2(e+1)}.$$

Verdien til $\theta_{max} = 1 + \sqrt{2(e+1)} = 1 + 2^{\frac{n+1}{2}}$ for Gold sekvensene er en konsekvens av skift-og-addér egenskapen til m-sekvenser som medfører at

Tabell 3: Familien av Goldsekvenser med periode 7

Sekvenskonstruksjon	Binærsekvens
$\{a(t)\}$	0010111
$\{b(t)\}$	0011101
$\{a(t)\} + \{b(t)\}$	0001010
$\{a(t)\} + \{b(t+1)\}$	0101101
$\{a(t)\} + \{b(t+2)\}$	1100011
$\{a(t)\} + \{b(t+3)\}$	1111110
$\{a(t)\} + \{b(t+4)\}$	1000100
$\{a(t)\} + \{b(t+5)\}$	0110000
$\{a(t)\} + \{b(t+6)\}$	1011001

auto- eller krysskorrelasjonen mellom to Goldsekvenser lett sees å være enten autokorrelasjonen for en m-sekvens eller en krysskorrelasjon mellom en m-sekvens og dens desimerte med d. Dette medfører at alle korrelasjonsverdiene som forekommer er i mengden $\{-1 - 2^{\frac{n+1}{2}}, -1, -1 + 2^{\frac{n+1}{2}}\}$.

Det finnes nedre skranker for θ_{max} som gjelder for alle binære sekvensfamilier for gitt M og e. Disse skrankene viser at Goldsekvensene utgjør en optimal familie i den forstand at for den gitte verdi av M og e er det umulig å finne en familie med lavere θ_{max}. Goldsekvenser har vært brukt i 30 år og anvendelser inkluderer Navstar GPS. Også neste generasjons mobilkommunikasjon vil anvende Goldsekvenser (av lengde $e = 2^{25} - 1$). Figur 2 viser skiftregistre som genererer familien av Goldsekvenser av lengde $e = 7$, vist i Tabell 3.

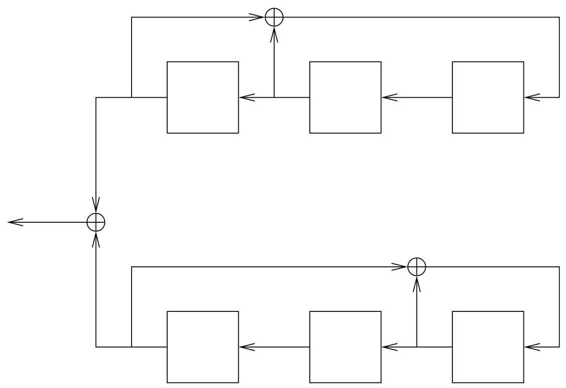
5 Kasamisekvenser

En annen familie av sekvenser skyldes Kasami. Denne familien er mindre enn Goldfamilien men har til gjengjeld en lavere verdi av θ_{max}. Kasamifamilien er i likhet med Goldfamilien konstruert ved hjelp av m-sekvenser.

Familien av Kasamisekvenser kan beskrives på følgende måte. La $n = 2k$, og la $\{a(t)\}$ være en m-sekvens med periode $e = 2^n - 1$. La $\{b(t)\}$ være en m-sekvens med periode $2^k - 1$. Familien av Kasamisekvenser er definert ved

$$\mathcal{K} \;=\; \{a(t)\} \cup \{\{a(t) + b(t+\tau)\} \mid 0 \leq \tau \leq 2^k - 2\}.$$

Figur 2: Skiftregister som genererer Goldsekvenser med periode 7



Tabell 4: Familien av Kasamisekvenser med periode 15

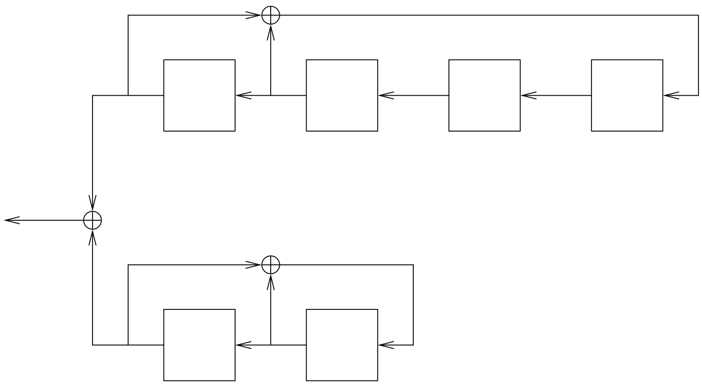
Sekvenskonstruksjon	Binærsekvens
$\{a(t)\}$	000100110101111
$\{a(t)\}+\{b(t)\}$	011111101110100
$\{a(t)\}+\{b(t+1)\}$	110010000011001
$\{a(t)\}+\{b(t+2)\}$	101001011000010

Kasamifamilien $\mathcal{K}$ inneholder $M = 2^k$ sekvenser av periode $e = 2^n - 1$. I dette tilfellet kan en vise at $\theta_{max} = 1 + 2^k$. Parametrene til Kasamifamilien er derfor

$$M = |\mathcal{K}| = \sqrt{e+1},\ e = 2^n - 1,\ n \text{ jamn },\ \theta_{max} = 1 + \sqrt{e+1}.$$

Kasamifamilien er optimal i den forstand at den har lavest mulige verdi av θ_{max} for de gitte verdier av e og M. Tabell 4 viser en familie av Kasamisekvenser av lengde $e = 15$. Bemerk at $\{b(t)\} = 011011011011011$ med periode 3 ikke er med i familien. Figur 3 viser skiftregistre som genererer en familie av Kasamisekvenser med periode $e = 15$.

Figur 3: Skiftregister som genererer Kasamisekvenser med periode 15



6 Sekvenser konstruert fra Z_4

Dersom en øker størrelsen på alfabetet kan en lage sekvensfamilier som er bedre enn i det binære tilfellet. Spesielt kan en konstruere sekvenser over Z_4 med gode korrelasjonsegenskaper og som er praktiske å implementere. Et utmerket eksempel på dette er familie $\mathcal{A}$.

Familie $\mathcal{A}$. La $f(x)$ være det karakteristiske polynomet for en binær m-sekvens av periode $2^n - 1$. Betrakt $f(x)$ som et polynom over Z_4. Da vil polynomet $(-1)^n f(x)f(-x)$ bare ha jamne koeffisienter, og definerer et polynom $g(x)$ over Z_4 av grad n gitt ved

$$g(x^2) = (-1)^n f(x)f(-x).$$

La $g(x) = \sum_{i=0}^{n} g_i x^i$ og studer de 4^n sekvenser $\{a(t)\}$ over Z_4 som oppfyller rekursjonen

$$\sum_{i=0}^{n} g_i a(t+i) = 0.$$

Det viser seg at med unntak av nullsekvensen så vil alle sekvensene generert på denne måten ha periode $2^n - 1$. Altså vil rekursjonen generere en familie $\mathcal{A}$ som består av $2^n + 1$ syklisk forskjellige sekvenser over Z_4. En detaljert studie viser at den maksimale korrelasjonen θ_{max} for denne familien oppfyller $\theta_{max} \leq 1 + \sqrt{2^n}$ når n er odde. Sammenlignet med familien av Goldsekvenser, gir familie $\mathcal{A}$ en lavere verdi for θ_{max} (med en faktor $\sqrt{2}$) med samme familie

Tabell 5: Sekvensfamilie $\mathcal{A}$ med periode 7

0012311
0020222
0032133
0103332
0111203
0131021
0230313
1132212
1223233

størrelse. Parametrene til familie $\mathcal{A}$ er derfor

$$M = |\mathcal{A}| = e + 2, \ e = 2^n - 1, \ n \text{ odde}, \ \theta_{max} = 1 + \sqrt{e+1}.$$

Sammenlignet ned familien av Kasamisekvenser er familie $\mathcal{A}$ en mye større familie med samme skranke på θ_{max}.

Eksempel. La $f(x) = x^3 + x + 1$ være det karakteristiske polynomet til m-sekvensen $\{a(t)\}$. Da gjelder over Z_4

$$g(x^2) = (-1)^3 f(x) f(-x) = x^6 + 2x^4 + x^2 + 3$$

som gir $g(x) = x^3 + 2x^2 + x + 3$.

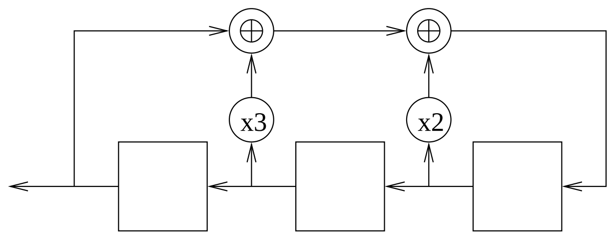
Sekvensene i familie $\mathcal{A}$ er derfor generert av rekursjonen over Z_4, gitt ved

$$s(t+3) + 2s(t+2) + s(t+1) + 3s(t) = 0.$$

Figur 4 viser skiftregistre som ved å variere starttilstandene genererer de 9 sekvensene med lengde $e = 7$ fra familie $\mathcal{A}$, vist i Tabell 5. I dette tilfellet er $\theta_{max} \leq 1 + \sqrt{8}$.

Kerdocksekvenser. Dette er en familie binære sekvenser generert ved hjelp av en modifisering av sekvensene i familie $\mathcal{A}$. La $h(x) = -g(-x) = \sum_{i=0}^{n} h_i x^i$, der $g(x)$ genererer familien av sekvenser i familie $\mathcal{A}$. La S bestå av alle Z_4 sekvenser som oppfyller rekursjonen $\sum_{i=0}^{n} h_i s(t+i) = 0$. Da vil S inneholde 4^n forskjellige sekvenser $\{u(t)\}$ som svarer til alle starttilstander i skiftregisteret.

Figur 4: Skiftregister generering av familie $\mathcal{A}$ med periode 7



Disse sekvensene er på formen $u(t) = (-1)^t s(t)$ der $\{s(t)\}$ er en sekvens i familie $\mathcal{A}$, og vil alle ha periode $2(2^n - 1)$.

La T betegne undermengden S av de 2^n sekvenser som fås ved initialisering av skiftregisteret ved bare å bruke symbolene 0 og 2 i Z_4. Da vil $S - T$ inneholde $4^n - 2^n$ sekvenser, og inneholde en undermengde $\mathcal{U}$ med 2^{n-1} syklisk forskjellige sekvenser som hver har periode $2(2^n - 1)$.

Gitt $x = a + 2b \ \in Z_4$ med $a, b \in \{0, 1\}$, la μ betegne mest signifikante bit, $\mu(x) = b$. La $\mathcal{K}_E$ være familien av 2^{n-1} binære sekvenser som fås ved å anvende μ på alle sekvensene i $\mathcal{U}$. Det viser seg at alle sekvensene in $\mathcal{U}$ også har periode $2(2^n - 1)$, og videre gjelder for familien $\mathcal{K}_E$, at $\theta_{max} \leq 2 + \sqrt{2^{n+1}}$. Parametrene til familien av Kerdocksekvenser er derfor

$$M = |\mathcal{K}_E| = (e + 2)/4, \ e = 2(2^n - 1), \ n \text{ odde }, \ \theta_{max} \leq 2 + \sqrt{e + 2}.$$

Dette betyr at $\mathcal{K}_E$ er en vesentlig større familie enn Kasami familien, samtidig som den har nesten samme verdi for θ_{max}.

Eksempel. La $n = 3$ og $f(x) = x^3 + x + 1$, da er $g(x) = x^3 + 2x^2 + x + 3$, som gir $h(x) = -g(-x) = x^3 + 2x^2 + x + 1$. De tilsvarende Kerdocksekvenser genereres ved hjelp av et skiftregister med karakteristisk polynom $h(x)$ kombinert med avbildningen μ ved utgangen av skiftregisteret. Man utelukker starttilstander av skiftregisteret som bare har 0'ere and 2'ere. Dette gir en familie av 4 syklisk forskjellige sekvenser med periode 14.

7 Familie S(2)

I tredje generasjons globale mobile kommunikasjonsstandard benyttes lange Goldsekvenser av lengde $2^{25} - 1$. I tillegg, for avanserte anvendelser, er valgt

Tabell 6: Parametre for noen sekvensfamilier

Familie	Alfabet	Periode e	Størrelse	θ_{max}
Gold	$GF(2)$	$2^n - 1$, n odde	$e+2$	$1+\sqrt{2(e+1)}$
Kasami	$GF(2)$	$2^n - 1$, n jamn	$\sqrt{e+1}$	$1+\sqrt{e+1}$
Kerdock	$GF(2)$	$2(2^n - 1)$, n odde	$(e+2)/4$	$2+\sqrt{e+2}$
$\mathcal{A}$	Z_4	$2^n - 1$, n odde	$e+2$	$1+\sqrt{e+1}$
$S(2)$	Z_4	$2^n - 1$	e^3	$1+4\sqrt{e+1}$

en familie av korte sekvenser av lengde $e = 255$ over Z_4, betegnet $S(2)$, som er konstruert av Kumar, Helleseth, Calderbank og Hammons [6]. Figur 5 viser de tre skiftregistrene som implementerer sekvensfamilien $S(2)$.

La $f(x)$ være det binære primitive polynomet

$$f(x) = x^8 + x^5 + x^3 + x^2 + 1.$$

Definer $g(x)$ over Z_4 ved å oppfatte $f(x)$ som et polynom over Z_4, og beregn $g(x^2) = (-1)^n f(x)f(-x)$ med metoden som er illustrert tidligere. Dette gir

$$g(x) = x^8 + x^5 + 3x^3 + x^2 + 2x + 1.$$

Det nederste skiftregisteret har $g(x)$ som sitt karakteristiske polynom og genererer sekvenser over Z_4, i henhold til rekursjonen

$$u(t+8) + u(t+5) + 3u(t+3) + u(t+2) + 2u(t+1) + u(t) = 0.$$

Det midterste skiftregisteret har

$$f_1(x) = x^8 + x^7 + x^5 + x + 1$$

som sitt binære karakteristiske polynom. Polynomet $f_1(x)$ er valgt med egenskapen at røttene er 3-dje potens av røttene i $f(x)$. Det midterste registeret genererer sekvenser fra rekursjonen

$$v_1(t+8) + v_1(t+7) + v_1(t+5) + v_1(t+1) + v_1(t) = 0.$$

Det øverste skiftregisteret har

$$f_2(x) = x^8 + x^7 + x^5 + x^4 + 1$$

som sitt binære karakteristisk polynom. Polynomet $f_2(x)$ er valgt slik at røttene er 5-te potens av røttene i $f(x)$. Det øverste registeret genererer sekvenser fra rekursjonen

$$v_2(t+8) + v_2(t+7) + v_2(t+5) + v_2(t+4) + v_2(t) = 0.$$

Ved utgangen multipliseres de to første registre med 2 (mod 4). Dette betyr at skiftregistrene genererer sekvenser av formen:

$$u(t) + 2v_1(t) + 2v_2(t).$$

Antall initialiseringer av de tre skiftregistrene er $4^8 \cdot 2^8 \cdot 2^8 = 2^{32}$. Av disse er $2^8 \cdot 2^8 \cdot 2^8 = 2^{24}$ initialiseringer med bare 0'ere og 2'ere. Dersom vi fjerner disse intialiseringer vil alle sekvensene ha periode $e = 2^8 - 1 = 255$, og genererer $(2^{32} - 2^{24})/(2^8 - 1) = 2^{24}$ syklisk forskjellige sekvenser som utgjør familien $S(2)$. For å generere de syklisk forskjellige sekvensene initialiseres det nederste register med bare 0'ere og 2'ere og deretter adderes 1 til den venstre bit i det nederste registeret.

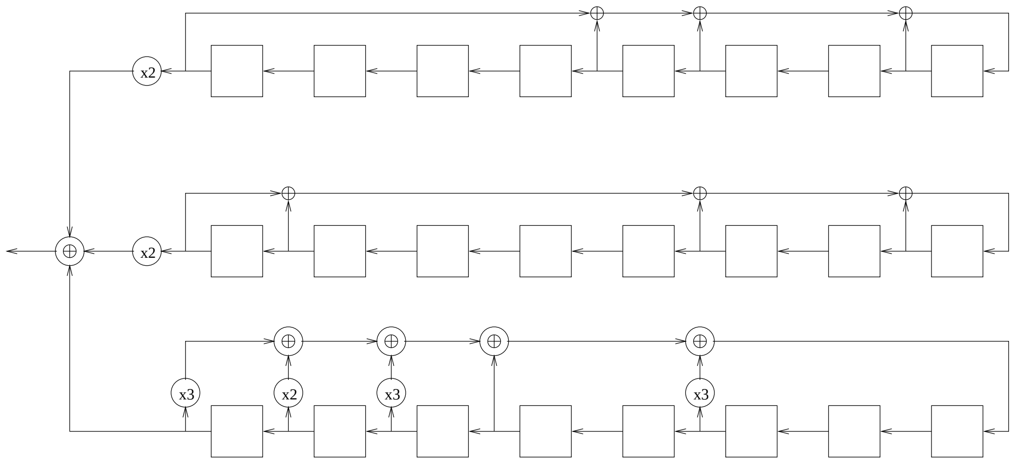
Det er interessant å bemerke at det nederste skiftregisteret genererer sekvenser i familie $\mathcal{A}$. De to nederste skiftregistrene genererer Goldsekvensene med $\{0, 2\}$ istedenfor $\{0, 1\}$, slik at Goldsekvenser er en undermengde av $S(2)$ familien. Kumar, Helleseth og Calderbank [5] har også vist hvorledes større sekvensfamilier kan konstrueres.

8 Matematiske metoder i sekvensanalyse

I analysen av sekvensfamiliene ovenfor benytter en mange algebraiske metoder i Galoiskropper og/eller Galoisringer. Spesielt vil årsakene til de forskjellige egenskapene til sekvensfamiliene skyldes egenskaper til eksponensial summer i endelige kropper og ringer. Vi vil gi en svært kort forklaring som indikerer noen av disse sammenhengende.

La $GF(p) = \{0, 1, \ldots, p-1\}$ være heltallene mod p, der p er et primtall. Denne utgjør en kropp under addisjon og multiplikasjon mod p. Alle endelige kropper er isomorfe og har p^n elementer og betegnes $GF(p^n)$. Disse konstrueres ved å velge et polynom $f(x) \in GF(p)[x]$ av grad n som er irredusibelt over $GF(p)$ og regne modulo $f(x)$. Den endelige kroppen $GF(p^n)$ er da gitt ved $GF(p)[x]/(f(x))$. For eksempel er $GF(2^3) = GF(2)[x]/(x^3 + x + 1)$.

Figur 5: Skiftregister generering av S(2) familien



La $f(x)$ være et primitivt polynom av grad n med (det primitive elementet) $\alpha \in GF(2^n)$ som nullpunkt. La $Tr(x)$ betegne Frobenius' trace-avbildning $Tr : GF(2^n) \to GF(2)$, gitt ved $Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$. En m-sekvens med karakteristisk polynom $f(x)$ kan beskrives på formen

$$s(t) = Tr(a\alpha^t), \quad a \in GF(2^n) \setminus \{0\}.$$

De fleste egenskapene til binære sekvenser generert av lineære skiftregistre kan bestemmes ved å studere egenskaper i $GF(2^n)$.

Sekvensene i Goldfamilien består derfor av sekvensen $\{Tr(\alpha^t)\}$ og de 2^n sekvensene

$$\{Tr(\alpha^t + b\alpha^{2^k+1})\}, \quad b \in GF(2^n).$$

For eksempel følger umiddelbart fra definisjonen at krysskorrelasjonsverdiene mellom sekvensene i Goldfamilien antar verdier bestemt ved

$$-1 + \sum_{x \in GF(2^n)} (-1)^{Tr(ax+bx^{2^k+1})}, \quad a, b \in GF(2^n),$$

som Gold [1] viste var i mengden $\{-1, 1 \pm 2^{\frac{n+1}{2}}\}$ for odde n og $gcd(k, n) = 1$.

Galois ringer av grad n og karakteristikk p^r, der p er et primtall, er isomorfe og betegnes $GR(p^r, n)$. Disse konstrueres ved å velge et polynom $f(x) \in$

$Z_{p^r}[x]$ av grad n som også er irredusibelt mod p. For eksempel er $GR(4,3) = Z_4[x]/(x^3+2x^2+x+3)$.

For å studere sekvenser over Z_4 må vi studere egenskaper i Galoisringer $GR(4,n)$ med karakteristikk 4. Vi kan også her definere en trace-avbildning $T : GR(4,n) \to Z_4 = GR(4,1)$ som gir oss en metode å studere sekvenser over Z_4. For eksempel er sekvensene i familie $\mathcal{A}$ gitt ved

$$s(t) = T(a\beta^t), \;\; a \in GR(4,n) \setminus \{0\},$$

der β er en generator for en (entydig) multiplikativ gruppe av orden $2^n - 1$ i $GR(4,n)$. La $\mathcal{T} =< \beta > \cup\{0\}$, da vil $a = 2$ og $a = 1 + 2\delta$, $\delta \in \mathcal{T}$ gi de $2^n + 1$ syklisk forskjellige sekvensene i familie $\mathcal{A}$.

Sekvensene i familien $S(2)$ er alle på formen

$$T(ax + 2bx^3 + 2cx^5), \;\; a \in GR(4,n), \; b, c \in \mathcal{T},$$

for passende valg av a, b og c. En detaljert analyse av denne spesielle sekvensfamilien og tilhørende eksponensialsummer er utført i [6]. For generalisering og analyse av generelle sekvensfamilier over andre alfabeter ved å studere eksponensial summer over Galoisringer henvises til [5].

9 Konklusjon

Vi har gitt en oversikt over maksimalsekvenser og hvorledes disse spiller en sentral rolle for å konstruere familier av sekvenser for anvendelse i CDMA. Vi har også beskrevet flere binære sekvensfamilier som Gold,- Kasami- og Kerdocksekvenser. I tillegg har vi beskrevet familie $\mathcal{A}$ over Z_4 samt familien $S(2)$ som inneholder Goldsekvenser og familie $\mathcal{A}$ sekvenser som en undermengde, og som har gode korrelasjonsegenskaper. Disse sekvensene benyttes i standarden for tredje generasjons mobilkommunikasjon for avanserte anvendelser.

Referanser

[1] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. Inform. Theory*, vol. 14, 154–156, 1968.

[2] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, *Discrete Math.*, vol. 16, 209–232, 1976.

[3] T. Helleseth and P.Vijay Kumar, Sequences with low correlation, Chapter 21 in: Handbook of Coding Theory (Eds. V.S. Pless and W.C. Huffman), North-Holland 1998.

[4] T. Helleseth og P.Vijay Kumar, Pseudonoise sequences, Chapter 8 in: The Mobile Communications Handbook (Ed. J.D. Gibson), CRC Press and IEEE Press 1999.

[5] P.V. Kumar, T. Helleseth and A.R. Calderbank, An upper bound for Weil exponential sums over Galois rings and applications, *IEEE Trans. Inform. Theory*, vol. 41, 456–468, 1995.

[6] P.V. Kumar, T. Helleseth, A.R. Calderbank and A.R. Hammons, Jr., Large families of quaternary sequences with low correlation, *IEEE Trans. Inform. Theory*, vol. 42, 579–592, 1996.

[7] R. Lidl and H. Niederreiter, *Finite Fields*. Vol. 20 Encyclopedia of Mathematics and its Applications, Reading, MA: Addison-Wesley, 1983.