Hadamard Matricer

Williamsons Metode og Ortogonale Designs

Bachelorprojekt i matematik

Af Jonas Lindstrøm Jensen, 20033834

Vejleder: Jørgen Brandt

Institut For Matematiske Fag – Århus Universitet, Juni 2006

Indhold

Kapitel 1

Definition og basale egenskaber

1.1 Definition

Definition 1.1.1 (Hadamard Matrix)**.** Lad $n \in \mathbb{N}$ og $H \in \mathrm{Mat}_n(\pm 1)$. Så kaldes H en Hadamard Matrix af orden n, hvis

$$HH^\top = nI \tag{1.1.1}$$

Bemærkning 1.1.2. Definitionen ovenfor er ækvivalent med, at H er en ortogonalmatrix med indgange ± 1, så vi kan frit permutere rækker og søjler. Desuden kan vi multiplicere rækker og søjler med -1, idet det bevarer ortogonalitet.

Man kan gange søjler med -1, så alle indgange i øverste række er 1. Det kaldes en normaliseret Hadamard Matrix.

1.2 Nødvendig eksistensbetingelse

Lad os nu vise følgende nødvendige eksistensbetingelse for Hadamard Matricer

Lemma 1.2.1. *Lad $n \in \mathbb{N}$ og lad H være en Hadamard Matrix af orden n. Så gælder at $n = 1, 2$ eller $n \equiv 0 \pmod 4$.*

Bevis. At n kan være enten eller 2 er klart. Så lad os antage, at $n \geqslant 3$. Lad H være en Hadamard Matrix af orden n, og antag at H er normaliseret. Nu kan vi permutere søjlerne i H, så de første 3 rækker er på følgende form (vi skriver + istedet for 1, og - istedet for -1).

$$H = \left(\begin{array}{ccc|ccc|ccc|ccc} + & \cdots & + & + & \cdots & + & + & \cdots & + & + & \cdots & + \\ + & \cdots & + & + & \cdots & + & - & \cdots & - & - & \cdots & - \\ + & \cdots & + & - & \cdots & - & - & \cdots & - & + & \cdots & + \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}\right)$$

Antag, at der er a søjler af den første type, b af den næste, c af den tredje og d af den fjerde. Så har vi

$$a + b + c + d = n \tag{1.2.1}$$

Da rækkerne skal være ortogonale giver de indre produker af de tre første rækker følgende ligninger

$$\begin{aligned} a+b-c-d &= 0 \\ a-b-c+d &= 0 \\ a-b+c-d &= 0 \end{aligned}$$

Lægges disse 3 ligninger sammen med (1.2.1) fås at

$$4a = n$$

Da $a \in \mathbb{N}$ må $n \equiv 0 \pmod 4$. □

Så vi ved altså, at Hadamard Matricer nødvendigvis må have orden 1, 2, eller en orden der er delelig med 4. Det åbenlyse spørgsmål er nu, om der så findes Hadamard Matricer af alle disse ordner – det kaldes for Hadamard Formodningen. I denne opgave vil jeg se på to metoder der viser eksistensen af Hadamard Matricer for nogle ordner.

Den første – Williamsons Metode – er en konstruktion der ender med en computersøgning, og er blevet brugt til at finde Hadamard Matricer af bestemte ordner.

Den anden giver eksistensen af en hel klasse Hadamard Matricer af orden $2^t q$ for $t \geqslant s$ hvor s afhænger af q. Her når jeg dog ikke til samme resultat som de artikler jeg har skrevet ud fra, idet jeg har fundet en fejl i disse. Denne fejl vil jeg også berøre kort.

Ingen af disse har givet løsningen til Hadamard Formodning, der den dag i dag står uløst.

Kapitel 2

Williamsons metode

2.1 Idé og indledning

Vi vil nu se på en måde at konstruere Hadamard Matricer kaldet Williamsons Metode. Den er baseret på, at multiplikations-matricen for quaternions ganget med sin egen transponerede netop er normen for disse quaternions. Idéen formulerer vi i følgende lemma.

Lemma 2.1.1. *Lad $n \in \mathbb{N}$ og lad $A_1, A_2, A_3, A_4 \in \mathrm{Mat}_n(\pm 1)$ være symmestriske og antag de kommuterer indbyrdes. Antag yderligere at*

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n \tag{2.1.1}$$

Så er $H \in \mathrm{Mat}_{4n}(\pm 1)$ givet ved

$$H = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix}$$

en Hadamard Matrix.

Bevis. Kan bevises ved direkte udregning. Antag at $A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n$. Så er

$$\begin{aligned} HH^\top &= \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix} \begin{pmatrix} A_1 & -A_2 & -A_3 & -A_4 \\ A_2 & A_1 & A_4 & -A_3 \\ A_3 & -A_4 & A_1 & A_2 \\ A_4 & A_3 & -A_2 & A_1 \end{pmatrix} \\ &= \begin{pmatrix} 4nI_n & & & \\ & 4nI_n & & \\ & & 4nI_n & \\ & & & 4nI_n \end{pmatrix} = 4nI_n \end{aligned} \tag{2.1.2}$$

□

Det er ikke umiddelbart klart at det er nemmere at finde sådanne A_i'er end at finde en Hadamard Matrix ved blot at prøve sig frem. Men der findes faktisk en glimrende metode til

at reducere problemet med at finde sådanne matricer væsentligt. Lad os nu definere A_i'erne så de kommuterer indbyrdes og er symmetriske. Det gør vi på følgende måde.

Lad $n \in \mathbb{N}$ og lad $U \in \mathrm{Mat}_n(0,1)$ være matricen svarende til permutationen $(1\,2\,3\ldots n) \in S_n$, dvs

$$U = \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & 0 & \ldots & 0 \end{pmatrix} \tag{2.1.3}$$

Lad nu A_1, A_2, A_3, A_4 være polynomier over U med koeficienter ± 1. Dvs (da $U^n = I$)

$$A_i = a_{i,0}I + a_{i,1}U + a_{i,2}U^2 + \cdots + a_{i,n-1}U^{n-1} \quad a_{i,j} = \pm 1 \tag{2.1.4}$$

Da $U^iU^j = U^jU^i$ for alle i, j vil A_i'erne kommutere. Det ses at $U^\top = U^{-1} = U^{n-1}$, så hvis vi sætter $a_{i,n-j} = a_{i,j} \quad \forall j = 1, \ldots, n-1$ vil A_i være symmetrisk. Desuden vil A_i'erne være ± 1-matricer.

A_1, A_2, A_3, A_4 opfylder nu alt i lemma 2.1.1, undtagen ligningen (2.1.1). Vores mål er nu at sætte en computer til at finde koefficienterne, men før vi kan gøre det må vi omskrive lidt på problemet, så vores computer-søgning bliver nemmere.

2.2 En ækvivalent betingelse

Vi vil fra nu af regne mere generelt, nemlig i grupperingen $\mathbb{Z}[G] = \{c_0 + c_1u + c_2u^2 + \cdots c_{n-1}u^{n-1} \mid c_i \in \mathbb{Z} \quad , i = 1, 2, \ldots, n-1\}$, hvor $G = \{u\}$ er en cykliske gruppe frembragt af et element u med $u^n = 1$. Dvs at $\mathrm{ord}(G) | n$. Lad os først definere to forskellige typer af 4-tupler af elementer i $\mathbb{Z}[G]$.

Definition 2.2.1 (Williamson-Type 1)**.** Lad $V_1, V_2, V_3, V_4 \in \mathbb{Z}[G]$. Disse siges at være af Williamson-Type 1 hvis de er på formen

$$V_i = 1 + v_{i,1}u + v_{i,2}u^2 + \cdots + v_{i,n-1}u^{n-1} \quad i = 1, 2, 3, 4$$

hvor $v_{i,j} = \pm 1$ og $v_{i,j} = v_{i,n-j}$ for $i = 1, 2, 3, 4$ og $j > 0$. Desuden skal

$$V_1^2 + V_2^2 + V_3^2 + V_4^2 = 4n$$

Bemærkning 2.2.2. Det ses, at hvis $A_1, A_2, A_3, A_4 \in \mathbb{Z}[U]$ som givet i (2.1.4) er af Williamson-Type 1 giver Lemma 2.1.1 på forrige side og vores overvejelser i kapitel 2.1 en Hadamard Matrix af orden n.

Definition 2.2.3 (Williamson-Type 2)**.** Lad $W_1, W_2, W_3, W_4 \in \mathbb{Z}[G]$. Disse siges at være af Williamson-Type 2 hvis de er på formen

$$W_i = 1 + w_{i,1}u + w_{i,2}u^2 + \cdots + w_{i,n-1}u^{n-1} \quad i = 1, 2, 3, 4$$

hvor $w_{i,j} \in \{-2, 0, 2\}$ og $w_{i,j} = w_{i,n-j}$ for $i = 1, 2, 3, 4$ og $j > 0$, og hvor der for alle j kun findes netop ét i så $w_{i,j} \neq 0$. Desuden skal der gælde følgende lighed

$$W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4n$$

Sætning 2.2.4 (Williamson)**.** *Antag at n er ulige og lad $V_1, V_2, V_3, V_4 \in \mathbb{Z}[G]$. Lad $W_1, W_2, W_3, W_4 \in \mathbb{Z}[G]$ være givet ved*

$$W_1 = \frac{1}{2}(-V_1 + V_2 + V_3 + V_4) \qquad W_2 = \frac{1}{2}(V_1 - V_2 + V_3 + V_4)$$
$$W_3 = \frac{1}{2}(V_1 + V_2 - V_3 + V_4) \qquad W_4 = \frac{1}{2}(V_1 + V_2 + V_3 - V_4)$$

Så gælder

$$V_1, V_2, V_3, V_4 \text{ er af Williamson-Type 1} \iff W_1, W_2, W_3, W_4 \text{ er af Williamson-Type 2}$$

Bevis. Lad $V_1, V_2, V_3, V_4 \in \mathbb{Z}[G]$ og lad $W_1, W_2, W_3, W_4 \in \mathbb{Z}[G]$ være givet som ovenfor, dvs. $W_i = \frac{1}{2}(V_1 + V_2 + V_3 + V_4 - 2V_i)$ for $i = 1, 2, 3, 4$.

($\Rightarrow$) Antag først at $V_1, V_2, V_3, V_4 \in \mathbb{Z}[G]$ er af Williamson-Type 1. Vi vil nu vise, at W_1, W_2, W_3, W_4 er af Williamson-Type 2. Lad os nu dele V_i'erne op i positiv og negativ del

$$P_i = \sum_{j \,|\, v_{i,j}=1} u^j \qquad N_i = \sum_{j \,|\, v_{i,j}=-1} u^j \qquad i = 1, 2, 3, 4$$

Så har vi for $i = 1, 2, 3, 4$

$$V_i = P_i - N_i$$

Lad nu

$$T = 1 + u + \cdots + u^{n-1}$$

Så er $T = P_i + N_i$ og dermed er $V_i = 2P_i - T$ for alle i. Da V_i'erne er af Williamson-Type 1, har vi

$$V_1^2 + V_2^2 + V_3^2 + V_4^2 = 4n$$

Og da $V_i = 2P_i - T$ for alle i bliver det

$$(2P_1 - T)^2 + (2P_2 - T)^2 + (2P_3 - T)^2 + (2P_4 - T)^2 = 4n \tag{2.2.1}$$

Lad $p_i = \#\{j \,|\, v_{i,j} = 1\}$ betegne antallet af positive led i V_i, dvs antallet af led i P_i. Lad os nu bemærke, at $u^j T = T$ for alle j, da $u^{n+j} = u^j$. Vi får da følgende identiteter

$$TP_i = T\left(\sum_{j \,|\, v_{i,j}=1} u^j\right) = \sum_{j \,|\, v_{i,j}=1} T = p_i T$$

$$T^2 = T(1 + u + \cdots + u^{n-1}) = nT$$

for $i = 1, 2, 3, 4$. Lad os nu regne lidt på et af leddene på VS af (2.2.1).

$$(2P_i - T)^2 = 4P_i^2 - 4P_iT + T^2 = 4P_i^2 - 4p_iT + nT$$

Indsættes dette i (2.2.1) fås

$$4(P_1^2 + P_2^2 + P_3^2 + P_4^2) - 4(p_1 + p_2 + p_3 + p_4)T + 4nT = 4n$$

eller ækvivalent

$$P_1^2 + P_2^2 + P_3^2 + P_4^2 = (p_1 + p_2 + p_3 + p_4 - n)T + n \tag{2.2.2}$$

Lad os nu vise følgende påstand

Påstand. Lad $k \in \{1, 2, \dots n-1\}$. Så findes indbyrdes forskellige i_1, i_2, i_3 så $v_{i_1,k} = v_{i_2,k} = v_{i_3,k}$

Da V_i'erne er af Williamson-Type 1, har vi for $j > 0$ at $v_{i,j} = v_{i,n-j}$, så de positive led optræder parvist. Da $v_{i,0} = 1$ er der derfor et ulige antal positive led i V_i - dvs at p_i er ulige for alle i. Da vi i sætningen har antaget at n er ulige er $p_1 + p_2 + p_3 + p_4 - n$ derfor et ulige tal. I ligningen (2.2.2) har u^j derfor en ulige koefficient for alle $j > 0$ (nemlig $p_1 + p_2 + p_3 + p_4 - n$). 0'te grads-leddet bliver lige (nemlig $p_1 + p_2 + p_3 + p_4$. Derfor bliver HS i (2.2.2) følgende i modulus 2

$$(p_1 + p_2 + p_3 + p_4 - n)T + n \equiv \sum_{j=1}^{n-1} u^j \pmod 2$$

Lad os nu se på VS i (2.2.2) i modulus 2

$$P_i^2 = \left(\sum_{j \mid v_{i,j}=1} u^j \right)^2 = \sum_{j \mid v_{i,j}=1} (u^j)^2 + \sum_{j \neq m \mid v_{i,m}=v_{i,j}=1} 2u^j \equiv \sum_{j \mid v_{i,j}=1} u^{2j} \pmod 2$$

Så (2.2.2) bliver følgende i modulus 2

$$\sum_{j \mid v_{1,j}=1} u^{2j} + \sum_{j \mid v_{2,j}=1} u^{2j} + \sum_{j \mid v_{3,j}=1} u^{2j} + \sum_{j \mid v_{4,j}=1} u^{2j} \equiv \sum_{j=1}^{n-1} u^j \pmod 2 \quad (2.2.3)$$

Lad nu $k \in \{1, 2, \dots, n-1\}$ være givet. Lad os nu bemærke, at da n er ulige findes der et entydigt $c \in \{1, 2, \dots n-1\}$ så $u^c = u^{2k}$, thi hvis $2k \leqslant n-1$, sæt da $c = 2k$, og hvis $2k \geqslant n$, sæt da $c = 2k - n - 1$. Det ses at u^c optræder med koefficient 1 i HS af (2.2.3), dvs u^c må indgå i enten 1 eller 3 af summene på VS. Altså må u^k indgå i 1 eller 3 af P_i'erne. I tilfældet hvor det er i 1 af dem, sæt da i_1, i_2, i_3 til at være de tre andre, hvor vi så har $v_{i_1,k} = v_{i_2,k} = v_{i_3,k} = -1$. I tilfældet hvor u^k indgår i 3 af dem, sæt da i_1, i_2, i_3 til at være disse 3. Så er $v_{i_1,k} = v_{i_2,k} = v_{i_3,k} = +1$. Dette viser vores påstand.

Vi er nu klar til at vise, at W_i'erne er af Williamson-Type 2. Her er flere ting at vise. Lad os først bemærke, at man ved direkte udregning og ved at udnytte at $W_i = \frac{1}{2}(V_1 + V_2 + V_3 + V_4 - 2V_i)$ og $V_1^2 + V_2^2 + V_3^2 + V_4^2 = 4n$ kan se at $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4n$.

Lad os nu vise, at $w_{i,0} = 1$ for alle i. Da $v_{i,0} = 1$ for alle i har vi at

$$w_{i,0} = \frac{1}{2}(v_{1,0} + v_{2,0} + v_{3,0} + v_{4,0} - 2v_{i,0}) = 1$$

Lad os så vise, at for $j > 0$ er $w_{i,j} \in \{0, \pm 2\}$. Dette fås af vores påstand ovenfor, for lad $i = 1, 2, 3, 4$ og $k \in \{1, 2, \dots n-1\}$ være givet. Så er

$$w_{i,k} = \frac{1}{2}(v_{1,k} + v_{2,k} + v_{3,k} + v_{4,k} - 2v_{i,k})$$

Vi ved at der findes i_1, i_2, i_3 så $v_{i_1,k} = v_{i_2,k} = v_{i_3,k}$. Lad os antage at disse er $+1$. Antag at vores givne i ikke er et af disse. Da er $v_{i,k} = -1$. Så er

$$w_{i,k} = \frac{1}{2}(v_{i_1,k} + v_{i_2,k} + v_{i_3,k} - v_{i,k}) = \frac{1}{2}(3 - (-1)) = 2$$

Antag nu at vores givne i er blandt de 3 ens, der er $+1$. Så er

$$w_{i,k} = 0$$

Tilsvarende udregninger viser, at hvis de tre er negative, er $w_{i,k} = 0$ hvis vores givne i er blandt de 3, og $w_{i,k} = -2$ hvis ikke. I begge tilfælde er netop en af $w_{i,k}$'erne ikke nul for hvert i. Det er et andet af betingelserne for Williamson-Type 2.

Lad os nu vise, at $w_{i,j} = w_{i,n-j}$. Dette gælder da $v_{i,j} = v_{i,n-j}$. For vi har for alle i, j at

$$\begin{aligned} w_{i,j} &= \frac{1}{2}(v_{1,j} + v_{2,j} + v_{3,j} + v_{4,j} - 2v_{i,j}) \\ &= \frac{1}{2}(v_{1,n-j} + v_{2,n-j} + v_{3,n-j} + v_{4,n-j} - 2v_{i,n-j}) = w_{i,n-j} \end{aligned}$$

($\Leftarrow$) Antag at W_1, W_2, W_3, W_4 er af Williamson-Type 2. V_i'erne er givet ved

$$\begin{aligned} V_1 &= \frac{1}{2}(-W_1 + W_2 + W_3 + W_4) & V_2 &= \frac{1}{2}(W_1 - W_2 + W_3 + W_4) \\ V_3 &= \frac{1}{2}(W_1 + W_2 - W_3 + W_4) & V_4 &= \frac{1}{2}(W_1 + W_2 + W_3 - W_4) \end{aligned}$$

Thi lad $i = 1, 2, 3, 4$ givet, så er

$$\begin{aligned} \frac{1}{2}(W_1 + W_2 + W_3 + W_4 - 2W_i) = \frac{1}{2}\Big\{ &\frac{1}{2}(-V_1 + V_2 + V_3 + V_4) + \frac{1}{2}(V_1 - V_2 + V_3 + V_4) \\ &+ \frac{1}{2}(V_1 + V_2 - V_3 + V_4) + \frac{1}{2}(V_1 + V_2 + V_3 - V_4) - (V_1 + V_2 + V_3 + V_4 - 2V_i)\Big\} = V_i \end{aligned}$$

Lad os nu vise, at V_i'erne er af Williamson-Type 1. Lad os først bemærke, at man ved kan ved direkte udregning kan se at $V_1^2 + V_2^2 + V_3^2 + V_4^2 = 4n$

Lad os nu vise, at $v_{i,j} = \pm 1$ for alle i, j. Lad i, j givet. Det ses at

$$v_{i,j} = \frac{1}{2}(w_{1,j} + w_{2,j} + w_{3,j} + w_{4,j} - 2w_{i,j})$$

Da W_i'erne er af Williamson-Type 2, er præcis en af koefficienterne på HS enten 2 eller -2. Antag at det er netop $w_{i,j}$. Så er

$$v_{i,j} = \frac{1}{2}(w_{1,j} + w_{2,j} + w_{3,j} + w_{4,j} - 2w_{i,j}) = \pm 1$$

Hvis det ikke er $w_{i,j}$ fås samme resultat. Tilbage er nu at vise, at $v_{i,j} = v_{i,n-j}$ for alle i, j. Men dette gælder da $w_{i,j} = w_{i,n-j}$ for alle i, j, thi

$$\begin{aligned} v_{i,j} &= \frac{1}{2}(w_{1,j} + w_{2,j} + w_{3,j} + w_{4,j} - 2w_{i,j}) \\ &= \frac{1}{2}(w_{1,n-j} + w_{2,n-j} + w_{3,n-j} + w_{4,n-j} - 2w_{i,n-j}) = v_{i,n-j} \end{aligned}$$

□

Koefficienterne til W_i'erne må være lidt nemmere at finde, da vi for givet j kun har en koefficient forskellig fra 0 i netop én af W_i'erne. Tidligere havde vi for hvert k $2^4 = 16$ forskellige valg til $v_{i,k}$'erne. Nu har vi $4 \cdot 2 = 8$ valg til $w_{i,k}$'erne.

2.3 Endnu en ækvivalent betingelse

Lad os nu indføre endnu en type 4-tuppel af polynomier over u.

Definition 2.3.1 (Williamson-Type 3)**.** Lad $W_1, W_2, W_3, W_4 \in \mathbb{Z}[u]$. Disse siges at være af Williamson-Type 3, hvis $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4n$ og

$$W_i = 1 + P_i - N_i \tag{2.3.1}$$

Hvor

$$P_i = \sum_{j \in \mathscr{P}_i} 2(u^j + u^{n-j}) \qquad N_i = \sum_{j \in \mathscr{N}_i} 2(u^j + u^{n-j})$$

og $\mathscr{P}_i$'erne og $\mathscr{N}_i$'erne tilsammen udgør en disjunkt forening af $\{1, 2, \ldots, (n-1)/2\}$ under følgende betingelser: For $i = 1, 2, 3, 4$ skal gælde

$$|P_i| - |N_i| = \begin{cases} m_i & \text{hvis } k_i \equiv 1 \pmod 4 \\ -m_i & \text{hvis } k_i \equiv 3 \pmod 4 \end{cases} \tag{2.3.2}$$

hvor m_i'erne er defineret ved $k_i^2 = (1 + 4m_i)^2$ hvor $k_i := |\sum_{j=0}^{n-1} w_{i,j}|$.

At man kan finde entydige m_i'er så den sidste betingelse er opfyldt skal lige overvejes. Lad os først bemærke at da $w_{i,0} = 1$ og $w_{i,j} \in \{\pm 2, 0\}$ for $j > 0$ er k_i'erne ulige. Lad os så vise eksistensen og entydigheden af et sådant m i følgende lemma.

Lemma 2.3.2. *Lad $k \in \mathbb{Z}$ være et positivt ulige tal. Så findes entydigt $m \in \mathbb{Z}$ så*

$$k^2 = (1 + 4m)^2$$

Og ydermere gælder, at hvis $k \equiv 1 \pmod 4$ så er m ikke-negativ og hvis $k \equiv 3 \pmod 4$ er m ikke-positiv.

Bevis. Der er to tilfælde

- $k \equiv 1 \pmod 4$: Så er $k = 4d + 1$ for et $d \in \mathbb{Z}$. Sæt da $m = d$.
- $k \equiv 3 \pmod 4$: Så er $k = 4d - 1$ for et $d \in \mathbb{Z}$. Dvs. at $k^2 = (-(4d-1))^2 = (1-4d)^2$. Sæt derfor $m = -d$

Da d i begge tilfælde er ikke-negativ, har vi vores betingelse på m. Entydigheden får vi på følgende måde. Antag at både m_1 og m_2 opfylder at $k^2 = (1 + 4m_i)^2$. Så er

$$(1 + 4m_1)^2 = (1 + 4m_2)^2$$

Dvs at

$$1 + 4m_1 = \pm(1 + 4m_2)$$

Hvis $1 + 4m_1 = 1 + 4m_2$ er $m_1 = m_2$. Hvis $1 + 4m_1 = -(1 + 4m_2)$ får vi at

$$1/2 + m_1 = -m_2$$

Men da både m_1 og m_2 er hele tal, kan det ikke lade sig gøre. Altså må $m_1 = m_2$.

□

Vi vil nu vise, at det at være Williamson-Type 2 og Williamson-Type 3 er det samme.

Sætning 2.3.3. *Lad n være ulige og lad $W_1, W_2, W_3, W_4 \in \mathbb{Z}[G]$. Så er W_1, W_2, W_3, W_4 af Williamson-Type 2 hvis og kun hvis de er af Williamson Type 3.*

Bevis. Der er to veje at vise. Lad først $W_1, W_2, W_3, W_4 \in \mathbb{Z}[G]$ være af Williamson-Type 2. Lad $k_i = |\sum_{j=0}^{n-1} w_{i,j}|$ for $i = 1, 2, 3, 4$. Lad $m_i, i = 1, 2, 3, 4$ være givet så $k_i^2 = (1 + 4m_i)^2$, som givet i Lemma 2.3.2 på forrige side.

Lad nu et $i \in \{1, 2, 3, 4\}$ være givet. Sæt nu $y_j = u^j + u^{n-j}$. Da $w_{i,j} = w_{i,n-j}$ for alle j har vi at

$$W_i = 1 + w_{i,j_1} y_{j_1} + \cdots + w_{i,j_p} y_{j_p} \tag{2.3.3}$$

for passende $j_l \in \{1, 2, \ldots, (n-1)/2\}, l = 1, \ldots, p$. Dette gælder for alle u med $u^n = 1$, så hvis vi sætter $u = 1$ får vi at $y_j = 2$ for alle j så

$$W_i = 1 + 2w_{i,j_1} + \cdots + 2w_{i,j_p}$$

Men dette er jo præcis summen af W_i's koefficienter, der jo er defineret til at være k_i. Da vi har ligheden $k_i^2 = (1 + 4m_i)^2$ har vi så

$$(1 + 4m_i)^2 = k_i^2 = (1 + 2w_{i,j_1} + \cdots + 2w_{i,j_p})^2$$

Da m_i var entydig, har vi så at

$$4m_i = 2w_{i,j_1} + \cdots + 2w_{i,j_p}$$

eller ækvivalent

$$2m_i = w_{i,j_1} + \cdots + w_{i,j_p} \tag{2.3.4}$$

Lad os nu dele op i to tilfælde:

$\mathbf{k_i \equiv 1}$ (mod 4) – Så er m_i ikke-negativ ifølge Lemma 2.3.2 på modstående side. Husk nu at $w_{i,j_l} = \pm 2$ for alle l. Så hvis (2.3.4) skal gælde, må m_i af w_{i,j_l}'erne være lig med 2— disse j_l'er skal ligge i $\mathscr{P}_i$ – og resten skal være skiftevist 2 og -2, så de ophæver hinanden. Disse j_l'er skal være i hendholdsvis $\mathscr{P}_i$ og $\mathscr{N}_i$. Sammenholdes dette med (2.3.3) får vi præcis formen i (2.4.3).

$\mathbf{k_i \equiv 3}$ (mod 4) – Her er m_i ikke-positiv ifølge Lemma 2.3.2 på forrige side. Med samme argumentation som ovenfor, må $|m_i|$ af w_{i,j_l}'erne være lig med -2 – disse j_l'er skal ligge i $\mathscr{P}_i$, og resten skal være skiftevis 2 og -2 så de ophæver hinanden. Det opnås ved at de lægges i henheoldsvis $\mathscr{P}$ og $\mathscr{N}$. Sammenholdes dette med (2.3.3) får vi præcis formen i (2.4.3)

Det ses, at i begge tilfælde er (2.4.2 opfyldt. Tilbage er at vise, at $\mathscr{P}_i$'erne og $\mathscr{N}_i$'erne tilsammen udgør en disjunkt partition af $\{1, 2, \ldots, (n-1)/2\}$. Lad os først bemærke, at for et givet i, er $\mathscr{P}_i$ og $\mathscr{N}_i$ disjunkte ifølge vores konstruktion ovenfor. Og af definitionen af Williamson-Type 2 får vi, at for hvert $j > 0$ er $w_{i,j} \neq 0$ for netop et i. Så et givet j indgår i en af $\mathscr{P}_i$ eller $\mathscr{N}_i$ for *netop* et i. Og da alle $w_{i,j}$'er indgår i en af W_i'erne, og ethvert j derfor indgår i en af mængderne, har vi en disjunkt partition.

Antag nu, at W_i'erne er af Williamson-Type 3. Vi vil nu vise at de også er af Williamson-Type 2. Sæt igen $y_j = u^j + u^{n-j}$. Per antagelse opfylder de at $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4n$.

Vi vil nu vise, at $w_{i,0} = 1$ for alle i. Men det ses direkte af (2.4.3). Her ses det også, at alle $w_{i,j}$'er må være 0 eller ± 2.

At $w_{i,j} = w_{i,n-j}$ for alle i og j ses af, at da $y_j = u_j + u_{n-j}$, vil u_j og u_{n-j} have samme koefficient i W_i for et givet i.

Tilbage er at vise, at for givet j, er netop een af $w_{i,j}$'erne forskellig fra nul. Så lad j givet. Da $w_{i,j} = w_{i,n-j}$ kan vi antage at $j \leqslant (n-1)/2$. Da $\mathscr{P}_i$'erne og $\mathscr{N}_i$'erne udgør en disjunkt partition af $\{1, 2, \ldots, (n-1)/2\}$ ligger j i netop en af disse. Derfor vil kun en af W_i'erne have $w_{i,j}$ forskellig fra nul. □

Korollar 2.3.4. *Lad $n > 0$ være ulige, og lad $B_1, B_2, B_3, B_4 \in \mathbb{Z}[U]$. Sæt*

$$A_i = \frac{1}{2}(B_1 + B_2 + B_3 + B_4 - 2B_i) \quad i = 1, 2, 3, 4$$

Antag at B_1, B_2, B_3, B_4 er af Williamson-Type 3, så findes en Hadamard Matrix af orden n

Bevis. Dette fås umiddelbart af Sætning 2.3.3 på forrige side, Sætning 2.2.4 på side 7 og Bemærkning 2.2.2 på side 6. □

Nu er vi klar til en søgning efter polynomier over U af Williamson-Type 3. Lad os nu kigge på følgende lemma, der siger os noget om for hvilke k_i'er vi behøver at lave en søgning.

Lemma 2.3.5. *Lad $W_1, W_2, W_3, W_4 \in \mathbb{Z}[G]$ være af Williamson-Type 3. Så opfylder k_i'erne*

$$4n = k_1^2 + k_2^2 + k_3^2 + k_4^2$$

hvor $k_i := \sum_{j=0}^{n-1} w_{i,j}$. Desuden er alle k_i'erne ulige.

Bevis. W_i'erne er på formen

$$W_i = w_{i,0} + w_{i,1}u + w_{i,2}u^2 + \cdots + w_{i,n-1}u^{n-1} \qquad i = 1, 2, 3, 4$$

Vi har antaget at u opfylder $u^n = 1$. Det opfyldes specielt af 1, så hvis vi sætter $u = 1$ får vi

$$|W_i| = |\sum_{j=0}^{n-1} w_{i,j}| = k_i \qquad i = 1, 2, 3, 4$$

Hvoraf påstanden så følger, da $W_1^2 + W_2^2 + W_3^2 + W_4^2 = 4n$. At alle k_i'erne er ulige får vi af, at $w_{i,0} = 1$ og $w_{i,j} = \pm 2$ for $j > 0$. □

2.4 Søgning

Ifølge Korollar 2.3.4 har vi, at hvis n er ulige og vi har 4 polynomier over U, $B_1, B_2, B_3, B_4 \in \mathbb{Z}[U]$ af Williamson-Type 3, så er A_1, A_2, A_3, A_4 givet ved

$$A_1 = \frac{1}{2}(B_1 + B_2 + B_3 + B_4 - 2B_i) \quad i = 1, 2, 3, 4 \tag{2.4.1}$$

af Williamson-Type 1, og giver da en Hadamard Matrix af orden n. Af Lemma 2.3.5 har vi at k_i'erne er ulige, så for alle opskrivninger af $4n$ i en sum af 4 ulige kvadrater, $k_1^2 + k_2^2 + k_3^2 + k_4^2 = 4n$, skal vi prøve med alle partioner af $\{1, 2, \ldots, (n-1)/2\}$ i $\mathscr{P}_i$'er og $\mathscr{N}_i$'er så

$$|P_i| - |N_i| = \begin{cases} m_i & \text{hvis } k_i \equiv 1 \pmod 4 \\ -m_i & \text{hvis } k_i \equiv 3 \pmod 4 \end{cases} \tag{2.4.2}$$

hvor m_i'erne er defineret ved $k_i^2 = (1+4m_i)^2$ hvor $k_i := |\sum_{j=0}^{n-1} w_{i,j}|$. Så sætter vi

$$B_i = 1 + P_i - N_i \tag{2.4.3}$$

hvor

$$P_i = \sum_{j \in \mathscr{P}_i} 2(U^j + U^{n-j}) \qquad N_i = \sum_{j \in \mathscr{N}_i} 2(U^j + U^{n-j})$$

og så prøver vi om $B_1^2 + B_2^2 + B_3^2 + B_4^2 = 4n$. Hvis vi finder sådanne B_i'er giver A_1, A_2, A_3, A_4 givet ved (2.4.1) en Hadamard Matrix af orden $4n$.

Eksempel 2.4.1. Lad os nu prøve at lave en Hadamard Matrix vha. Williamsons Metode. Vi vil her lave én af størrelse 92, dvs $n = 23$. 92 kan skrives som en sum af 4 ulige kvadrater på følgende måde

$$92 = 9^2 + 3^2 + 1^2 + 1^2$$

Så vi ved at vores W_i'er må opfylde

$$92 = (1 + P_1 - N_1)^2 + (1 + P_2 - N_2)^2 + (1 + P_3 - N_3)^2 + (1 + P_4 + N_4)^2$$

Hvor $|P_1| - |N_1| = 2$, $|P_2| - |N_2| = -1$ og $|P_3| - |N_3| = |P_4| - |N_4| = 0$. Vores søgning går nu ud på, at vi skal finde ud af hvordan $\mathscr{P}_i$'erne og $\mathscr{N}_i$'erne skal udgøre en disjunkt partition af $\{1, 2, \ldots, 11\}$.

Der er nogle symmetriske tilfælde – fx er det ligemeget hvordan vi vender B_3 og B_4, da de giver samme bidrag til summen. Nu løber vi så alle forskellige muligheder (fraregnet symmetriske tilfælde) igennem for hvorledes vi kan konstruere B_1, B_2, B_3, B_4. I alt kommer vi igennem godt 15 mio. måder. For hver af disse ser vi om $B_1^2 + B_2^2 + B_3^2 + B_4^2 = 4n$. Vi får så følgende løsninger hvor $V_j = 2(U_j + U_{23-j})$ (én løsning pr. række)

$B_1 = I + V_1 + V_8$	$B_2 = I + V_4 - V_6 - V_{11}$	$B_3 = I + V_2 + V_{10} - V_7 - V_9$	$B_4 = I + V_3 - V_5$
$B_1 = I + V_1 + V_3$	$B_2 = I + V_{11} - V_5 - V_{10}$	$B_3 = I + V_6 + V_7 - V_2 - V_4$	$B_4 = I + V_9 - V_8$
$B_1 = I + V_2 + V_6$	$B_2 = I + V_1 - V_3 - V_{10}$	$B_3 = I + V_6 + V_7 - V_2 - V_4$	$B_4 = I + V_9 - V_8$
$B_1 = I + V_2 + V_7$	$B_2 = I + V_8 - V_1 - V_{11}$	$B_3 = I + V_3 + V_4 - V_5 - V_9$	$B_4 = I + V_6 - V_{10}$
$B_1 = I + V_4 + V_9$	$B_2 = I + V_7 - V_1 - V_2$	$B_3 = I + V_6 + V_8 - V_5 - V_{10}$	$B_4 = I + V_{11} - V_3$
$B_1 = I + V_4 + V_{11}$	$B_2 = I + V_2 - V_3 - V_6$	$B_3 = I + V_1 + V_5 - V_7 - V_8$	$B_4 = I + V_{10} - V_9$
$B_1 = I + V_1 + V_8$	$B_2 = I + V_4 - V_6 - V_{11}$	$B_3 = I + V_2 + V_{10} - V_7 - V_9$	$B_4 = I + V_3 - V_5$
$B_1 = I + V_7 + V_{10}$	$B_2 = I + V_5 - V_4 - V_8$	$B_3 = I + V_1 + V_9 - V_3 - V_6$	$B_4 = I + V_2 - V_{11}$
$B_1 = I + V_{10} + V_{11}$	$B_2 = I + V_6 - V_5 - V_9$	$B_3 = I + V_3 + V_8 - V_1 - V_2$	$B_4 = I + V_7 - V_4$
$B_1 = I + V_5 + V_6$	$B_2 = I + V_3 - V_7 - V_9$	$B_3 = I + V_4 + V_{10} - V_1 - V_{11}$	$B_4 = I + V_8 - V_2$
$B_1 = I + V_5 + V_8$	$B_2 = I + V_9 - V_2 - V_4$	$B_3 = I + V_7 + V_{11} - V_3 - V_{10}$	$B_4 = I + V_1 - V_6$
$B_1 = I + V_3 + V_9$	$B_2 = I + V_{10} - V_7 - V_8$	$B_3 = I + V_2 + V_5 - V_6 - V_{11}$	$B_4 = I + V_4 - V_1$

Vi ser her det lidt spøjse, at alle disse er på samme form, nemlig 2 positive og ingen negative led i B_1, 1 positivt og to negative led i B_2 osv. Hvordan det kan være ved jeg ikke.

Hele søgningen tager 171 sekunder på min 2 GHz laptop, hvilket formodentlig er noget hurtigere end Baumert, Golomb og Hall gjorde det i 1962 (se [6]). Programmet med kildekode kan hentes på http://home.imf.au.dk/jonas/Williamson.

Der skal iøvrigt lyde en tak til Rune Lehard Hansen Stubbe for hjælp med implementeringen og udarbejdelse af programmet.

2.5 Kommentarer til Williamsons Metode

Det er velkendt, at et vilkårligt tal altid kan skrives som en sum af 4 kvadrater. Det kan også vises, at hvis n er ulige kan $4n$ skrives som en sum af 4 ulige kvadrater[1]. Vores søgning startede netop med at skrive $4n$ som en sum af 4 ulige kvadrater – dette kan altså altid gøres. Det er derimod uvist, om man altid kan finde B_i'er så $B_1^2 + B_2^2 + B_3^2 + B_4^2 = 4n$ som beskrevet ovenfor, men det er lykkedes for alle n hvor en søgning er lavet. Det er dog ikke lykkedes for alle opskrivninger af $4n$ i 4 ulige kvadrater – nogle gange er der flere måder at skrive et tal som en sum i ulige kvadrater, hvor nogle af dem ikke virker. Men hidtil har der altid været en der virkede.[2]

Hvis man kunne vise at vi for n ulige kan finde en Hadamard Matrix af orden $4n$, ville Hadamard Formodningen være vist, idet ethvert tal kan skrives som $2^t n$ for n ulige og $t \geqslant 0$. Der findes Hadamard Matricer af orden 2^t for alle $t \geqslant 0$, og en af Paleys konstruktioner (se næste kapitel, Lemma 3.3.3 på side 19) giver at Hadamard Matricer af orden $4n$ og af orden 2^t giver en Hadamard Matrix af orden $4n2^t$.

[1] [8], s. 255
[2] [8], s. 257

Kapitel 3

Ortogonale designs

3.1 Definition og indledning

I dette kapitel, vil vi vise et asymtotisk resultat, der giver eksistensen af en nogle Hadamard Matricer udfra Ortogonale Designs. I [2] og [3] påstås det, at for ethvert naturligt tal $q > 3$ findes et heltal t så vi har en Hadamard Matrix af størrelse $2^s q$ for alle $s > t$. Det vil jeg også vise. I [2] og [3] er også en vurdering på, hvor lille vi kan vælge dette t. Jeg vil i kapitel 3.4 vise, at den vurdering er forkert. Beviser og fremgangsmåde indtil da, er delvist taget fra [2] og [3].

Definition 3.1.1 (Ortogonalt Design)**.** Et ortogonalt design af orden $n \in \mathbb{N}$ og type $(u_1, \ldots, u_s)$ hvor u_i'erne er ikke-negative heltal, på s indbyrdes kommuterende variable $x_1, \ldots, x_s$, er en matrix $n \times n$-matrix X med indgange $0, \pm x_1, \ldots, \pm x_s$ så

$$XX^\top = \left(\sum_{i=1}^{s} u_i x_i^2 \right) I_n \tag{3.1.1}$$

Bemærkning 3.1.2. Lad os bemærke, at vi kan permutere u_i'erne. For hvis vi ombytter u_i og u_j, skal vi bare ombytte x_i og x_j i X. Bemærk også, at et design af type $(u_1, \ldots, u_s)$ er ækvivalent med eksistensen af et design af type $(u_1, \ldots, u_s, 0)$.

3.2 Rekursiv kontruktion

Vi vil nu bevise en række lemmaer, der alle sammen skal bruges til at konstruere ortogonale designs. Senere skal disse designs så bruges til at vise eksistensen af Hadamard Matricer.

Lemma 3.2.1. *Lad X være et ortogonalt design af orden n og type $(u_1, \ldots, u_s)$ på $x_1, \ldots, x_s$. Så findes et ortogonalt design af orden n og type $(u_1, \ldots, u_i + u_j, \ldots, u_s)$ (u_i og u_j er fjernet, og $u_i + u_j$ er tilføjet) på de $s-1$ variable $x_1, \ldots, \bar{x}, \ldots, x_s$ (x_i og x_j er fjernet og $\bar{x}$ er tilføjet).*

Bevis. Lad $\bar{x} := x_i$, og erstat x_i og x_j med $\bar{x}$ i X. Så er

$$\begin{aligned} XX^\top = \left(\sum_{i=1}^{s} u_i x_i^2 \right) I_n &= \left(u_1 x_1^2 + \cdots + u_i \bar{x} + \cdots + u_j \bar{x} + \cdots + u_s x_s^2 \right) I_n \\ &= \left(u_1 x_1^2 + \cdots + (u_i + u_j) \bar{x} + \cdots + u_s x_s^2 \right) I_n \end{aligned} \tag{3.2.1}$$

□

Lemma 3.2.2. *Lad X være et ortogonalt design af orden n og type $(u_1, \ldots, u_s)$. Så findes ortogonale designs af typen*

1. $(e_1u_1, e_2u_2, \ldots, e_su_s)$ *hvor* $e_i \in \{1, 2\}$
2. $(u_1, u_1, fu_2, \ldots, fu_s)$ *hvor* $f \in \{1, 2\}$

af orden $2n$.

Bevis. Lad $x_1, \ldots x_s$ være kommuterende variable. Lad os først se på *(i)*. Sæt for alle $i \in \{1, 2, \ldots, s\}$

$$y_i = \begin{pmatrix} x_i & 0 \\ 0 & x_i \end{pmatrix} \text{ hvis } e_i = 1$$

$$y_i = \begin{pmatrix} x_i & x_i \\ x_i & -x_i \end{pmatrix} \text{ hvis } e_i = 2$$

og lad så Y være $2n \times 2n$-matricen hvor vi erstatter x_i med y_i i X. Så er

$$YY^\top = \left(\sum_{i=1}^{s} u_i y_i^2 \right) \times I_n$$

Af vores konstruktion af y_i'erne får vi at $y_i^2 = e_i x_i^2 I_2$. Dvs at

$$YY^\top = \left(\sum_{i=1}^{s} u_i e_i x_i^2 \right) I_{2n}$$

som ønsket. Lad os nu se på *(ii)*. Lad $x_0, \ldots x_s$ være kommuterende variable. Sæt

$$y_1 = \begin{pmatrix} x_1 & x_0 \\ x_0 & -x_1 \end{pmatrix}$$

Og sæt for $i > 1$

$$y_i = \begin{pmatrix} x_i & 0 \\ 0 & x_i \end{pmatrix} \text{ hvis } f = 1 \quad \text{og} \quad y_i = \begin{pmatrix} x_i & x_i \\ x_i & -x_i \end{pmatrix} \text{ hvis } f = 2$$

Det ses så, at $y_i^2 = f x_i I_2$ for $i > 1$ og at $y_1^2 = (x_0^2 + x_1^2) I_2$. Sæt nu Y til at være $2n \times 2n$-matricen hvor vi i X erstatter x_i med y_i. Så vi har at

$$YY^\top = \left(\sum_{i=1}^{s} u_i y_i^2 \right) \times I_n = \left(u_1 x_0^2 + u_1 x_1^2 + \sum_{i=2}^{s} u_i f x_i^2 \right) I_{2_n}$$

som ønsket. □

Vi vil bruge disse lemmaer til at vise følgende

Lemma 3.2.3. *Antag at alle ortogonale designs af type $(a, b, n - a - b)$, $0 \leqslant a, b \leqslant n$, findes af orden n. Så findes alle ortogonale designs af type $(x, y, 2n - x - y)$, $0 \leqslant x, y \leqslant 2n$, af orden $2n$.*

Bevis. Lad $n \in \mathbb{N}$ være givet og lad $0 \leqslant x, y \leqslant n$ være givet. Vi må have, at $x + y \leqslant 2n$ og $a + b \leqslant n$ da $2n - x - y$ og $n - a - b$ begge skal være ikke-negative. Vi kan uden tab af genralitet antage, at $x \leqslant y$. Vi har nu tre tilfælde

1. Antag at både x og y er lige. Så er $x = 2a$ og $y = 2b$ for passende $a, b \leqslant n$. Vi har at $a + b \leqslant n$, for hvis ikke, ville enten $x = 2a$ eller $y = 2b$ være større end $2n$. Vi har af 1. i Lemma 3.2.2 på modstående side eksistensen af et ortogonalt design af type $(2a, 2b, 2n - 2a - 2b)$ – dvs af type $(x, y, 2n - x - y)$.

2. Antag at x er ulige og y er ulige. Så er $x = a$ og $y = 2b + a$ for passende $a, b \leqslant n$. Men af 2. i Lemma 3.2.2 på forrige side har vi eksistensen af et design af type $(a, a, 2b, 2n - 2a - 2b)$ og af Lemma 3.2.1 på side 15 får vi så eksistensen af et design af type $(a, 2b + a, 2n - 2a - 2b)$ – dvs af type $(x, y, 2n - x - y)$.

3. Antag at x er lige og y er ulige. Hvis $y \leqslant n$ er $x = 2a$ og $y = b$ for passende $a, b \leqslant n$. Af 2. i Lemma 3.2.2 på forrige side får vi eksistensen af et design af type $(a, a, 2b, 2n - 2a - 2b)$ af orden $2n$, og af Lemma 3.2.1 på side 15 får vi så eksistensen af et design af type $(a, 2b, 2n - a - 2b)$ – dvs af type $(x, y, 2n - x - y)$. Hvis $y > n$, må $2n - x - y$ være ulige og mindre end n. Så findes $a, b \leqslant n$ så $a = 2n - x - y$ og $x = 2b$. Af samme argumentation som før får vi, at der findes et ortogonalt design af type $(a, 2b, 2n - a - b)$ – dvs $(2n - x - y, x, y)$. Da vi frit kan permutere rækkefølgen får vi det ønskede.

4. Antag at x er ulige og y er lige. Da $x + y \leqslant n$ og $x \leqslant y$ må $x \leqslant n$. Så vi har $x = a$ og $y = 2b$ for $a, b \leqslant n$. Af 2. i Lemma 3.2.2 på forrige side får vi eksistensen af et design af type $(a, a, 2b, 2n - 2a - 2b)$ og af Lemma 3.2.1 på side 15 får vi så eksistensen af et design af type $(a, 2b, 2n - a - 2b)$ – dvs af type $(x, y, 2n - x - y)$.

□

Følgende korollar er det vi skal bruge til konstruktion af Hadamard Matricer.

Korollar 3.2.4. *Alle ortogonale desings af type $(a, b, 4 - a - b)$ findes af orden 4 for $0 \leqslant a, b \leqslant 4$, og dermed findes ortogonale desings af type $(x, y, 2^t - x - y)$ for $0 \leqslant x, y \leqslant 2^t$ for alle $t \geqslant 2$.*

Bevis. Dette kan vises ved induktion. Vi har givet induktionsstarten, idet vi antager at alle ortogonale desings af type $(a, b, 2^2 - a - b)$ findes af orden 2^2 for $0 \leqslant a, b \leqslant 2^2$. Hvis vi antager at ortogonale designs af type $(a, b, 2^{t-1} - a - b)$ af orden 2^{t-1} findes, giver Lemma 3.2.3 på forrige side at alle ortogonale designs af typen $(a, b, 2^t - a - b)$ af orden 2^t findes, og vi er færdige. Tilbage er at vise, at alle ortogonale desings af type $(a, b, 4 - a - b)$ findes af orden 4 for $0 \leqslant a, b \leqslant 4$ findes. Da vi frit kan ændre rækkefølgen en type, skal vi finde designs af type $(4, 0, 0)$, $(3, 1, 0)$, $(2, 2, 0)$ og $(2, 1, 1)$.

De fås af Lemma 3.2.1 på side 15, da der findes et design af orden 4 og type $(1, 1, 1, 1)$. På 4 kommuterende variable x_1, x_2, x_3, x_4 er denne nemlig givet ved

$$X = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ -x_3 & x_4 & x_1 & -x_2 \\ -x_4 & -x_3 & x_2 & x_1 \end{pmatrix}$$

Det ses så, at

$$XX^\top = (x_1^2 + x_2^2 + x_3^2 + x_4^2)I_4$$

som ønsket. □

3.3 Konstruktion af Hadamard Matricer

Vi skal nu bruge en talteoretisk sætning, der blev bevist af Sylvester.

Sætning 3.3.1 (Frobenius' Mønt-problem)**.** *Lad to indbyrdes primiske heltal $x, y \in \mathbb{Z}$ være givet. Lad $N \geqslant (x-1)(y-1)$ være et heltal. Så findes $a, b \geqslant 0$ så $N = ax + by$.*

Bevis. Følgende bevis er delvist taget fra [7]. Antag at vi har to indbyrdes primiske tal x, y, og antag WLOG at $x \geqslant y$. Lad os først vise følgende påstand:

Påstand. Tallene $0, y, 2y, \ldots, (x-1)y$ forskellige modulo a

Vi vil vise dette per modstrid. Antag at der findes $0 \leqslant n, m < a$ så $ny \equiv my \pmod{x}$. Det er ensbetydende med, at a går op i $my - ny = (m-n)y$. Men da x og y er indbyrdes primiske betyder det, at x går op i $m-n$. Men da begge disse er mindre end x må $m-n = 0$ Lad os nu bevise en anden påstand:

Påstand. $(x-1)(y-1)-1$ kan ikke skrives som en linearkombination af x, y med ikke-negative heltalskoefficienter.

Igen vil vi vise påstanden ved modstrid. Antag at der findes $k, l \geqslant 0$ så

$$kx + ly = (x-1)(y-1) - 1 = xy - x - y$$

Ved at flytte lidt rundt på leddene fås

$$xy = (k+1)x + (l+1)y \tag{3.3.1}$$

Det ses nu, at $0 < l + 1$, da $l \geqslant 0$ og at $l + 1 < x$, thi hvis $l + 1 = x$, måtte $(k+1)x = 0$, hvilket er umuligt, da både $k+1$ og x er skarpt større end 0. Ved at se på (3.3.1) modulo x får vi nu:

$$0 \equiv l + 1 \pmod{x}$$

Men det er modstrid mod den foregående påstand da $0 < l + 1 < x$.

Definer nu følgende mængder

$$S_1 = \{xy - x - y + 1, xy - x - y + 2, xy - x - y + 3, \ldots, xy - y\}$$
$$S_2 = \{k_0 x, k_1 x + y, k_2 x + 2y, \ldots, k_{x-1} x + (x-1)y\}$$

Det ses så at begge mængder består af x heltal, der er indbyrdes forskellige modulo x, ligegyldigt hvad k_i'erne er for nogle tal. Ved at vælge k_i'erne rigtigt, kan vi derfor få mængderne til at være ens.

Lad os nu bemærke, at hvis vi kan bevise, at alle tallene i S_1 kan skrives som ikke-negative heltallige linearkombinationer af x, y er vi færdige, idet S_1 er x styk heltal 'på linje', og at vi for at repræsentere højere tal, blot kan gøre koefficienten til x passende større.

Lad os nu vise, at hvis alle k_i'erne er nul, er alle elementerne i S_1 er større end elementerne i S_2. Lad os derfor se på det mindste element i S_1:

$$\begin{aligned} xy - x - y + 1 &= (x-1)y + 1 - x \\ &> (x-1)y - y \\ &= (x-2)y \\ &\geqslant iy \end{aligned}$$

for $i = 0, 1, 2, \ldots, a-2$. Så vi har vist, at elementerne i S_1 er større end alle elementer i S_2 – undtagen elementet $(x-1)y \in S_2$. Men det ses, at dette element netop er lig med elementet $xy - y \in S_1$. Så vi kan nu konkludere, at de k_i'er vi vælger for at få $S_1 = S_2$ alle er ikke-negative. Dvs. at et element i S_1, $xy - x - y + j \in S_1$ kan skrives på følgende måde

$$xy - x - y + j = k_i x + iy$$

for passende $i, k_i \geqslant 0$. Hermed er vi færdige. □

Det er følgende korrollar vi skal bruge.

Korollar 3.3.2. *Lad $v > 3$ være ulige. Så findes $a, b, t \in \mathbb{N}$ så*

$$a(v+1) + b(v-3) = 2^t$$

Bevis. Sæt $d = \gcd(v+1, v-3)$. Da v er ulige, er d enten 2 eller 4. Definer nu s så stor, at

$$2^s > \left(\frac{v+1}{d} - 1\right)\left(\frac{v-3}{d} - 1\right)$$

Af sætningen får vi nu, at der findes $a, b \in \mathbb{N}$ så

$$a\left(\frac{v+1}{d}\right) + b\left(\frac{v-3}{d}\right) = 2^s$$

Da $d \in \{2, 4\}$, er $d = 2^k$, hvor $k \in \{1, 2\}$. Så ved at gange med 2^k får vi

$$a(v+1) + b(v-3) = 2^{s+k}$$

Sæt nu $t = s + k$, så har vi det ønskede. □

Vi får også brug for følgende lemma.

Lemma 3.3.3. *Lad H være en Hadamard Matrix af orden n og lad G være en Hadamard Matrix af orden m. Så er $H \times G$ en Hadamard Matrix af orden nm.*

Bevis. Dette kommer umiddelbart af regneregler for Kroenecker Produktet af matricer, da

$$(A \times B)^\top = A^\top \times B^\top$$

og

$$(A \times B)(C \times D) = (AC) \times (BD)$$

for vilkårlige matricer af størrelse så udtrykkene giver mening. Så vi får at

$$(H \times G)(H \times G)^\top = (H \times G)(H^\top \times G^\top) = (HH^\top) \times (GG^\top) = I_n \times I_m = I_{mn}$$

hvilket viser det ønskede. □

Nu vil vi vise et par lemmaer, der giver Hadamard Matricer ud fra ortogonale designs. Lad os dog først definere følgende funktion, som vi får brug for.

Definition 3.3.4 (χ-funktionen)**.** Lad $q \in \mathbb{N}$ være et ulige primtal. Så er χ-funktionen med grundtal q en afbildning $\chi : \mathbb{Z} \to \{-1, 0, 1\}$ givet ved

$$\chi(a) = \begin{cases} 0 & \text{hvis } a \equiv 0 \pmod{q} \\ 1 & \text{hvis der findes } x \in \mathbb{Z}, q \nmid x, \text{ så } a \equiv x^2 \pmod{q} \\ -1 & \text{ellers} \end{cases}$$

Vi bemærker, at nogle steder i litteraturen kaldes χ for den kvadratiske rest, og betegnes $\left(\frac{a}{q}\right)$.

Proposition 3.3.5 (Egenskaber for χ-funktionen)**.** *Lad q være et ulige primtal, og lad χ være den tilhørende χ-funktion som givet ovenfor. Lad $a, b \in \mathbb{Z}$, så gælder følgende.*

1. $\chi(a) = \chi(b)$ *hvis* $a \equiv b \pmod{q}$.
2. $\chi(a) = 1$ *for halvdelen af* $a \in \{1, 2, \ldots, q-1\}$ *og* $\chi(a) = -1$ *for den anden halvdel.*
3. $\chi(a)\chi(b) = \chi(ab)$
4. $\sum_{a=1}^{q} \chi(a) = 0$
5. $\sum_{a=1}^{q} \chi(a)\chi(a+b) = -1$ *hvis a og b ikke er ækvivalente modulus q.*
6. $\chi(-1) = 1$ *hvis* $q \equiv 1 \pmod{4}$ *og* $\chi(-1) = -1$ *hvis* $q \equiv 3 \pmod{4}$.

Bevis. 1 er klart ud fra definitionen. Bevis for 2, 3 og 6 kan findes i [4], side 37-38. 4 følger af 2, da $\chi(0) = 0$. Lad os nu vise 5. Da q er et primtal, udgør $\{0, 1, 2, \ldots, q-1\}$ et legeme med den sædvanlige addition og multiplikation. Idet vi lader b^{-1} betegne det inverse element til b i legemet bemærker vi at

$$\chi(a+b) = \chi(a)\chi(1+ab^{-1})$$

For $1 \leqslant a \leqslant q-1$ er $\chi(a)^2 = 1$ og $\chi(q) = 0$ så

$$\sum_{a=1}^{q} \chi(a)\chi(a+b) = \sum_{a=1}^{q-1} \chi(a)^2\chi(1+ab^{-1}) = \sum_{a=1}^{q-1} \chi(1+ab^{-1})$$

Afbildningen $a \mapsto ab^{-1}$ er en bijektion på $\{1, 2, \ldots, q-1\}$ hvis vi regner modulo q, hvilket er tilstrækkeligt ifølge 1 – dette fås af at se på $\{1, 2, \ldots, q-1\}$ som en gruppe med multiplikation som komposition. I en gruppe er multiplikation nemlig bijektivt. I dette tilfælde er den inverse afbildning givet ved $a \mapsto ab$. Da $\chi(0) = 0$ og $\chi(q) = \chi(0)$ har vi derfor

$$\sum_{a=1}^{q-1} \chi(1+ab^{-1}) = \sum_{a=1}^{q-1} \chi(1+a) = \sum_{a=2}^{q-1} \chi(a)$$

og det ønskede følger så af 4, da $\chi(1) = 1$. □

Lemma 3.3.6. *Lad $v \equiv 3 \pmod{4}$ være et primtal, $v \geqslant 3$. Så findes en Hadamard Matrix af orden $2^t v$ for et passende t.*

Bevis. Af Korollar 3.3.2 på side 19 får vi, at der findes $a, b, t \geqslant 0$ så

$$a(v+1) + b(v-3) = 2^t$$

Vi har klart at $a, b \leqslant 2^t$ og af Korollar 3.2.4 på side 17 får vi så, at der findes et ortogonalt design af type $(a, b, 2^t - a - b)$ med orden 2^t på 3 kommuterende variable. Sæt nu disse tre variable til at være $v \times v$-matricerne J, $J - 2I$ og B, hvor J er matricen med lutter ettaller, I er identiteten og B er givet ved $B = (Q + I)R$ hvor R er bag-diagonal matricen med et-taller på bag-diagonalen

$$R = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \iddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

og Q er givet ud fra χ-funktionen med grundtal v ved at

$$(Q)_{ij} = \chi(j - i)$$

Påstand. J, $J - 2I$ og B kommuterer.

J og $J - 2I$ kommuterer klart, da $J^2 = vJ$. Lad os nu se, at B kommuterer med J. Vi bemærker at $JR = J$, så vi har

$$BJ = (Q + I)RJ = (Q + I)J = QJ + J$$

Vi påstår nu, at $QJ = 0$. Det fås af 4 i Proposition 3.3.5 på forrige side da den i, j'te indgang i QJ er givet ved

$$(QJ)_{ij} = \sum_{k=1}^{v} \chi(k - i) = 0$$

Tilsvarende får vi, at $JQ = 0$ så

$$JB = J(Q + I)R = (JQ + J)R = JR = J$$

Og vi har så at $BJ = J = JB$. Tilbage er at vise, at B kommuterer med $J - 2I$. Det får vi af at

$$B(J - 2I) = (J - 2I) = BJ - 2B = -2B$$

og tilsvarende er $(J - 2I)B = -2B$ så B og $J - 2I$ kommuterer.

Vi har altså et ortogonalt design $X \in \mathrm{Mat}_{2^t v}$ af type $(a, b, 2^t - a - b)$ af orden 2^t på de kommuterende variable $J, J - 2I$ og B. Dvs vi har ligheden

$$XX^\top = (aJ^2 + b(J - 2I)^2 + (2^t - a - b)B^2) \times I_{2^t} \tag{3.3.2}$$

Lad os nu vise nogle ting om B og Q.

Påstand. B er symmetrisk

Vi får nu brug for, at B er symmetrisk, så lad os vise det. Af definitionen af Q har vi at den i,j'te indgang i $Q+I$ er givet ved

$$(Q+I)_{ij} = \begin{cases} 1 & \text{hvis der findes } x \in \mathbb{Z} \text{ så } j-i \equiv x^2 \pmod{v} \\ -1 & \text{ellers} \end{cases}$$

Læg mærke til, at x godt kan være nul, idet diagonalen, $i=j$ er et-taller. At multiplicere med R fra højre svarer til at ombytte den i,j'te indgang med den $i,n-j+1$'te indgang. Så $B=(Q+I)R$ er så givet ved

$$(B)_{ij} = \begin{cases} 1 & \text{hvis der findes } x \in \mathbb{Z} \text{ så } n-j+1-i \equiv x^2 \pmod{v} \\ -1 & \text{ellers} \end{cases}$$

Det ses så, at B er symmetrisk, idet $(B)_{ij} = (B)_{ji}$ for alle i og j.

Da B er symmetrisk, kan vi i (3.3.2) erstatte B^2 med $BB^\top$. Da $RR^\top = I$ er

$$BB^\top = (Q+I)RR^\top(Q^\top+I) = QQ^\top + Q + Q^\top + I \tag{3.3.3}$$

Påstand. $Q^\top = -Q$

Af 3 i Proposition 3.3.5 på side 20 får vi, at den i,j'te indgang i $Q^\top$ er givet ved

$$(Q^\top)_{ij} = (Q)_{ji} = \chi(i-j) = \chi(-1)\chi(j-i) = \chi(-1)(Q)_{ij}$$

og 6 i propositionen giver, at da $v \equiv 3 \pmod 4$ er $\chi(-1) = -1$, dvs. at $Q^\top = -Q$.

Påstand. $QQ^\top = vI - J$

Den i,j'te indgang i $QQ^\top$ er givet ved

$$(QQ^\top)_{ij} = \sum_{k=1}^{v} \chi(k-i)\chi(k-j)$$

Hvis $i=j$ er $\chi(k-i)\chi(k-j) = 1$ for alle k undtagen når $k=i=j$. Så er $\chi(k-i)\chi(k-j) = 0$. Så

$$(QQ^\top)_{ii} = v-1$$

Hvis $i \neq j$ giver 5 i Proposition 3.3.5 på side 20 at

$$(QQ^\top)_{ij} = \sum_{k=1}^{v} \chi(k-i)\chi(k-j) = -1$$

Alt i alt har vi, at $QQ^\top = vI - J$.

Påstand. $BB^\top = (v+1)I - J$

Vi ved af ovenstående påstande, at $Q^\top = -Q$ og at $QQ^\top = vI - J$. Så hvis vi indsætter det i (3.3.3) får vi

$$BB^\top = vI - J + Q - Q + I = (v+1)I - J$$

Vi påstår nu, at vores ortogonale design X er en Hadamard Matrix af orden $2^t v$. Vi ved at $B^2 = BB^\top = (v+1)I - J$. Desuden ses det, at $J^2 = vJ$ og $(J-2I)^2 = (v-4)J + 4I$. Lad

os indsætte det i (3.3.2)

$$\begin{aligned}
XX^\top &= \Big(aJ^2 + b(J-2I)^2 + (2^t - a - b)B^2\Big) \times I_{2^t} \\
&= \Big(avJ + b((v-4)J + 4I) + (2^t - a - b)((v+1)I - J)\Big) \times I_{2^t} \\
&= \Big(\big[2^t(v+1) - a(v+1) - b(v-3)\big]I + \big[a(v+1) + b(v-3) - 2^t\big]J\Big) \times I_{2^t} \\
&= 2^t v I \times I_{2^t} \\
&= 2^t v I_{2^t v}
\end{aligned}$$

Undervejs udnyttede vi, at $a(v+1) + b(v-3) = 2^t$. Vi har nu, at $XX^\top = 2^t v I_{2^t v}$, og altså er X en Hadmard Matrix af orden $2^t v$. □

Lemma 3.3.7. *Lad $v \equiv 1 \pmod 4$ være et primtal, $v \geqslant 3$. Så findes en Hadamard Matrix af orden $2^t v$ for et passende t.*

Bevis. Dette bevis ligner meget beviset fra ovenfor, så vi vil nogen steder blot referere til argumenter til det bevis. Af Korollar 3.3.2 på side 19 får vi, at der findes $a, b, t \geqslant 0$ så (brug korrolaret med $a, b, t-1$)

$$a(v+1) + b(v-3) = 2^{t-1}$$

Af Korollar 3.2.4 på side 17 får vi, at der findes et ortogonalt design af type $(a, b, 2^t - a - b)$ af orden 2^{t-1} og punkt 2 i Lemma 3.2.2 på side 16 giver så, at der findes et ortogonalt designs, X af type $(2a, 2b, 2^t - a - b, 2^t - a - b)$ og orden 2^{t+1} på 4 kommuterende variable. Sæt nu disse variable til at være $v \times v$-matricerne J, $2I - J$, $Q - I$ og $Q + I$ hvor J er matricen med lutter et-taller, og hvor Q er givet som i beviset ovenfor.

Påstand. J, $2I - J$, $Q - I$ og $Q + I$ kommuterer indbyrdes.

I beviset ovenfor så vi, at $QJ = JQ = 0$, så J og Q kommuterer. Da I kommuterer med alle matricer har vi vist vores påstand. Da vi har 4 kommuterende variable har vi altså et ortogonalt design

$$XX^\top = \big[2aJ^2 + 2b(J-2I)^2 + (2^{t-1} - a - b)(Q-I)^2 + (2^{t-1} - a - b)(Q+I)^2\big] \times I_{2^{t-1}} \quad (3.3.4)$$

Vi påstår nu, at Q er symmetrisk. For af punkt 3 og 6 i Proposition 3.3.5 på side 20 får vi nu, at

$$(Q)_{ij} = \chi(j-i) = \chi(-1)\chi(i-j) = \chi(i-j) = (Q)_{ji}$$

I beviset for lemmaet ovenfor viste vi, at $QQ^\top = (v+1)I - J$, så det vil vi ikke gøre igen. Da $Q^2 = QQ^\top = vI - J$ har vi altså at $(Q-I)^2 + (Q+I)^2 = 2Q^2 - 2I = 2(v+1)I - J$. Vi ved ydermere at $J^2 = vJ$ og at $(J-2I)^2 = (v-4)J + 4I$ så vores ortogonale design X giver

$$\begin{aligned}
XX^\top &= \Big(2aJ^2 + 2b(J-2I)^2 + (2^{t-1} - a - b)(Q-I)^2 + (2^{t-1} - a - b)(Q+I)^2\Big) \times I_{2^t} \\
&= \Big(2avJ + 2b((v-4)J + 4I) + (2^{t-1} - a - b)(2(v+1)I - J)\Big) \times I_{2^t} \\
&= \Big(\big[2^t(v+1) - 2a(v+1) - 2b(v-3)\big]I + \big[2a(v+1) + 2b(v-3) - 2^t\big]J\Big) \times I_{2^t} \\
&= 2^t v I_{2^t v}
\end{aligned}$$

Undervejs benyttede vi, at $a(v+1) + b(v-3) = 2^{t-1}$. □

Lemma 3.3.8. *Der findes Hadamard Matricer af orden* $2, 2^t3, 2^t5, 2^t7$ *for* $t = 2$.

Bevis. Fås af Paley-konstruktion, se fx [5]. □

Sætning 3.3.9. *Lad* $v \in \mathbb{N}$. *Så findes et* t *afhængigt af* v, *således at der findes Hadamard Matricer af orden* $2^s v$ *for alle* $s \geqslant t$.

Bevis. Lad os bemærke, at med Lemma 3.3.3 på side 19 er det nok at vise, at der findes et t så vi har en Hadamard Matrix af orden $2^t v$.

Den finder vi vha. de tre foregående lemmaer, idet vi først primfaktoriserer v

$$v = p_1 \cdots p_n$$

og derefter benytter et af de tre foregående lemmaer på hver faktor. Det giver for hver primfaktor en Hadamard Matrix af størrelse $2^{t_i} p_i, i = 1, \ldots, n$, og til sidst kan vi så konstruere en Hadamard Matrix af orden $2^t v$ hvor $t = t_1 \cdots t_n$, vha. Lemma 3.3.3 på side 19. □

3.4 Hvorfor Seberry tager fejl

Ved dette punkt, begynder Seberry [2] at vurdere hvor stort t vi skal vælge, for at der findes Hadamard Matricer af størrelse $2^s v$ for $s \geqslant t$. Hun konkluderer på side 193 i [2], at hvis $v \equiv 1 \pmod 4$ og vi vælger $t = \lfloor 2 \log_2(v-3) \rfloor - 1$, giver lemma 9 i [2] en Hadamard Matrix af størrelse $2^{t+1} v$. Det påstår jeg er forkert. Lad os vise det ved et eksempel. Alle referencer til sider og sætninger i dette afsnit er til [2].

Lad $v = 13$. I korollar 7 skal vi vælge m, så

$$m = 2^j > \left(\frac{v+1}{d} - 1\right)\left(\frac{v-3}{d} - 1\right)$$

I dette tilfælde er $d = \gcd(14, 10) = 2$, så vi skal altså vælge j så

$$2^j > \left(\frac{14}{2} - 1\right)\left(\frac{10}{2} - 1\right) = 6 \cdot 4 = 24$$

Dvs at $j \geqslant 5$. Af theorem 6 i får vi så, at der findes $a, b \geqslant 0$ så

$$a\frac{14}{2} + b\frac{10}{2} = 2^5$$

og ved at gange igennem med 2 får vi

$$14a + 10b = 2^6$$

Læg mærke til, at vores to-potens bliver en større. I beviset for lemma 9 i bruger vi, at der findes $a, b \geqslant 0$ så $a(v+1) + b(v-3) = 2^t$ til at finde en Hadamard Matrix af størrelse $2^{t+1} v$, dvs i vores tilfælde en Hadamard Matrix af størrelse $2^7 \cdot 13$.

Seberry påstår i afsnit 6 i, at lemma 9 giver en Hadamard Matrix af størrelse $2^{t+1} \cdot 13$, hvor $t = \lfloor 2 \log_2(13-3) \rfloor - 1 = \lfloor 6.6438 \rfloor - 1 = 5$ – dvs en Hadamard Matrix af størrelse $2^6 \cdot 13$, hvilket altså er halvt så stor som det metoden reelt giver.

Denne fejl får faktisk hele beviset til at falde fra hinanden, idet vi nu for $v \equiv 1 \pmod 4$ får en Hadamard Matrix af størrelse $2^t v$ hvor $t = \lfloor 2\log_2(v-3) \rfloor + 1$, og multiplikativiteten ikke længere gælder, idet vi ikke kan lave følgende vurdering for 2 primtal $p, q \equiv 1 \pmod 4$:

$$\lfloor 2\log_2(p-3) \rfloor + 1 + \lfloor 2\log_2(q-3) \rfloor + 1 \leqslant \lfloor 2\log_2(pq-3) \rfloor + 1$$

Så vi kan ikke længere udvide resultatet fra primtal til alle tal vha. primfaktorisering.

Jeg har læst andre udgaver af beviset, men alle kommer med samme vurdering, som jeg vil påstå er forkert.

Vi er altså rendt i en temmelig alvorlig fejl i Seberrys argument. Vi kan dog stadig konstruere Hadamard Matricer af orden $2^t v$, for alle v hvor t afhænger af v, men den pæne vurdering af hvor stor et t vi skal vælge, er forsvundet. Jeg har skrevet en e-mail til Jennifer Seberry og beskrevet problemstillingen, men har endnu ikke modtaget noget svar. Et eventuelt svar vil havne på min hjemmeside http://home.imf.au.dk/jonas.

Litteratur

[1] R. E. A. C. Paley (1933), On orthogonal matrices, *J. Math. Phys.* ***12***, 311-320

[2] J. Seburry Wallis (1976), On the Existence of Hadamard Matrices, *J. Comb. Theory (A)* ***21***, 188-195

[3] A. V. Geramita & J. Seburry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*

[4] N. Lauritzen (2003), *Concrete Abstract Algebra*, Cambridge University Press, United Kingdom

[5] J. H. van Lint & R. M. Wilson (1999), *A Course In Combinatorics*, Cambridge University Press, United Kingdom

[6] Baumert, Golomb & Hall (1962), Discovery of an Hadamard matrix of order 92, *Bull.Amer. Soc.* ***68***, 237-238

[7] Daniel J. Acosta, *On The Frobenius Coin Problem: Collaborative Undergraduate Research*, http://maa.mc.edu/proceedings/spring2003/DanielAcosta.pdf

[8] M. Hall (1986), *Combinatorial Theory*, John Wiley & Sons inc., New York