Übungen zur Codierungstheorie

Blatt 8 SoS 2023 — H. Kiechle

Präsenzaufgaben

28. *Reed-Muller-Codes erster Ordung*

Wir definieren rekursiv für alle $i \in \mathbb{N}$ je einen binären $(2^i, i+1)$-Code $\mathcal{R}_i$:

$$\mathcal{R}_1 := \mathbb{Z}_2^2 \quad \text{und} \quad \mathcal{R}_{i+1} := \left\{ \mathbf{xx}, \mathbf{xx}^* \in \mathbb{Z}_2^{2^{i+1}} \; ; \; \mathbf{x} \in \mathcal{R}_i \right\} \quad \text{für alle } i \in \mathbb{N}.$$

Wir schreiben $\mathbf{0} := 00\ldots0$ für das „Nullwort“ und $\mathbf{1} := 11\ldots1$ für das „Einswort“ jeweils passender Länge.

(a) Für $\mathbf{x} \in \mathbb{Z}_2^n$ gilt $\mathbf{x}^* = \mathbf{x} + \mathbf{1}$ (vgl. Aufgabe 19).

(b) $\mathcal{R}_i$ ist linear.

(c) Es sei $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$ eine Basis von $\mathcal{R}_i$, wobei $k = \dim \mathcal{R}_i$ und $\mathbf{0}, \mathbf{1} \in \mathbb{Z}_2^{2^i}$.

Dann ist $(\mathbf{b}_1\mathbf{b}_1, \ldots, \mathbf{b}_k\mathbf{b}_k, \mathbf{01})$ eine Basis von $\mathcal{R}_{i+1}$.

(d) Folgern Sie mit Induktion, dass $\dim \mathcal{R}_i = i + 1$.

29. Wahr oder falsch?

(a) Für $\mathbf{x} \in \mathbb{Z}_2^n$ gilt $\mathbf{x} \cdot \mathbf{x} = 0 \iff \gamma(\mathbf{x})$ ist gerade.

(b) Falls es $\mathbf{x} \in \mathbb{Z}_q^n$ mit $\mathbf{x} \cdot \mathbf{x} = 0$ gibt, so folgt $q = 2$.

Hausaufgaben

30. *Reed-Muller-Codes erster Ordung* (Fortsetzung von Aufgabe 28)

Wir definieren rekursiv für alle $i \in \mathbb{N}$ die Matrizen

$$G_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad G_{i+1} := \begin{pmatrix} G_i & G_i \\ \mathbf{0} & \mathbf{1} \end{pmatrix} \quad \text{für alle } i \in \mathbb{N}.$$

(a) Bestimmen Sie explizit G_2 und G_3 und bringen Sie beide auf reduzierte Zeilenstufenform.

i. Welchen (bekannten) Code beschreibt G_2?

ii. Geben Sie eine Kontrollmatix für $\mathcal{R}_2$ an.

iii. $\mathcal{R}_3$ ist äquivalent zum $(8,4)$-Bauer-Code.

(b) Beweisen Sie mit Induktion (und Aufgabe 28(c)):

Für alle $i \in \mathbb{N}$ ist G_i eine Generatormatrix von $\mathcal{R}_i$ ist.

(c) Beweisen Sie mit Induktion:

$\mathcal{R}_i$ enthält die Worte $\mathbf{0}$ und $\mathbf{1}$. Alle anderen Codewörter haben das Gewicht 2^{i-1}.

(d) Daher gilt $\gamma_{\min}(\mathcal{R}_i) = \ldots$.

bitte wenden!

31. Wir wenden die Konstruktion aus Aufgabe 27 auf den $(7,4)$-Hamming-Code $\mathcal{H}$ an und erhalten den (n,k)-Code $\mathcal{H}'$.

(a) Geben Sie (n,k) an.

(b) Geben Sie eine Generatormatrix G für $\mathcal{H}'$ an. Evtl. hilft die Generatormatrix für $\mathcal{H}$ aus (4.1.6).

(c) Erzeugen Sie aus G durch elementare Zeilenumformungen eine Matrix H, die *rechts* eine Einheitsmatrix stehen hat.

(d) Zeigen Sie, dass H eine Kontrollmatrix von $\mathcal{H}$ ist.

(e) Was folgt daraus für den Code $\mathcal{H}'$?

Anmerkung: Der Reed-Muller-Code $\mathcal{R}_5$ wurde 1969 – 1976 bei den Mariner Expeditionen zum Mars genutzt um Bilder auf die Erde zu übertragen.