2.3 Hadamard-Codes

Eine $n \times n$-Matrix H mit Einträgen $+1$ oder -1 heißt *Hadamard-Matrix* der *Ordnung* n, falls

$$H \cdot H^\top = nE_n$$

gilt, wobei E_n die Einheitsmatrix der Ordnung n bezeichnet. Die Determinante einer reellen $n \times n$-Matrix mit Einträgen aus dem reellen Intervall $[-1, +1]$ ist beschränkt durch $n^{n/2}$, und Hadamard-Matrizen sind genau diejenigen, für die diese Schranke angenommen wird. Man beachte, daß der (i, j)-te Eintrag von $HH^\top$ das Produkt der i-ten und der j-ten Zeile von H ist. Im Fall einer reellen $n \times n$-Matrix H mit Einträgen $+1$ oder -1 ist das Produkt einer Zeile mit sich selbst gleich n, so daß ein solches H genau dann eine Hadamard-Matrix ist, wenn das Produkt verschiedener Zeilen 0 ist, diese Zeilen also orthogonal sind.

$S_0 := (+1)$ und $S_1 := \left(\begin{smallmatrix} +1 & +1 \\ +1 & -1 \end{smallmatrix}\right)$ sind Hadamard-Matrizen.

Eine größere Klasse von Beispielen erhält man, in dem man sich die $n := 2^m$ vielen Elemente des Vektorraumes $V := {\mathbb{Z}_2}^m$ in einer festen Weise angeordnet denkt und

$$H(a, b) := (-1)^{a^\top b} \text{ für } a, b \in V$$

setzt.[1] Die hierdurch definierte $n \times n$-Matrix H über $\{-1, +1\}$ ist dann eine Hadamard-Matrix der Ordnung n. Für $a \in V$ gilt nämlich

$$\sum_{c \in V} H(a, c)H^\top(c, a) = \sum_{c \in V} H(a, c)H(a, c) = \sum_{c \in V} 1 = n.$$

Für $a \neq b$ aus V gibt es ein i mit $a(i) \neq b(i)$, und bezeichnet e_i wie üblich den i-ten Einheitsvektor in ${\mathbb{Z}_2}^m$, so kommt

$$\begin{aligned}
\sum_{c \in V} H(a, c)H^\top(c, b) &= \sum_{c \in V} H(a, c)H(b, c) \\
&= \sum_{c \in V} (-1)^{a^\top c}(-1)^{b^\top c} \\
&= \sum_{c \in V} (-1)^{(a+b)^\top c} \\
&= \sum_{\substack{c \in V \\ c(i)=0}} \underbrace{\left((-1)^{(a+b)^\top c} + (-1)^{(a+b)^\top (c+e_i)}\right)}_{=0} \\
&= 0.
\end{aligned}$$

Im vorletzten Schritt werden die Paare $c, c + e_i$ von Vektoren, die sich nur an der Stelle i unterscheiden, zusammengefasst. Wegen $(a + b)^\top (c + e_i) = (a + b)^\top c + (a + b)^\top e_i = (a + b)^\top c + 1$ sind die beiden entsprechenden Summanden

[1] Dabei wird das Ergebnis von $a^\top b$, per se 0 oder 1 aus $\mathbb{Z}_2$, als natürliche Zahl interpretiert.

$(-1)^{(a+b)^\top c}$, $(-1)^{(a+b)^\top (c+e_i)}$ gleich $+1, -1$ oder gleich $-1, +1$, heben sich also gegenseitig auf.

Daher gilt $HH^\top = nE_n$.

Der folgende Satz fast zwei kombinatorische Eigenschaften von Hadamard-Matrizen zusammen.

Satz 3 *Sei H eine Hadamard-Matrix der Ordnung n. Dann gilt:*

(i) Ist $n > 1$, so ist n gerade und je zwei verschiedene Zeilen von H stimmen an genau $n/2$ Stellen überein.

(ii) Ist $n > 2$, so ist n durch vier teilbar und je drei Zeilen von H stimmen an genau $n/4$ Stellen überein.

Beweis. Seien x, y die i-te bzw. j-te Zeile von H und

$$A(x,y) := \{k \in \{1,\dots,n\} : x_k = y_k\}$$

sowie $\overline{A}(x,y) := \{1,\dots,n\} \setminus A(x,y)$. Für $i \neq j$ ist

$$0 = (HH^\top)(i,j) = \sum_{k=1}^{n} x_k y_k;$$

jedes $k \in A(x,y)$ trägt 1 zur Summe bei, jedes $k \in \overline{A}(x,y)$ dagegen -1, und so folgt $|A(x,y)| = |\overline{A}(x,y)|$, also (i).

Für drei verschiedene Zeilen x, y, z ist dagegen

$$\begin{aligned} & 2|A(x,y) \cap A(x,z)| \\ = \;& |A(x,y)| - |A(x,y) \cap \overline{A}(x,z)| + |A(x,z)| - |A(x,z) \cap \overline{A}(x,y)| \\ = \;& |A(x,y)| + |A(x,z)| - |\overline{A}(y,z)|, \end{aligned}$$

woraus (ii) folgt. Die zweite Gleichung gilt, da für jedes $k \in \{1,\dots,k\}$ genau dann $(x_k = y_k \wedge x_k \neq z_k) \vee (x_k = z_k \wedge x_k \neq y_k)$ ist, wenn $y_k \neq z_k$ ist. □

Satz 3 besagt, daß die Ordnung einer Hadamard Matrix entweder gleich 1 oder 2 oder aber durch 4 teilbar ist. Es wird vermutet, ist aber bis heute unbewiesen, daß es zu *jeder* durch 4 teilbaren Zahl n auch eine Hadamard-Matrix der Ordnung n gibt. Der erste offene Fall ist $n = 668$.

*

Wir nennen eine Matrix C *symmetrisch*, falls $C^\top = C$ gilt und *antisymmetrisch*, falls $C^\top = -C$ gilt. Eine $n \times n$-Matrix C über $\{0, 1, -1\}$ heißt *Konferenzmatrix*, falls

$$C(i,j) = 0 \longleftrightarrow i = j \text{ für } i,j \in \{1,\dots,n\} \text{ und}$$

$$CC^\top = (n-1)E_n$$

gilt. Aus symmetrischen und antisymmetrischen Konferenzmatrizen lassen sich Hadamard-Matrizen herstellen wie folgt.

Satz 4 *Sei C eine Konferenzmatrix der Ordnung n. Dann gilt:*

(i) Ist C antisymmetrisch, so ist $C + E_n$ eine Hadamard-Matrix.

(ii) Ist C symmetrisch, so ist $H := \left(\begin{smallmatrix} +C+E_n & +C-E_n \\ +C-E_n & -C-E_n \end{smallmatrix}\right)$ eine Hadamard-Matrix.

Beweis. Aus $C^\top = -C$ folgt $(C + E_n)(C + E_n)^\top = CC^\top + C + C^\top + E_n = CC^\top + E_n = (n-1)E_n + E_n = nE_n$, also gilt (i). Mit $C = C^\top$ folgt für die Matrix H aus (ii) durch Rechnung: $HH^\top = 2nE_{2n}$ (Übung). □

Wir rufen uns ein wenig höhere Algebra in Erinnerung.

Sei H eine Untergruppe der Gruppe G mit $\cdot$, das heißt $1 \in H$, $ab \in H$ für alle $a, b \in H$ und $a^{-1} \in H$ für alle $a \in H$. Zu $a \in G$ definiert man die *Links- und Rechtsnebenklasse* zu a durch $aH := \{ax : x \in H\}$ bzw. $Ha := \{ax : x \in H\}$. Die Linksnebenklassen sind genau die Äquivalenzklassen der durch

$$a \equiv b \,\text{modulo}\, H \;:\longleftrightarrow\; b^{-1}a \in H$$

gegebenen Äquivalenzrelation auf G; folglich ist die Menge $G/H := \{aH : a \in G\}$ aller Linksnebenklassen eine Partition von G in lauter zu H gleichmächtige Mengen (letzteres wird durch die Bijektion $x \mapsto ax$ von H nach aH zertifiziert). Das ist der Satz von Lagrange; für endliches G folgt sofort

$$|G| = |G/H||H|.$$

Die Untergruppe H heißt *Normalteiler* von G, falls $aH = Ha$ für alle $a \in G$. In diesem Fall (und nur dann) ist die durch $aH \cdot bH := (ab)H$ gegebene Operation auf G/H wohldefiniert; G/H mit $\cdot$ ist dann eine Gruppe.

Sind G und H Gruppen, so heißt eine Abbildung $\varphi : G \to H$ ein *Homomorphismus*, falls $\varphi(ab) = \varphi(a)\varphi(b)$ für alle a, b aus G gilt. Daraus läßt sich $\varphi(1) = 1$ und $\varphi(a^{-1}) = \varphi(a)^{-1}$ herleiten. Wie üblich gilt: Das Bild $\varphi(G) = \{\varphi(x) : x \in G\}$ ist eine Untergruppe von H, und der *Kern* von φ, definiert durch

$$\text{Kern}\varphi := \{x \in G : \varphi(x) = 1\}$$

ist eine Untergruppe von G und genau dann gleich $\{1\}$, wenn φ injektiv ist. Tatsächlich ist $H := \text{Kern}\varphi$ bereits ein Normalteiler von G, denn ist $z \in aH$, also $z = ax$ für ein $x \in H$, so ist $\varphi(axa^{-1}) = \varphi(a)\varphi(1)\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = 1$ und folglich $y = axa^{-1} \in H$, daher $z = axa^{-1}a$ in Ha, daher gilt $aH \subseteq Ha$ und analog $Ha \subseteq aH$. Ein bijektiver Homomorphismus ist ein *Isomorphismus*,

und der Homomorphiesatz besagt, daß für jeden Homomorphismus φ die Abbildung $\psi : G/\text{Kern}\varphi \to \varphi(G)$, $\psi(a\text{Kern}\varphi) := \varphi(a)$ wohldefiniert und ein Isomorphismus sind, das heißt die Gruppen $G/\text{Kern}\varphi$ und $\varphi(G)$ sind isomorph. (Beweis: Es sind äquivalent: $a\text{Kern}\varphi = b\text{Kern}\varphi$, $a^{-1}b \in \text{Kern}\varphi$, $\varphi(a^{-1}b) = 1$, $\varphi(a) = \varphi(b)$.)

In der Algebra zeigt man, daß die Einheitengruppe $K^* = K \setminus \{0\}$ eines endlichen Körpers K *zyklisch* ist, das heißt von der Form

$$K^* = \{g^i : i \in \mathbb{Z}\}$$

für einen geeigneten *Erzeuger* g. Wegen $g^{|K^*|} = 1$ gilt sogar

$$K^* = \{g^0, g^1, \ldots, g^{|K|-2}\}.$$

So ist zum Beispiel 2 ein Erzeuger von $\mathbb{Z}_5^*$, denn

$$\mathbb{Z}_5^* = \{2^0, 2^1, 2^2, 2^3\} = \{1, 2, 4, 3\}.$$

Sei G eine Gruppe und T die Gruppe der Elemente des komplexen Einheitskreises mit der gewöhnlichen Multiplikation komplexer Zahlen. Ein Homomorphismus $\chi : G \to T$ heißt *Charakter* von G, und im Fall χ konstant 1 der *triviale Charakter*. Für jeden nichttrivialen Charakter χ gibt es ein $a \in G$ mit $\chi(a) \neq 1$, und wir rechnen

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(ax) = \sum_{x \in G} \chi(a)\chi(x) = \chi(a) \sum_{x \in G} \chi(x),$$

was notwendig

$$\sum_{x \in G} \chi(x) = 0$$

nach sich zieht.

Wir sind nun vorbereitet für die Konstruktion von Konferenzmatrizen.

Satz 5 *Sei K Körper mit q Elementen, wobei q eine ungerade Primzahlpotenz ist, und g ein Erzeuger von K^*. Sei χ der durch $\chi(g^i) := (-1)^i$ definierte (!) nichttriviale Charakter von K^* und $\chi(0) := 0$. Durch $Q(x, y) := \chi(x - y)$ für $x, y \in K$ wird eine $q \times q$-Matrix über $\{0, +1, -1\}$ definiert. Sei J die $1 \times q$-Matrix mit lauter Einträgen 1. Dann gilt:*

(i) Ist $q \equiv 1$ modulo 4, so ist $C := \left(\begin{smallmatrix} 0 & J \\ J^\top & Q \end{smallmatrix}\right)$ symmetrische Konferenzmatrix.

(ii) Ist $q \equiv 3$ modulo 4, so ist $C := \left(\begin{smallmatrix} 0 & J \\ -J^\top & Q \end{smallmatrix}\right)$ schiefsymmetrische Konferenzmatrix.

Beweis. Genau dann besitzt für $a \in K$ die Gleichung $a = x^2$ eine Lösung, wenn $a = g^i$ für ein geradzahliges i ist, wenn also $\chi(a) = 1$ ist. Die Gleichung $x^2 = 1$ hat nur die Lösungen $x = 1$ und $x = -1$, wobei $+1 \neq -1$ gilt. Ferner ist $a := g^{|K^*|/2} = -1$, denn $a \neq 1$ und $a^2 = g^{|K^*|} = 1$.

Im Fall $q \equiv 1$ modulo 4 ist $(g^{|K^*|/4})^2 = -1$, also $\chi(-1) = 1$.

Im Fall $q \equiv 3$ modulo 4 betrachte man den Gruppenhomomorphismus

$$\varphi : K^* \to K^*,\ \varphi(x) := x^2.$$

Es ist $|\text{Kern}\varphi| = |\{-1, +1\}| = 2$, also gilt mit dem Satz von Lagrange über die Gleichmächtigkeit der Linksnebenklassen und dem Homomorphiesatz:

$$|K^*| = |K^*/\text{Kern}\varphi||\text{Kern}\varphi| = 2|\varphi(K^*)|.$$

Wegen $|K^*| \equiv 2 \bmod 4$ (nach Fallvoraussetzung) ist $|\varphi(K^*)|$ ungerade und folglich $\{-1, +1\}$ keine Untergruppe von $\varphi(K^*)$, also $-1 \notin \varphi(K^*)$; also hat $-1 = x^2$ keine Lösung, somit $\chi(-1) = -1$.

Wegen

$$Q(y, x) = \chi(y - x) = \chi((-1)(x - y)) = \chi(-1)Q(x, y)$$

sind die Matrizen Q und folglich auch C in (i), (ii) symmetrisch bzw. schiefsymmetrisch.

Es bleibt noch $CC^\top = qE_{q+1}$ zu zeigen; dazu sei h die erste Zeile von C und h_x die Zeile von C mit der x-ten Zeile von Q. Offenbar gilt $hh = q$ und $h_x h_x = 1 + q - 1 = q$. Mit $\sum_{y \in K^*} \chi(y) = 0$ ist auch $\sum_{y \in K} \chi(y) = 0$ und $\sum_{y \in K} \chi(x - y) = 0$, also $hh_x = h_x h = 0$. Für $x \neq y$ aus K kommt

$$\begin{aligned}
h_x h_y &= 1 + \sum_{z \in K} \chi(x - z)\chi(y - z) \\
&= 1 + \sum_{z \in K} \chi(z)\chi((y - x) + z) \\
&= 1 + \sum_{z \in K^*} \chi(z)\chi(z(z^{-1}(y - x) + 1)) \\
&= 1 + \sum_{z \in K^*} \chi(z)\chi(z)\chi((z^{-1}(y - x) + 1)) \\
&= 1 + \sum_{z \in K^*} \chi((z^{-1}(y - x) + 1)) \\
&= 1 + \sum_{z \in K \setminus \{1\}} \chi(z) \\
&= \sum_{z \in K} \chi(z) \\
&= 0.
\end{aligned}$$

□

Satz 6 *Sei q eine ungerade Primzahlpotenz. Dann gilt:*

(i) Ist $q \equiv 1$ mod 4, so existiert eine Hadamard-Matrix der Ordnung $2q + 2$.

(ii) Ist $q \equiv 3$ mod 4, so existiert eine Hadamard-Matrix der Ordnung $q + 1$.

Beweis. Sofort aus Satz 5 und Satz 4. □

Weitere Hadamard-Matrizen erhält man durch Konstruktionen mittels des Kronecker-Produkts (Übungen).

Satz 7 *Sei H eine Hadamard-Matrix der Ordnung $n > 1$. Die Matrix M entstehe aus der $2n \times n$ Matrix $\binom{+H}{-H}$ durch Ersetzen von -1 durch 0. Wir fassen sie als Matrix über $\mathbb{Z}_2$ auf. Die Menge $C \subseteq {\mathbb{Z}_2}^n$ ist dann ein n-Code der Größe $2n$ mit Minimalabstand $n/2$, der sogenante mit H assozierte* Hadamard-Code.

Beweis. Wegen Satz 3 stimmen je zwei Zeilen von H an genau $n/2$ Stellen nicht überein. Hieraus folgt, daß je zwei Zeilen von M an genau $n/2$ Stellen oder an allen Stellen nicht übereinstimmen. □