universität innsbruck

Die Hadamard-Matrizen

Ben MERTENS, 11918801

Innsbruck, Juli 2023

Bachelorarbeit

eingereicht an der Universität Innsbruck, Fakultät für Mathematik, Informatik und Physik
zur Erlangung des akademischen Grades

Bachelor of Science (BSc)

Bachelorstudium Mathematik

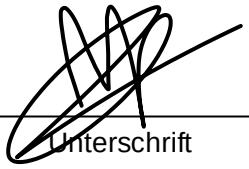
Betreuer:
Ass.-Prof. Dr. Fritz
Institut für Mathematik
Fakultät für Mathematik, Informatik und Physik

universität innsbruck

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt durch meine eigenhändige Unterschrift, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht.

Ich erkläre mich mit der Archivierung der vorliegenden Bachelorarbeit einverstanden.

15.07.2023	
Datum	Unterschrift

Inhaltsverzeichnis

1 Einleitung

1.1 Einführung

Die Hadamard-Matrizen sind nach dem französischen Mathematiker Jacques Hadamard (1865-1963) benannt. Es handelt sich dabei um $n \times n$ -Matrizen, wobei die Einträge alle entweder 1 oder -1 sind. Sie haben die Eigenschaft, dass sowohl alle Spalten als auch Zeilen orthogonal zueinander sind. Daraus folgt für eine Hadamard-Matrix H die Gleichung $H^T \cdot H = H \cdot H^T = n \cdot I$ welche auch als Definition von Hadamard-Matrizen verwendet werden kann, da sonst keine Matrix, deren Einträge nur 1 oder -1 sind, diese Gleichung erfüllt.

Anders ausgedrückt, eine quadratische $(+1, -1)$-Matrix ist Hadamard, wenn das innere Produkt zweier verschiedener Zeilen 0 ist.

1.2 Beispiel

Beispiele von Hadamard-Matrizen sind:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

Diese Matrizen wurden zunächst als Hadamard-Determinanten betrachtet.
Sie wurden so genannt, weil wenn $X = x_{ij}$ eine Matrix der Größe n ist, wobei $|x_{ij}| \leq 1$ für alle i und j, dann gilt $|\det X| \leq n^{n/2}$.

1.3 Eigenschaften

Wenn die Zeilen oder Spalten einer Hadamard-Matrix vertauscht werden, bleibt die Matrix Hadamard. Es ist auch wahr, dass die Hadamard-Eigenschaft erhalten bleibt, wenn eine Zeile oder Spalte mit -1 multipliziert wird. Es ist also immer möglich, die erste Zeile und die erste Spalte einer Hadamard-Matrix so anzuordnen, dass sie nur +1 Einträge enthalten. Eine Hadamard-Matrix in dieser Form wird als normalisiert bezeichnet.

1.4 Erklärung der Problemstellung

Seit anderthalb Jahrhunderten schon üben Hadamard-Matrizen eine Faszination auf uns aus. Sie sind einfach zu beschreiben, allgegenwärtig und nützlich, aber dennoch ist immer noch eine ganz einfache Frage ungeklärt: Für welche Größen existiert eine Hadamard-Matrix?

Es ist bekannt, dass es eine Hadamard-Matrix für die Größen 1 und 2 gibt, allerdings keine der Größe 3. Andererseits ist es noch ungelöst, ob für jede natürliche Zahl n eine Hadamard-Matrix der Größe 4n existiert. Es wird jedoch allgemein angenommen, dass dieses Problem bejaht werden kann, aber dennoch gibt es dazu immer noch keinen Beweis und es bleibt eines der großen ungelösten Probleme der Mathematik.

Hadamard-Matrizen sind für viele der möglichen Größen bekannt: die kleinste Größe, für die die Existenz einer Hadamard-Matrix in Frage steht, ist derzeit 668 (Eine Lösung für den bis dahin unbekannten Fall von 428 wurde von Kharaghani und Tayfeh-Rezaie im Juni 2004 bekannt gegeben).

Im täglichen Leben ist die praktische Anwendung der Hadamard-Matrizen weitgehend unsichtbar. Dennoch wird die Hadamard–Rademacher–Walsh-Transformation allgemein als schnelle diskrete Transformation verwendet (siehe Abschnitt 2.1). Fehlerkorrekturcodes (Reed-Muller-Codes), die in frühen Satellitenübertragungen verwendet wurden – zum Beispiel bei der Mariner-Mission zum Mars von 1972 (siehe Abschnitt 2.2) oder beim Vorbeiflug von äußeren Planeten im Sonnensystem - basieren auf Hadamard-Matrizen. Moderne CDMA-Mobiltelefone verwenden Hadamard-Matrizen (Walsh-Abdeckungen), um die Übertragung auf der Uplink-Verbindung zu modulieren und Beeinträchtigungen mit anderen Übertragungen zur Basisstation zu minimieren.

Neue Anwendungen sind überall um uns herum, zum Beispiel in der Bildmustererkennung, den Neurowissenschaften, der optischen Nachrichtenübertragung oder dem Schützen von Daten. Trotz all dieser Informationen gibt es noch keine einheitliche Technik zur Konstruktion aller bekannten Hadamard-Matrizen.

2 Anwendungen

2.1 Hadamard-Transformation

Die Hadamard–Rademacher–Walsh-Transformation, oder kurz Hadamard-Transformation ist eine diskrete Transformation aus dem Bereich der Fourier-Analysis. Sie ist benannt nach den Mathematikern Jacques Hadamard, Joseph L. Walsh und Hans Rademacher.

Die Hadamard-Transformation H_m wird aus einer $2^m \times 2^m$-Hadamard-Matrix, skaliert mit einem Normalisierungsfaktor, gebildet, welche eine Eingangsfolge (x_n) der Länge 2^m von reellen Zahlen mittels einer Matrix-Vektor-Multiplikation in eine Ausgangsfolge (X_k) der Länge 2^m von reellen Zahlen transformiert.

2.1.1 Rekursive Transformation

Rekursiv definieren wir die 1×1 Hadamard-Transformation H_0 durch die Identität $H_0 = 1$ und definieren dann H_m für $m > 0$ durch $H_m = \frac{1}{\sqrt{2}} \begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix}$ wobei das $\frac{1}{\sqrt{2}}$ eine Normierung ist, die manchmal weggelassen wird.

Für $m > 1$ können wir H_m definieren als: $H_m = H_1 \otimes H_{m-1}$ wobei $\otimes$ das Kronecker-Produkt bezeichnet. Abgesehen von diesem Normalisierungsfaktor bestehen die Hadamard-Matrizen also ausschließlich aus 1 und -1.

2.1.2 Binäre Darstellung der Indizes n und k

Äquivalent dazu können wir die Hadamard-Matrix durch ihren (k, n)-ten Eintrag definieren, indem wir schreiben

$$k = \sum_{i=0}^{m-1} k_i 2^i = k_{m-1}2^{m-1} + k_{m-2}2^{m-2} + ... + k_1 2 + k_0$$

$$n = \sum_{i=0}^{m-1} n_i 2^i = n_{m-1}2^{m-1} + n_{m-2}2^{m-2} + ... + n_1 2 + n_0$$

wobei k_j und n_j die Bitelemente (0 oder 1) von k bzw. n sind. Zu beachten ist, dass für das Element in der linken oberen Ecke gilt: $k = n = 0$.
In diesem Fall haben wir: $(H_m)_{k,n} = \frac{1}{2^{m/2}}(-1)^{\sum_j k_j n_j}$

2.1.3 Beispiel

$$H_0 = (1) \qquad H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$(H_n)_{i,j} = \frac{1}{2^{n/2}}(-1)^{i \cdot j}$ wobei $i \cdot j$ das bitweise Punktprodukt der binären Darstellungen der Zahlen i und j ist. Wenn zum Beispiel $n \geq 2$, dann

$$(H_n)_{3,2} = (-1)^{3 \cdot 2} = (-1)^{(1,1) \cdot (1,0)} = (-1)^{1+0} = (-1)^1 = -1$$

Das stimmt mit dem obigen überein (ohne Berücksichtigung der Konstante). Zu beachten ist, dass das Element der ersten Zeile und der ersten Spalte der Matrix mit $(H_n)_{0,0}$ bezeichnet wird.

2.2 Anwendung in der Raumfahrt

2.2.1 Einleitung

Die Mariner 9-Mission der NASA ist am 30. Mai 1971 gestartet und am 14. November 1971 angekommen. Das Ende der Mission war am 27. Oktober 1972.

Bei der Mariner 8-Mission wurde 70% der Marsoberfläche kartiert. Das Ziel bei der Mariner 9-Mission war die Untersuchung zeitlicher Veränderungen in der Marsatmosphäre und dessen Oberflächeneigenschaften.

Dabei wurde eine Schwarz-Weiß-Fernsehkamera verwendet, um "Live" Bilder von der Marsoberfläche zu senden.

Das Problem ist dabei die Übermittlung von Nachrichten. Genauer gesagt, wir möchten eine Nachricht übermitteln und wissen, dass während der Übertragung schwache Signale, sporadische Stromstöße und andere natürlich auftretende Störungen die Übermittlung stören werden. Wir wollen sicherstellen, dass die beabsichtigte Nachricht (unsere ursprüngliche Übertragung) aus dem rekonstruierbar ist was auch immer tatsächlich empfangen wird.

2.2.2 Der Reed-Muller-Code

Bei der NASA Raumsonde Mariner 9 bestehen die Daten aus binären 6-Tupeln ($2^6 = 64$ Graustufen) und die Übertragungsbeschränkungen lassen eine Kodierung zu, die die übertragenen Wörter auf etwa 30 Bit verlängern würde. Der gewählte Code ist ein Reed-Muller-Code.

Dieser gehört zur Familie von linearen, fehlerkorrigierenden Codes, die im Bereich der Kanalcodierung zur gesicherten Datenübertragung und Datenspeicherung verwendet werden. Diese Klasse von Codes wurden von Irving S. Reed und David E. Muller entwickelt. In der Praxis wurde dieser Code von der Nasa in den Mariner Expeditionen zum Mars benutzt, um die vom Mars gemachten Fotos an die Erde zu senden. Dabei sind die Codewörter 32 Bits lang und insgesamt gibt es $2^6 = 64$ von ihnen. Die Codewörter sind die Zeilen von zwei 32×32 Hadamard-Matrizen (eine die Negation der anderen).

Um diesen Code verstehen zu können, müssen wir hier ein paar Fachbegriffe einfügen:

2.2.3 Satz: Fehlerkorrektur

Die Fähigkeit eines Codes, Fehler zu korrigieren, steht in direktem Zusammenhang mit dem "Abstand" zwischen den Codewörtern.
Wir werden dieses Konzept im Folgendem weiter präzisieren.

2.2.4 Definition: Blockcodes

$V(n, k)$ = Die Blockcodes sind Teilmengen der Menge aller n-Tupel, deren Einträge aus einem Alphabet der Größe k stammen. Wir bezeichnen diese große Menge mit $V(n, k)$.

2.2.5 Der Hamming-Abstand

Die Anzahl der Stellen zwischen zwei Wörtern in $V(n, k)$ an denen sie sich unterscheiden.

Beispiel In $V(4, 4)$ haben die Wörter (0,1,2,3) und (1,1,2,2) Abstand 2. Dieser Hamming-Abstand ist eine Metrik.

2.2.6 Der Mindestabstand von einem Code

Der Mindestabstand von einem Code C ist der kleinste Abstand zwischen einem beliebigen Paar verschiedener Codewörter. Es ist der minimale Abstand eines Codes, der die Fehlerkorrekturfähigkeit eines Codes misst. Wenn der Mindestabstand eines Codes C gleich $2e + 1$ beträgt, dann ist C ein $2e$-Fehlererkennungscode, da $2e$ oder weniger Fehler in einem Codewort nicht in ein anderes Codewort gelangen und ist ein e-fehlerkorrigierender Code, da, wenn e oder weniger Fehler in einem Codewort auftreten, das resultierende Wort näher am ursprünglichen Codewort liegt als an jedem anderen Codewort und daher dann korrekt decodiert werden kann.

Beispiel Im 5-Wiederholungs-Code von $V(5, 4)$ (Codewörter: 00000, 11111, 22222, und 33333) beträgt der Mindestabstand 5. Der Code erkennt 4 oder weniger Fehler und korrigiert 2 oder weniger Fehler.

Der Reed-Muller-Code hat also die Paramater (32, 6, 16), damit werden 32 Bit lange Codewörter übertragen, die $2^6 = 64$ Werte kodieren, wobei die Codewörter untereinander einen Hamming-Abstand von 16 aufweisen. Diese Parameter wurden aufgrund der Kanalcharakteristik, der Bildauflösung und der Aufnahme- und Übertragungszeiten gewählt, die eine Wortlänge von 30 Bit sinnvoll machten.

Aus den Eigenschaften einer Hadamard-Matrix sehen wir, dass zwei unterschiedliche Zeilen der Matrix sich in genau der Hälfte ihrer Positionen unterscheiden (da das Skalarprodukt 0 ist). Wenn wir eine der zwei Zeilen nehmen und alle ihre Elemente negieren, ändert sich das Skalarprodukt nicht, so dass sich die beiden Zeilen wiederum in genau der Hälfte ihrer Elemente unterscheiden. Der Mindestabstand zwischen diesen Zeilen ist also die Hälfte der Länge der Zeilen.

In unserem Fall sind die Codewörter die Zeilen von zwei 32×32 Hadamard-Matrizen (eine die Negation der anderen), so dass der Mindestabstand 16 beträgt.
Der Code erkennt also 15 oder weniger Fehler und korrigiert 7 oder weniger Fehler (7-fehlerkorrigierender Code).

2.2.7 Die Kodierung

Da es 64 Codewörter und 64 Datentypen gibt, funktioniert jede Zuordnung von Code-Wort zum Datentyp, aber die Anforderung, dass die Kodierung keinen Speicherplatz benötigen soll, bedeutet, dass eine beliebige Zuweisung nicht ausreichen wird.
Die Verwendung von Hadamard-Matrizen macht den Code zu einem 6 dimensionalen Vektorraum, so dass es eine Basis mit 6 Elementen gibt (jede Linearkombination davon ergibt ein Codewort). Der Datentyp mit 6-Tupel wird verwendet, um die Koeffizienten für die Linearkombination der Basisvektoren bereitzustellen. Somit wird jedem Datentyp ein eindeutiges Codewort zugeordnet. Diese einfache Berechnung kann fest fixiert werden und erfordert nur einen sehr geringen Speicherplatz.

2.2.8 Die Dekodierung

Der Code hat einen sehr schnellen Dekodierungsalgorithmus, den wir jetzt beschreiben werden.
Zunächst werden alle Codewörter (und der empfangene Vektor) in ± 1 Vektoren umgewandelt, indem die 0 in -1 umgeschrieben wird. Wir nehmen das Skalarprodukt des empfangenen Vektors mit jedem der Codewörter. Sobald das Ergebnis 16 oder größer ist, dekodieren wir es als dieses Codewort.

Angenommen, bei der Übertragung sind keine Fehler aufgetreten. Dann ist das Skalarprodukt des empfangenen Vektors mit sich selbst 32 und mit jedem anderen anderen Codewort gleich 0 oder -32.

Daraus folgt, dass der Abstand zwischen zwei Codewörtern das Gewicht ihrer Differenz (die ein weiteres Codewort ist) und somit entweder 0, 16 oder 32 ist. Bei 0 sind die Codewörter identisch. Bei 32, haben die Codewörter keine gemeinsame Komponente und das Skalarprodukt der ± 1 Form ist dann -32. In allen anderen Fällen sind 16 Stellen gleich und 16 Stellen sind unterschiedlich, was ein Skalarprodukt von $16-16=0$ ergibt.

Für jeden Fehler, der auftritt, verringert sich das Skalarprodukt um 2 (oder wird bei einem fehlerhaften Codewort um 2 erhöht). Wenn nicht mehr als 7 Fehler auftreten, verringert sich das Skalarprodukt mit dem richtigen Codewort auf mindestens 18 und das Skalarprodukt mit den falschen Codewörtern erhöht sich auf höchstens 14, so dass eine korrekte Dekodierung erfolgt. Wenn 8 oder mehr Fehler auftreten, ergeben sich Skalarprodukte von mindestens 16 und eine korrekte Dekodierung ist nicht möglich.

3 Nachweis der Hadamard-Matrixgrößen

3.1 Satz: Die Größeneigenschaften von Hadamard-Matrizen

Die Größe einer Hadamard-Matrix ist entweder 1, 2 oder durch 4 teilbar.

Beweis:
$\begin{pmatrix} 1 \end{pmatrix}$ ist eine Hadamard-Matrix der Größe 1 und $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ hat die Größe 2.

Nehmen wir nun an, H sei eine Hadamard-Matrix der Größe $h > 2$.
Wir normalisieren H und ordnen die ersten drei Zeilen so um, dass sie wie folgt aussehen:

$+1 \ldots +1$	$+1 \ldots +1$	$+1 \ldots +1$	$+1 \ldots +1$
$+1 \ldots +1$	$+1 \ldots +1$	$-1 \ldots -1$	$-1 \ldots -1$
$+1 \ldots +1$	$-1 \ldots -1$	$+1 \ldots +1$	$-1 \ldots -1$
x	y	z	w

Dabei sind x, y, z, w die Anzahl der Spalten jedes Typs. Da die Größe h ist, muss gelten dass $x + y + z + w = h$ ist. Wenn man jetzt die inneren Produkte der Zeilen 1 und 2, 1 und 3 und 2 und 3 nimmt, erhält man:

$$\begin{aligned} x + y - z - w &= 0 \\ x - y + z - w &= 0 \\ x - y - z + w &= 0 \end{aligned}$$

Wenn wir dieses Gleichungssystem lösen, kriegt man $x = y = z = w = \frac{h}{4}$.
Die ganze Zahl h muss also durch 4 teilbar sein.

□

4 Konstruktionsmethoden

4.1 Konstruktion von Hadamard-Matrizen mit dem Kronecker-Produkt

Es gibt sehr viele Konstruktionsmethoden für Hadamard-Matrizen, wir betrachten hier nun eine der einfachsten, nämlich die Konstruktion mit dem Kronecker-Produkt. Gegeben sind Hadamard-Matrizen $H_1 = |h_{ij}|$ der Ordnung $m \times n$ und H_2 der Ordnung $p \times q$. Das Kronecker-Produkt $H_1 \otimes H_2$ ist dann eine $mp \times nq$ Matrix:

$$\begin{pmatrix} h_{11}H_2 & \dots & h_{1n}H_2 \\ \dots & \dots & \dots \\ h_{m1}H_2 & \dots & h_{mn}H_2 \end{pmatrix}$$

Seien also H_1 und H_2 zwei Hadamard-Matrizen, dann ergibt das Kronecker-Produkt wieder eine Hadamard-Matrix.

4.1.1 Beispiel

$$H_1 = H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Die Konstruktion ergibt dann:

$$H_1 \otimes H_2 = \begin{pmatrix} 1 \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & 1 \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ 1 \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} & -1 \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Das erlaubt uns also, immer größere Hadamard-Matrizen aus kleineren zu konstruieren. Wenn nämlich ihre Ordnungen jeweils n_{H_1} und n_{H_2} sind, ergibt das Kronecker-Produkt eine Hadamard-Matrix der Ordnung $n_{H_1} \cdot n_{H_2}$.

4.2 Konstruktion von Sylvester

Der englische Mathematiker James Joseph Sylvester studierte auch die Hadamard-Matrizen und erfand dabei eine Konstruktion die später nach ihm benannt wurde. Dabei handelt es sich um einen Spezialfall von der ersten Konstruktion (Konstruktion von Hadamard-Matrizen mit dem Kronecker-Produkt), wenn man diese nämlich wiederholt anwendet, kriegt man die Konstruktion von Sylvester.

Er erkannte dass man immer eine Hadamard-Matrix konstruieren kann wenn ihre Ordnung eine Potenz von 2 ist. Mit anderen Worten, bei einer beliebigen ganzen Zahl $k \geq 1$ können wir sicher sein, dass es eine Hadamard-Matrix der Ordnung $n = 2^k$ gibt.

Dies zeigt insbesondere, dass es unendlich viele Hadamard-Matrizen gibt. Sie können so groß werden, wie wir wollen. Genau das werden wir jetzt kurz zeigen:

Für den Fall $k = 0$ kriegen wir einfach $H_1 = (1)$, also eine Hadamard-Matrix der Ordnung $n = 2^0 = 1$.
Für $k = 1$ gilt $n = 2$, dementsprechend können wir H_2 schreiben als $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Im Allgemeinen kann also eine Hadamard-Matrix der Ordnung $n = 2^k$ rekursiv konstruiert werden, wenn eine kleinere Hadamard-Matrix der Ordnung $n = 2^{k-1}$ bekannt ist.

Es gilt also[1]: $H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix}$

So kriegt man dann auch ganz einfach die Hadamard-Matrix der Ordnung:

$$n = 2^2 = 4\text{: } H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Eine Möglichkeit zur Konstruktion einer Hadamard-Matrix der Ordnung $n = 2^k$ besteht darin, das Kronecker-Produkt von zwei Hadamard-Matrizen, $H_{2^{k-1}}$ und H_2, zu verwenden. Durch die Kombination dieser Matrizen lässt sich eine Hadamard-Matrix $H_2 \otimes H_{2^{k-1}}$ der Ordnung $n = 2 \times 2^{k-1} = 2^k$ erzeugen.

[1] Unterkapitel 2.1.1 Rekursive Transformation

4.3 Konstruktion von Paley

Der englische Mathematiker Raymond Paley hat eine Methode entwickelt um Hadamard-Matrizen zu konstruieren, deren Ordnung vom Typ $n = p^k + 1$ ist, wobei p eine Primzahl und $k > 0$ eine ganze Zahl ist.

Wir wissen bereits dass jede Ordnung $n > 2$ von einer Hadamard-Matrix durch 4 teilbar sein muss.
Diese Bedingung kann mathematisch wie folgt geschrieben werden: $p^k + 1 \equiv 0(\text{mod}4)$. Mit GF($p^k$) haben wir einen endlichen Körper der Ordnung p^k. Da er endlich ist, können wir alle p^k auflisten als Elemente a_i. Für $k = 1$ stimmen diese Elemente dann mit der Menge $\{0,1,\ldots,p-1\}$ überein. Im endlichen Körper GF(p^k) wird eines seiner Elemente b als zweite Potenz bezeichnet, wenn es ein a gibt so dass $a \times a = b$.

Beispiel: In GF(7) ist 2 eine zweite Potenz da $4 \times 4 \equiv 2(\text{mod}7)$.

Nun definieren wir folgende Funktion χ:

$$\chi(y) = \begin{cases} 0, & \text{wenn} \quad y = 0 \\ +1, & \text{wenn} \quad y \neq 0 \quad \text{ist eine zweite Potenz} \\ -1, & \text{wenn} \quad y \neq 0 \quad \text{ist keine zweite Potenz} \end{cases}$$

Nun können wir diese Informationen zusammenfassen, indem wir eine Matrix Q mit der Ordnung p^k konstruieren, so dass $Q_{i,j} = \chi(a_i - a_j)$ ist. Um H_{p^k+1} zu erhalten, benötigen wir eine weitere Zeile und Spalte und müssen die 0-wertigen Einträge irgendwie loswerden. Dies lässt sich in zwei Schritten machen:

1) Mit der Hilfe einer Spalte, die mit Einsen entlang ihrer p^k Einträge aufgefüllt wird, konstruieren wir S, eine quadratische Matrix der Ordnung $n = p^k + 1$ mit

$$S = \begin{pmatrix} 0 & 1^T \\ -1 & Q \end{pmatrix}$$

2) Aus S enthalten wir schließlich eine Hadamard-Matrix $H_{p^k+1} = S + I$ wobei I die Einheitsmatrix der Ordnung $p^k + 1$ ist.

Paley hat hier allerdings nicht aufgehört, er hat auch Konstruktionen für die Ordnungen $n = 2(p^k + 1)$ entwickelt, solange $p^k + 1 \equiv 2(\text{mod}4)$ gilt. GF(p^k) kann immer noch wie zuvor verwendet werden (zusammen mit den zugehörigen Matrizen Q und S). Der letzte Schliff kommt mit einer etwas anderen Note und zwar gilt dann:

$$H_{2(p^k+1)} = S \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} + I \otimes \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

Beispiel: Wir wollen eine 8×8 Hadamard-Matrix H_8 mit der Paley-Methode erstellen.

Dies erfordert die Arbeit mit GF(7) (d.h $p = 7$ und $k = 1$). Wir beginnen mit der Aufzählung der Elemente, sei $a_1 = 0, a_2 = 1, \ldots, a_7 = 6$.

Zunächst müssen wir in GF(7) die zweiten Potenzen durch Anwendung von χ ermitteln: Nun, per Definition gilt $\chi(0) = 0$ und für den Rest folgt: da $1 \equiv 1^2 (\text{mod} 7)$,
$2 \equiv 4^2 (\text{mod} 7)$ und $4 \equiv 2^2 (\text{mod} 7)$ sind 1,2 und 4 jeweils zweite Potenzen und somit gilt $\chi(1) = \chi(2) = \chi(4) = 1$.
Die restlichen Elemente sind keine zweite Potenzen, also gilt $\chi(3) = \chi(5) = \chi(6) = -1$.

Dabei ist zu beachten dass die gleiche zweite Potenz auf zwei Arten erhalten werden kann, zB: $1 = 1^2 = 6^2$. Wir können nun damit beginnen, unsere (7×7) Matrix Q zu füllen:

$$Q = \begin{pmatrix} \chi(0-0) & \ldots & \chi(0-6) \\ \ldots & \ldots & \ldots \\ \chi(6-0) & \ldots & \chi(6-6) \end{pmatrix}$$

Wir haben gerade χ für positive Argumente gerechnet und damit den unteren Teil von Q gebildet. Für negative Argumente (und den entsprechenden oberen Teil) berechnen wir einfach ihre Restklasse modulo 7: $-1 = 6, -2 = 5, -3 = 4, -4 = 3, -5 = 2$ und $-6 = 1$. Dann gilt:

$$Q = \begin{pmatrix} 0 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 0 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 0 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 0 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 0 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{pmatrix}$$

Nun erhalten wir S indem wir -1 zur ersten Spalte und 1 zur ersten Zeile hinzufügen.

$$S = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 0 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 0 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 0 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 0 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 0 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 0 \end{pmatrix}$$

Zum Schluss fügen wir noch Einser in der Diagonale ein und erhalten H_8:

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{pmatrix}$$

Somit haben wir gerade eine Hadamard-Matrix der Ordnung $n = 8 = 7^1 + 1$ erzeugt. Zu beachten ist dass $8 = 2^3$ und somit die Konstruktion von Sylvester auch funktionieren würde.

4.3.1 Beweis

Aussage:
Bei der Konstruktion von Paley handelt es sich um Hadamard-Matrizen

Wir wollen zeigen dass die Matrix $H_{p^k+1} = S + I$, wobei I die Einheitsmatrix der Ordnung $p^k + 1$ ist, tatsächlich eine Hadamard-Matrix ist.

Also müssen wir zwei Eigenschaften überprüfen:

1) Alle Einträge sind entweder +1 oder -1

2) Jede Zeile und jede Spalte ist orthogonal zu jeder anderen Zeile und jeder anderen Spalte

Wir prüfen zuerst die erste Eigenschaft: Die Matrix Q der Ordnung p^k besteht aus den Einträgen der Funktion χ angewendet auf die Differenzen zwischen den Elementen in GF(p^k), also $Q_{i,j} = \chi(a_i - a_j)$. Somit sind die Einträge von Q alle entweder $+1$,-1 oder 0. Dabei ist zu bemerken, dass $\chi(y)$ genau dann 0 ergibt, wenn $y = 0$ gilt. Also ist der Eintrag $Q_{i,j} = 0$ wenn $i = j$ gilt, also immer genau auf der Diagonalen der Matrix Q. Nun wissen wir also, dass die Matrix Q überall $+1$ und -1 Einträge hat, außer auf der Diagonalen.

Die Matrix S der Ordnung $p^k + 1$ ist definiert als $S = \begin{pmatrix} 0 & 1^T \\ -1 & Q \end{pmatrix}$.

Also sind die Elemente von S auch alle entweder $+1$,-1 oder 0. Da Q auf der Diagonalen nur 0-Einträge hat, hat also die Matrix S überall $+1$ oder -1 Einträge, außer auf der Diagonalen ($= 0$).

Die Einheitsmatrix I besteht aus Einsen auf der Diagonalen und Nullen sonst. Das heißt also, dass wenn wir $S + I$ addieren, die Null Elemente auf der Diagonalen von S durch die $+1$ Elemente auf der Diagonalen von I ersetzt werden. Damit hat $H_{p^k+1} = S + I$ nur noch $+1$ und -1 Einträge und somit ist die erste Eigenschaft überprüft.

Nun betrachten wir die orthogonale Eigenschaft der Zeilen von H_{p^k+1}.

Die Matrix Q besteht aus Einträgen der Funktion χ angewendet auf die Differenzen zwischen den Elementen in $\mathrm{GF}(p^k)$. Die Eigenschaft[1] $\sum_b \chi(b) \cdot \chi(b + c) = -1$ für $b \in \mathrm{GF}(p^k)$ und $c \neq 0$ ermöglicht es uns zu zeigen, dass das Skalarprodukt zwischen verschiedenen Zeilen von Q gleich -1 ist. Das bedeutet, dass die Zeilen von Q nicht orthogonal zueinander sind.
Um die Orthogonalität der Zeilen von $H_{p^k+1} = S + I$ zu erreichen, fügen wir der ersten Spalte von Q den Wert -1 hinzu und der ersten Zeile den Wert 1. Dadurch erhalten wir die Matrix S, deren Zeilen orthogonal zueinander sind.

Die Matrix H_{p^k+1} erhält man, indem man die beiden Matrizen S und I addiert. Dadurch werden die Null Elemente auf der Diagionalen von S durch die $+1$ Elemente auf der Diagonalen von I ersetzt.

Schauen wir uns diese Vorgehensweise am vorherigen Beispiel der Konstruktion einer 8×8 Hadamard-Matrix H_8 an. Wir betrachten z.B. die Zeilen 2 und 3 der Matrix S. Indem man I addiert, wird der Eintrag 0 an der Stelle $(2, 2)$ und $(3, 3)$ zu $+1$. Aber es ändert sich nichts am Skalarprodukt der Zeilen 2 und 3 da sich die beiden veränderten Einträge gegenseitig wegkürzen $(1 \cdot 1 + (-1) \cdot 1 = 1 - 1 = 0)$.
Somit bleiben die Zeilen 2 und 3 von S auch nach addieren von I orthogonal zueinander.

Im allgemeinen Fall kann man das durch die Eigenschaften der Funktion χ beschreiben. Wir wissen bereits, dass für die Ordnung n gelten muss, dass $n = p^k + 1 \equiv 0(\mathrm{mod}4)$ und mit $\mathrm{GF}(p^k)$ haben wir einen endlichen Körper der Ordnung p^k.

Wir zeigen den allgemeinen Fall der Orthogonalität der Zeilen von H_{p^k+1} mithilfe des verallgemeinerten Euler-Kriteriums und leiten die relevante Eigenschaft der Funktion χ ab.

Das verallgemeinerte Euler-Kriterium besagt, dass für ein beliebiges Element $a \in \mathrm{GF}(p^k)$ mit einer ungeraden Primzahl p und einer ganzen Zahl $k \geq 1$ ein Element $x \in \mathrm{GF}(p^k)$ existiert, sodass $a = x^2$ in $\mathrm{GF}(p^k)$, genau dann wenn $a^{(p^k-1)/2} = 1$ in $\mathrm{GF}(p^k)$.

Wir wollen nun zeigen dass die Gleichung $\chi(-a) = -\chi(a)\ \forall a \in \mathrm{GF}(p^k)$ gilt.

Zunächst setzen wir in das verallgemeinerte Euler-Kriterium ein und erhalten dass $\chi(-a) = (-a)^{(p^k-1)/2}$ und $\chi(a) = a^{(p^k-1)/2}$ ist.

[1] Marshall Hall Jr *Combinatorial Theory*, 1976, Lemma 14.1.1.

Wir müssen also zeigen dass $(-a)^{(p^k-1)/2} = -a^{(p^k-1)/2}$ gilt.

Also gilt es zu überprüfen ob der Exponent $(p^k-1)/2$ ungerade ist. Beim vorherigen Beispiel[1] für $p = 7$ und $k = 1$ ist der Exponent ungerade und es gilt $\chi(-a) = -\chi(a)$. Ein weiters Beispiel wäre für $p = 5$ und $k = 1$, allerdings ist dann der Exponent gerade und somit ist die Gleichung nicht mehr erfüllt. Deswegen haben wir bei der Konstruktion von Paley noch die zusätzliche Bedingung, dass für die Ordnung n gelten muss dass $n = p^k + 1 \equiv 0(\text{mod}4)$. Wenn man diese Bedingung auf unseren Exponenten anwendet, muss also $p^k - 1 \equiv 2(\text{mod}4)$ gelten.

Wegen dieser Bedingung folgt dann dass der Exponent $(p^k-1)/2$ immer ungerade ist. Somit gilt die Gleichung $\chi(-a) = -\chi(a)\ \forall a \in \text{GF}(p^k)$.
Aus dieser Gleichung können wir schlussfolgern, dass bei der Konstruktion von Paley auch $\chi(a-b) = -\chi(b-a)\ \forall a, b \in \text{GF}(p^k)$ gilt, daraus folgt also dass beim Skalarprodukt der verschiedenen Zeilen die Einträge in der Matrix sich selbst wegkürzen. Insofern folgt die gewünschte Symmetrie der Zeilen und somit ist jede Zeile orthogonal zu jeder anderen Zeile. Die Orthogonalität der Spalten gilt dann per Definition von orthogonalen Matrizen automatisch.

Nachdem wir nun die beiden Eigenschaften überprüft haben können wir schlussfolgern dass die Matrix H_{p^k+1} tatsächlich eine Hadamard-Matrix ist.

□

[1] Beispiel Seite 12

5 Gruppentheoretische Aspekte von Hadamard-Matrizen

5.1 Erinnerung an die Gruppentheorie

Eine Gruppe ist ein Paar $(G, *)$,wobei G eine Menge ist und $*$ eine Verknüpfung darstellt. Dabei gilt die Abbildung $* : G \times G \to G, (a, b) \mapsto a * b$. Damit $(G, *)$ als Gruppe bezeichnet werden kann, muss die Verknüpfung assoziativ sein, ein neutrales Element und inverse Elemente besitzen.
Die Gruppe $(G, *)$ heißt abelsch, falls zusätzlich noch die Kommutativität erfüllt ist.

5.2 Verbindung zur Gruppentheorie

5.2.1 Einführung in kozyklische Hadamard-Matrizen

Viele Codes und Sequenzen, die für eine robuste oder sichere Kommunikation entwickelt wurden, werden aus Hadamard-Matrizen aufgebaut. Dabei werden die -1 Einträge zu Nullen umgewandelt und somit besteht das Alphabet nur noch aus $\{0, 1\}$.

In dieser Einführung beschreiben wir den notwendigen Hintergrund zu Kozykeln und ihren Eigenschaften. Außerdem stellen wir die aktuellen Ergebnisse zur Theorie der kozyklischen Hadamard-Matrizen und ihre Anwendungen in dem Bereich der Fehlerkorrekturcodes dar.

Wir befassen uns hier nur mit 2-Koykeln, obwohl n-Kozykel auf endlichen Gruppen für jedes $n \geq 1$ definiert sind. Der Schwerpunkt liegt auf der Darstellung von 2-Kozykeln als zweidimensionale Matrizen mit interner Struktur; die höherdimensionalen Matrizen, die höheren Kozykeln entsprechen, werden nicht betrachtet.

Später untersuchen wir die Auswirkungen der Einführung einer kombinatorischen Eigenschaft, die wir als Orthogonalität bezeichnen, auf Kozykel. Dies ist die Eigenschaft, die ein Kozykel haben muss, wenn er eine kozyklische Hadamard-Matrix hervorbringen soll. Leider bleibt die Orthogonalität bei der natürlichen Äquivalenzoperation, der Kohomologie, auf Zyklen nicht erhalten, was die Effektivität der Suche nach orthogonalen Kozyklen in der Gruppe der Kozyklen bisher eingeschränkt hat. Deswegen gibt es seit kurzem eine stärkere Äquivalenzbeziehung, die sogenannte Verschiebungsäquivalenz die die Orthogonalität bewahrt. Dies wird angewendet, um eine Korrespondenz zwischen "Bündeln" orthogonaler Kozykel und Äquivalenzklassen kozyklischer Hadamard-Matrizen herzustellen.

5.2.2 Kozykel

Sei G eine endliche Gruppe und C eine endliche abelsche Gruppe. Ein Kozykel ist eine Abbildung $\psi : G \times G \to C$, die die Kozykel-Gleichung erfüllt:

$$\psi(g,h)\psi(gh,k) = \psi(g,hk)\psi(h,k)$$

Ein auf $G \times G$ definierter Kozykel ψ wird als eine G-kozyklische Matrix dargestellt d.h. eine quadratische Matrix, deren Zeilen und Spalten durch die Elemente von G unter einer bestimmten Ordnung angegeben sind und deren Eintrag an der Position (g,h) gleich $\psi(g,h)$ ist. Wir schreiben $M_\psi = [\psi(g,h)]_{g,h\in G}$.

Beispiel:
Wenn $G = (\mathbb{Z}_2)^n$ mit Kennzeichnung durch die binäre Darstellung der ganzen Zahlen $\{0,\ldots,2^n-1\}$ und $C = \mathbb{Z}_2$ gegeben ist, dann ist $\psi(u,v) = (-1)^{u\cdot v}$, für alle $u,v \in G$ ein Kozykel und M_ψ ist die Sylvester-Hadamard Matrix[1] der Ordnung 2^n.

5.2.3 Eigenschaften von Kozykeln und kozyklischen Matrizen

Man beachte, dass $h = 1$ in der Kozykel-Gleichung bedeutet, dass $\psi(g,1) = \psi(1,k) = \psi(1,1), \forall g,k \in G$. Wir folgen dem üblichen Gebrauch und nehmen von nun an an, dass ψ normalisiert ist, d.h. $\psi(1,1) = 1$. Folglich kann die Matrix M_ψ so geschrieben werden, dass die erste Zeile und die erste Spalte alle 1en sind.

Definition:
Ein Kozykel ψ ist symmetrisch, wenn $\psi(g,h) = \psi(h,g)\ \forall g,h \in G$.
Äquivalent dazu ist M_ψ eine symmetrische Matrix.

Anmerkung:
Für jedes G und C bildet die Menge der Kozykeln eine abelsche Gruppe $\mathbb{Z}^2(G,C)$ unter punktweiser Multiplikation.

[1] Kapitel 4.2 Konstruktion von Sylvester

5.2.4 Orthogonale Kozykeln und ihre Äquivalenzen

Definition:
Ein Kozykel $\psi : G \times G \to \mathbb{Z}_2$ ist orthogonal, wenn für jedes $g \neq 1 \in G$ gilt:

$$|\{h \in G : \psi(g,h) = \pm 1\}| = |G|/2$$

oder äquivalent dazu, wenn im Gruppenring $\mathbb{Z}[\mathbb{Z}_2]$ für jedes $g \neq 1 \in G$ gilt:

$$\sum_{h \in G} \psi(g,h) = \frac{|G|}{2} \cdot e \quad \text{für} \quad e \coloneqq (+1) + (-1) \in \mathbb{Z}[\mathbb{Z}_2]$$

Satz:
Die Definition der kozyklischen Orthogonalität ist eine äquivalente Formulierung der Bedingung, dass die kozyklische G-Matrix M_ψ eine Hadamard-Matrix ist.

Beweis:
Wir wollen zeigen dass die kozyklische G-Matrix M_ψ eine Hadamard-Matrix ist.

Um zu beweisen, dass die kozyklische G-Matrix M_ψ eine Hadamard-Matrix ist, zeigen wir, dass alle Einträge entweder +1 oder -1 sind und dass alle Zeilen und Spalten orthogonal zueinander sind.

Die Gruppe $\mathbb{Z}_2$ besteht nur aus $\{-1, +1\}$ Elementen und daher sind alle Einträge von M_ψ entweder +1 oder -1.

Um zu zeigen, dass alle Zeilen von M_ψ orthogonal zueinander sind, verwenden wir Lemma 6.6 aus dem Buch von Horadam[1].

Lemma 6.6 besagt: Wenn G eine endliche Gruppe ist und $\psi \in \mathbb{Z}^2(G, \mathbb{Z}_2)$ ein Kozykel ist, dann gilt in $\mathbb{Z}[\mathbb{Z}_2]$ für jedes Paar $h, k \in G$:

$$\sum_{g \in G} \psi(h,g)\psi(k,g)^{-1} = \psi(hk^{-1}, k)^{-1} \sum_{g \in G} \psi(hk^{-1}, g) \tag{1}$$

Folglich ist M_ψ orthogonal sobald ψ orthogonal ist und für die Gruppe $\mathbb{Z}_2$ folgt dann die Orthogonalität der Zeilen und Spalten von der Matrix M_ψ.

[1] K.J.Horadam *Hadamard Matrices and Their Applications*, Princeton University Press, 2007

Der Beweis dieses Lemmas lautet wie folgt:

Beweis. Sei $d = hk^{-1}$. Dann haben wir:

$$\begin{aligned}\text{LHS} &= \sum_{g\in G} \psi(dk, g)\psi(k, g)^{-1} \\ &= \sum_{g\in G} (\psi(d, k)^{-1}\psi(d, kg)\psi(k, g))\psi(k, g)^{-1} \\ &= \psi(d, k)^{-1} \sum_{g\in G} \psi(d, kg) \\ &= \text{RHS}\end{aligned}$$

$\mathbb{Z}_2$ ist eine endliche Gruppe der Ordnung 2. Wenn ψ orthogonal ist, bedeutet dies dass für jedes $d \neq 1 \in G$ gilt: $\sum_{g\in G} \psi(d, g) = \frac{|G|}{2} \cdot e$. Daher ist die Gleichung (1) aus dem Lemma 6.6 gleich wie für $\frac{|G|}{2} \cdot e$ und somit ist M_ψ orthogonal.

□

Die Bedeutung von diesem Lemma ist dass eine kozyklische G-Matrix M_ψ über C eine normalisierte Hadamard-Matrix ist sobald ψ orthogonal ist.

Daraus folgt, dass alle Zeilen von M_ψ orthogonal zueinander sind.
Das gleiche Argument gilt auch für die Spalten von M_ψ und somit ist der zweite Teil des Beweises abgeschlossen.

□

5.2.5 Anwendungen auf fehlerkorrigierende Codes

Viele Codes werden aus Hadamard-Matrizen oder aus verwandten symmetrischen Blockdesigns oder Differenzmengen gebildet. Wenn die für die Konstruktionen verwendete Hadamard-Matrix kozyklisch ist, sind die resultierenden Codes kozyklische Hadamard Codes. Folglich ist z.B. der Reed-Muller-Code erster Ordnung (konstruiert aus den Sylvester-Hadamard-Matrizen) ein binär kozyklischer Hadamard-Code.

Literatur

[1] K.J.Horadam *Hadamard Matrices and Their Applications*, Princeton University Press, 2007.

[2] Marshall Hall Jr *Combinatorial Theory*, 1976.

[3] `https://inductiva.ai/blog/article/hadamard-matrices-1-a-motivation`

[4] `https://www.sciencedirect.com/science/article/pii/S0166218X99002334`