Prof. Dr. Matthias Kriesell
Fakultät für Mathematik und Naturwissenschaften

TECHNISCHE UNIVERSITÄT
**ILMENAU**

# 7. Studienbrief zur Informations- und Codierungstheorie

In den kommenden beiden Wochen wird es um Hadamard-Matrizen und die aus ihnen hervorgehenden Codes gehen. Ihr Lesepensum für diese Woche besteht einenteils aus einigen grundlegenden kombinatorischen Betrachtungen; zur Konstruktion sogenannter Konferenzmatrizen (in der kommenden Woche) ist allerdings ein wenig höhere Algebra nötig, nämlich der Satz von Lagrange und der Homomorphiesatz. Ich habe beides in den Abschnitt 2.3 aufgenommen, zusammen mit Beweisskizzen, zu beidem gibt es deutsche Wikipedia-Artikel. Der Satz, daß die multiplikative Gruppe eines endlichen Körpers zyklisch ist, wird hier nicht bewiesen; man zeigt das in der Informatik gelegentlich, wenn über die Konstruktion endlicher Körper zu reden ist, in der Mathematik gehört es in eine Algebra-Vorlesung.

*

**Lesepensum** bis zum 5. Juni 2020:

Kapitel 2 Teil 2 bis zur Mitte von Seite 4 „$\mathbb{Z}_5^* = [...]$". Es ist auch möglich, nur bis Satz 4 einschließlich Beweis zu arbeiten (die Woche ist schließlich kurz) — dann aber kommt in der nächsten Woche eine geballte Ladung Algebra auf Sie zu!

*

**Übungspensum** bis zum 12. Juni 2020:

Für die Aufgaben 4(iii),5,6 wird der Stoff der kommenden Woche benötigt: Der gesamte zweite Teil von Kapitel 2, wie er im Netz steht.

1. Führen Sie den Beweis von Satz 4 (ii) durch. Rechnen mit Blockmatrizen ist natürlich erlaubt!

2. Seien $A$ eine $m \times n$-Matrix und $B$ eine Matrix über demselben Ring. Das *Kronecker–Produkt* von $A$ und $B$ ist definiert durch

$$A \otimes B \quad := \quad \begin{pmatrix} A(1,1)B & A(1,2)B & \cdots & A(1,n)B \\ A(2,1)B & A(2,2)B & \cdots & A(2,n)B \\ \vdots & \vdots & \ddots & \vdots \\ A(m,1)B & A(m,2)B & \cdots & A(m,n)B \end{pmatrix}.$$

(Die rechte Seite ist als Blockmatrix zu lesen: Die $mn$ vielen Blöcke bestehen aus entsprechend skalierten Exemplaren der Matrix $B$.) Man beweise die folgenden Rechenregeln.

(i) $E_m \otimes E_n = E_{mn}$,

(ii) $(A \otimes B)^\top = A^\top \otimes B^\top$ und

(iii) $(A \otimes B) \cdot (C \otimes D) = (A \cdot C) \otimes (B \cdot D)$ für solche Matrizen $C, D$, für die die auftretenden Produkte erklärt sind. (Dabei ist $\cdot$ das gewöhnliche Matrix-Produkt.)

3. Man zeige: Ist $H$ eine Hadamard–Matrix der Ordnung $m$ und $I$ eine Hadamard–Matrix der Ordnung $n$, so ist $H \otimes I$ eine Hadamard–Matrix der Ordnung $m \cdot n$.

4. Die Hadamard-Matrix $S_1 = \left(\begin{smallmatrix} +1 & +1 \\ +1 & -1 \end{smallmatrix}\right)$ ist die sogenannte 1-te Sylvester-Matrix. Rekursiv definiert man die $(n+1)$-te Sylvester-Matrix durch

$$S_{n+1} := S_1 \otimes S_n.$$

(i) Man zeige: Für jedes $n \geq 1$ ist $S_n$ eine Hadamard-Matrix der Ordnung $2^n$.

(ii) Man gebe die dritte Sylvester-Matrix an.

(iii) Man zeige: Der mit $S_n$ assoziierte Hadamard-Code (siehe Satz 7) ist ein $(n+1)$-dimensionaler Untervektorraum von ${\mathbb{Z}_2}^{2^n}$.

5. Konstruieren Sie eine Konferenzmatrix der Ordnung $19$. Sie müssen nicht alle $361$ Einträge niederschreiben — vielleicht genügt ja eine „prototypische" Zeile, aus der Sie die anderen $18$ leicht gewinnen können.

6. Verifizieren Sie mit den Sätzen aus Abschnitt 2.3 und dieser Übung die Existenz von Hadamard-Matrizen der Ordnung $n = 1, 2, 4, 8, 12, 16, \ldots$ bis Sie auf das erste $n$ stoßen, für welches das nicht möglich ist.

*

Fragen und Anregungen gerne per email an mich — IC am Anfang der Betreffzeile nicht vergessen!

Ilmenau, den 2. Juni 2020 · Matthias Kriesell