7. Endliche Körper und lineare Codes

7.1. Endliche Körper

Für alle Primzahlen p hat man auf $\mathbb{Z}_p$ die Operationen $+$ und $\cdot$ zur Verfügung und diese sind gemäß dem Distributivgesetz miteinander verträglich.

Bsp: $p = 5$

$$3 \cdot (2+4) = 3 \cdot 1 = 3$$

$$(3 \cdot 2) + (3 \cdot 4) = 1 + 2 = 3$$

Allgemein heißt ein geordnetes 5-Tupel $(K, +, \cdot, 0, 1)$ bestehend aus

(i) einer endlichen nichtleeren Menge K,

(ii) einer Verknüpfung $+ : K \times K \to K$,

(iii) einer Verknüpfung $\cdot : K \times K \to K$ und

(iv) Elementen $0 \in K$, $1 \in K$

ein endlicher Körper, wenn die folgenden Eigenschaften erfüllt sind:

(1) $(K, +, 0)$ ist eine endliche kommutative Gruppe

(2) $(K \setminus \{0\}, \cdot, 1)$ ist eine endliche kommutative Gruppe

(3) $\forall a \in K \; \forall b \in K \; \forall c \in K \; \left(a \cdot (b+c) = a \cdot b + a \cdot c \right)$

Bsp: Für alle Primzahlen p ist $(\mathbb{Z}_p, +, \cdot, 0, 1)$ ein endlicher Körper.

Merke: In endlichen Körpern kann man rechnen, wie es es von den reellen Zahlen her kennt.

Bsp: Welches $x \in \mathbb{Z}_{17}$ erfüllt die Gleichung $12x + 4 = 0$?

$$12x + 4 = 0 \quad | +13$$
$$12x = 13 \quad | \cdot 10$$
$$x = 11$$

Das kleinste $n \in \mathbb{N} \setminus \{0,1\}$ mit $\underbrace{1+1+\ldots+1}_{n \text{ Summanden}} = 0$ heißt Charakteristik des endlichen Körpers $(K, +, \cdot, 0, 1)$.

Merke:

(1) Die Charakteristik eines endlichen Körpers ist stets eine Primzahl.

(2) Ein endlicher Körper der Charakteristik p enthält stets einen Teilkörper, der isomorph zu $(\mathbb{Z}_p, +, \cdot, 0, 1)$ ist.

(3) Zu jeder Primzahl p und jedem $n \in \mathbb{N} \setminus \{0\}$ gibt es bis auf Isomorphie genau einen endlichen Körper mit p^n Elementen. Andere endliche Körper gibt es nicht.

7.2. Vektorräume über endlichen Körpern

Sei $(K, +, \cdot, 0, 1)$ ein endlicher Körper. Dann betrachten wir für $n \in \mathbb{N} \setminus \{0\}$ Vektoren mit n Einträgen aus K.

Bsp: $K = \mathbb{Z}_5$, $n = 3$

$v = (1,2,4) \in K^3$, $u = (3,0,2) \in K^3$

$v + u = (1+3, 2+0, 4+2) = (4,2,1)$

$2 \cdot v = (2 \cdot 1, 2 \cdot 2, 2 \cdot 4) = (2,4,3)$

$\langle v, u \rangle = 1 \cdot 3 + 2 \cdot 0 + 4 \cdot 2 = 3 + 0 + 3 = 1$

Wichtig ist außerdem die Multiplikation mit Matrizen, die Einträge aus K haben.

Bsp: $K = \mathbb{Z}_2$

$v = (1,0,1,1)$, $u = (1,1,0)$

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$M \cdot v^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad u \cdot M = (1,1,1,0)$$

7.3 Lineare Codierer

$(K, +, \cdot, 0, 1)$ ... endlicher Körper

$k \in \mathbb{N}$ und $n \in \mathbb{N}$ mit $1 \leq k \leq n$

Ein Codierer ordnet jedem $x \in K^k$ (Nachricht genannt) ein $y \in K^n$ (Codevektor genannt) eineindeutig zu.

Ein Codierer ist linear, wenn es eine Matrix $G_1 \in K^{k \times n}$ gibt mit $y = x \cdot G_1$ für alle Nachrichten $x \in K^k$.

G_1 heißt die Generatormatrix des Codierers.

Bsp: $K = \mathbb{Z}_2$, $k = 4$, $n = 5$

Anhängen eines Paritätsbits erfolgt mit der Generatormatrix

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

$x = (0,1,0,0)$

$y = x \cdot G_1 = (0,1,0,0,1)$

Die Generatormatrix ist kanonisch, wenn sie die Gestalt $G_1 = (I_k \; A)$ für eine Matrix $A \in K^{k \times n-k}$ hat.

Grundidee:

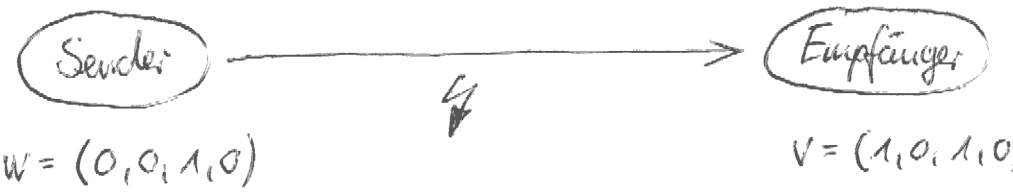
An jede Nachricht $x \in K^k$ werden mit G $(n-k)$ Kontrollstellen angehängt. Diese können dann z.B. verwendet werden, um auf Übertragungsfehler zu prüfen und solche Fehler ggf. zu korrigieren.

Die Menge der mit G erzeugbaren Codevektoren bezeichnen wir mit

$$C_G = \{ x \cdot G \; ; \; x \in K^k \}.$$

7.4. Fehlerkorrigierende lineare Codes

Bei der Übertragung eines Codevektors w wird jeder Eintrag von w unabhängig von den anderen Einträgen mit einer Wahrscheinlichkeit $p < \frac{1}{2}$ fehlerhaft empfangen:



$w = (0,0,1,0)$ $\qquad$ $v = (1,0,1,0) \neq w$

Der Empfänger sucht dann unter allen möglichen Codevektoren u des verwendeten Codierers denjenigen, der am ehesten zum empfangenen Codevektor v passt.

Messung des Abstands zweier Codevektoren u und v mit dem Hamming-Abstand:

$H(u,v)$ = Anzahl Positionen, an denen sich u und v unterscheiden

Bsp: $u = (\underline{0}, \underline{0}, 1, 1, \underline{0}, \underline{1}, 0)$, $v = (\underline{1}, \underline{1}, 1, 1, \underline{1}, \underline{0}, 0)$

$H(u,v) = 4$

Satz: Der Hamming-Abstand ist eine Metrik auf der Menge K^n, d.h. für alle $u, v, w \in K^n$ gilt:

(i) $H(u,v) \geq 0$

(ii) $H(u,v) = 0 \Leftrightarrow u = v$

(iii) $H(u,v) = H(v,u)$

(iv) $H(u,w) \leq H(u,v) + H(v,w)$ "Dreiecksungleichung"

[ohne Beweis]

Hamming-Gewicht einer Codevektors v:

$HG(v)$ = Anzahl Einträge ungleich 0

Bsp: $v = (0,1,0,0,1,1,0)$, $HG(v) = 3$

Es gilt immer: $H(u,v) = HG(u-v)$

Minimalabstand der Codevektoren in C_G:

$$d_G = \min\left(\{ H(u,v) : u,v \in C_G \wedge u \neq v \}\right)$$

Satz: Die maximale Anzahl von fehlerhaft übertragenen Positionen, die bei einem linearen Codierer mit Generatormatrix G sicher korrigiert werden kann, ist $r = \left\lfloor \frac{d_G - 1}{2} \right\rfloor$.

Bsp: $K = \mathbb{Z}_2$, $G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

x	$x \cdot G$
00	00000
01	01111
10	10110
11	11001

$d_G = 3$, $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$

↘ Höchstens eine fehlerhafte Position kann korrigiert werden.

Allgemein gilt für einen Codierer mit kanonischer Generatormatrix $G_k = (I_k \; A)$, dass $d_G \geq s+1$ ist, genau dann, wenn in der Kontrollmatrix $H = (-A^T I_{n-k})$ jede Menge von s Spalten-vektoren linear unabhängig ist.

Bsp: (von oben)

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Je zwei Spalten von H sind linear unabhängig.

Die drei markierten Spalten sind linear abhängig:

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Also gilt $d_G = 2+1 = 3$.