Allgemeine und Lineare Codes

Erklärung

Einführung: Definition Alphabet und Wort

Ein **Alphabet** $A = \{a_1, \ldots, a_k\}$ ist eine endliche Menge von Symbolen a_i mit $k \geq 2$.
Ein **Wort** w über dem Alphabet A ist ein Tupel $(a_{i_1}, \ldots, a_{i_l}) \in A^l$ von Elementen aus A.
Die Menge aller Wörter ist $A^* = \bigcup_{l=1}^{\infty} A^l$.

Definitionen Allgemeine Codes

Erklärung

- Ein **Code** C über dem Alphabet A ist eine nicht-leere Teilmenge von A.
- Ein **Blockcode** der Länge $n \in \mathbb{N}$ ist eine nichtleere Teilmenge von A^n.
- Codes über dem Alphabet $\mathbb{F}_2 = \{0, 1\}$ nennt man **binäre Codes**.

Erklärung

Hamming-Abstand

Es seien $x, y \in A^n$ zwei Wörter gleicher Länge über dem Alphabet A.
Der **Hammingabstand** von $x = (x_1, \ldots, x_n)$ zu $y = (y_1, \ldots, y_n)$ ist die Anzahl an Positionen, an denen sich x und y unterscheiden:

$$\text{dist}(x, y) := |\{i \in \{1, \ldots, n\} : x_i \neq y_i\}|$$

Der Hammingabstand ist eine Metrik und erfüllt die folgenden drei Kriterien:

Für alle $x, y, z \in A^n$ gilt:
1) Positivität: $\text{dist}(x, y) \geq 0, \text{dist}(x, x) = 0$.
2) Symmetrie: $\text{dist}(x, y) = \text{dist}(y, x)$.
3) Dreiecksungleichung:
$\text{dist}(x, y) \leq \text{dist}(x, z) + \text{dist}(z, y)$.

Erklärung

Minimalabstand und Hamming-Kugel

Der **Minimalabstand** eines Codes C ist definiert als $d(C) := \min\{\text{dist}(x, y) : x, y \in C, x \neq y\}$.

Sei A ein Alphabet, auf dem der Hammingabstand *dist* definiert ist und $x \in A$.
Dann ist $\mathcal{B}_r(x, A) = \{y \in A : d(x, y) \leq r\}$ die **Hamming-Kugel** um x mit Radius r in A.

Erklärung

Dekodieren mit dem Maximum Likelyhood Decoding (MLD)-Verfahren

Sei $w \in A^n$ ein Wort der Länge n, $C \subseteq A^n$ ein Blockcode der Länge n, und d der Minimalabstand von w zum Code C. Das MLD-Verfahren funktioniert wie folgt:

- Gibt es *nur ein* $\tilde{c} \in C$ mit $\text{dist}(\tilde{c}, w) = d$, so wird w das Codewort $\tilde{c}$ zugewiesen.
- Gibt es *mehrere* $c \in C$ mit $\text{dist}(c, w) = d$, so schlägt das Verfahren fehl.

Erklärung

Fehlererkennung und Fehlerkorrektur

Ein Code C heißt

- **t-fehlererkennend** mit $t \in \mathbb{N} \cup \{0\}$, wenn für jedes Codewort $c \in C$ gilt: Einfügen von bis zu t Fehlern in c erzeugt stets ein Wort w mit $w \notin C$.
- **t-fehlerkorrigierend** mit $t \in \mathbb{N} \cup \{0\}$, wenn für jedes Codewort $c \in C$ gilt: Einfügen von bis zu t Fehlern in c erzeugt stets ein Wort w, das beim Dekodieren mit MLD das Codewort c liefert.

Ein Code $C \subseteq A^n$ mit $t := d(C)$ ist $(t-1)$-fehlererkennend und $\lfloor \frac{t-1}{2} \rfloor$-fehlerkorrigierend.

Erklärung

Lineare Codes

Ein Code $C \subseteq (\mathbb{F}_p)^n$ heißt **linearer Code**, wenn C ein Untervektorraum von $(\mathbb{F}_p)^n$ ist. Man spricht von einem $[n, k]$-Code, falls C die Dimension k hat. Mit einem Minimalabstand von $d := d(C)$ spricht man von einem $[n, k, d]$-Code.

Erklärung

Generator- und Kontrollmatrix

Sei C ein linearer Blockcode der Dimension k und $g_1, \ldots, g_k \in C$ seien linear unabhängig. Die Matrix G mit Zeilen $g_1, \ldots, g_k$ ist eine **Generatormatrix** von C.
Die Generatormatrix erzeugt alle Codewörter und ordnet jedem Datenwort ein Codewort zu, d.h. für jedes Codewort c $w \in (\mathbb{F}_{\mathbb{P}}{}^n)$ Eine Matrix $H \in (\mathbb{F}_p)^{n \times l}$ ist eine **Kontrollmatrix** von C, falls für alle $x \in (\mathbb{F}_p)^n$ gilt: $x \in C \Leftrightarrow x \cdot H = (0, \ldots, 0)$.

Erklärung

Das Kontrollmatrix-Kriterium

Eine Matrix $H \in (\mathbb{F}_p)^{n \times l}$ ist genau dann eine Kontrollmatrix für C, wenn:

i) $\text{rang}(H) = n - k$ mit $k = \dim(C)$, ii) $\mathrm{G} \cdot \mathrm{H} = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix} \in (\mathbb{F}_p)^{k \times l}$.

Aufgaben

Allgemeine Codes

Lösung

Aufgabe 1. Gib ein Beispiel für ein Codewort in den folgenden Mengen an.
a) $\{0,1\}^3$ b) $\{0,1,2,3\}^5$ c) $\{A,M,E,S,N\}^5$.
Notiere zusätzlich das zugehörige Alphabet und die Länge des Codewortes.

Lösung

Aufgabe 2. Bestimme die Menge aller Codewörter von
a) $(\mathbb{F}_2)^3$ b) $(\mathbb{F}_5)^1$ c) $(\mathbb{F}_3)^2$

Lösung

Aufgabe 3. Schreibe einen Code
a) der Länge 2 über $\mathbb{F}_3$ b) der Länge 3 über $\mathbb{F}_2$ c) der Länge 6 über $\mathbb{F}_4$

Lösung

Aufgabe 4. Wie viele Codewörter besitzt ein (binärer) Code der Länge n höchstens?

Hamming-Abstand und Minimalabstand

Lösung

Aufgabe 5. Berechne den Minimalabstand der folgenden Codes:
a) $C_1 = \{00001, 00110, 11000\}$ b) $C_2 = \{01100, 10011, 11001, 10101\}$

Lösung

Aufgabe 6. Bestimme jeweils den minimalen und maximalen Hammingabstand der Wörter aus den Codes aus Aufgabe 3.

Fehlererkennung und Fehlerkorrektur

Lösung

Aufgabe 7. Wie viele Fehler können die folgenden Codes korrigieren?
a) $C = \{0101, 1110, 1001\}$ b) $C = \{00011, 11000, 11111, 00100\}$
c) $C = \{000000, 110001, 001111, 111110\}$ d) $C = \{000011, 110010, 001100, 111101\}$

Lösung

Aufgabe 8. Zeige, dass der folgende Code keine Fehler korrigieren kann:
$C_3 = \{0111, 0100, 1001\}$.

Lösung

Aufgabe 9. Gibt es einen Code mit 4 Codewörtern der Länge 8, der 3 Fehler korrigieren kann?

Lösung

Aufgabe 10. Zeige, dass ein Code $C \subseteq \mathbb{Z}_2^8$, der zwei Fehler korrigieren kann höchstens 4 Codewörter haben kann. Gibt es einen solchen Code?

Lösung

Aufgabe 11. Gib ein Beispiel an, wann das MLD-Verfahren fehlschlägt.

Lineare Codes

Lösung

Aufgabe 12. Sind die folgenden Codes linear?
a) $C = \{0000, 0001, 0011, 0010\}$ b) $C = \{00000, 10001, 01101, 11100, 11101\}$
c) $C = \{0011, 0001, 0010\}$ d) $C = \{00000, 10111, 01110, 11001\}$

Lösung

Aufgabe 13. Bestimme je einen $[4,k]$-Code in $\subseteq \mathbb{Z}_2^4$ mit unterschiedlichem Minimalabstand $d = 1$ und $d = 2$.

Lösung

Aufgabe 14. Bestimme für den folgenden linearen Code die Parameter k und n.

$$C := \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\}$$

Generator- und Kontrollmatrix

Aufgabe 15. Bestimme Generator- und Kontrollmatrizen von C_1 und C_2 mit

$$C_1 \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right\}, \quad C_2 \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\}.$$

Aufgabe 16. Gebe eine Kontrollmatrix H für C aus Aufgabe 14 an.

Aufgabe 17. Seien G eine Generatormatrix zum Code C und $c \in C$. Zeige, dass das Gleichungssystem $x \cdot G = c$ eindeutig lösbar ist. Welche Bedeutung hat damit die Generatormatrix?