Lineare Algebra für Informatiker

Abgabe: 29.06.2017

Adrian C. Hinrichs Matr.Nr. 367129
Georg C. Dorndorf Matr.Nr. 366511

#40	#41	Σ
5 / 10	9 / 10	14 / 20

N.T.

Definition: Seien $n, m \in \mathbb{N}$; K ein Körper und Matrizen $A, B \in K^{n\times m}$ gegeben. Genau dann wenn ein Kompositum elementarer Zeilenoperationen ζ existiert, so dass gilt $A \overset{\zeta}{\mapsto} B$, sei:

$$A \rightsquigarrow B := A \xmapsto{\zeta} B$$

Das geht nicht, weil durch deine Definition Informationen „verloren" gehen und somit ist diese Def. unzulässig. ^^

367129
366511

Aufgabe 41 | A. Hinrichs

Seien ein endlicher Körper K; $n \in \mathbb{N}$ ~~...~~ gegeben.
Ein Blockcode C der Länge n über K heisst perfekt, wenn

$$K^{n\times 1} = \bigcup_{c \in C} B_{\frac{d(C)}{2}}(c)$$

gilt.

a) Zu zeigen: $\forall r \in \mathbb{R}_{\geq 0}, a \in K^{n\times 1}$ ist $B_r(a)$ endlich und es gilt:

4

$$|B_r(a)| = \sum_{\substack{j \in [0,n] \\ j<r}} \binom{n}{j}(|K|-1)^j .$$

Sei $r \in \mathbb{R}_{\geq 0}$; $a \in K^{n\times 1}$

Beweis: $|B_r(a)| = \left|B\left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}\right)\right| = |\{ b \in K^{n\times 1} \mid d(a,b) < r\}|$

$$\overset{(4.9)}{=} |\{a+d \mid d \in \{e \in K^{n\times 1} \mid wt(e) < r\}\}|$$

$$= |\{d \in K^{n\times 1} \mid wt(d) < r\}|$$

$$= \left|\dot{\bigcup_{\substack{i \in [0,n] \\ i<r}}} \{c \in K^{n\times 1} \mid wt(c) = i\}\right|$$ ✓ // (a)

$$= \sum_{\substack{i \in [0,n] \\ i<r}} |\{c \in K^{n\times 1} \mid wt(c) = i\}|$$ ✓ // (1)

$$= \sum_{\substack{i \in [0,n] \\ i<r}} |\{c \in K^{n\times 1} \mid \text{exakt } i \text{ Einträge von } c \text{ sind ungleich } 0\}|$$

$$\overset{\blacktriangle}{=} \sum_{\substack{i \in [0,n] \\ i<r}} \binom{n}{i}(|K|-i)^i$$ ✓ □

~~Also gilt die Glei~~

▲: Die Menge der ~~Codewörter~~ Vektoren ~~c~~ mit genau i 1-Einträgen lässt sich modellieren als:

$$M := \{v \in K^{n\times 1} \mid (v_k) = \chi_M(k))_{k \in [1,n]} \text{ für } M \in Comb_i([1,n])\} \;*$$

Es gilt

$$|M| = |Comb_i([1,n])| = \binom{n}{i}$$ ✓ // (1)

Die Anzahl der ~~nicht~~ Vektoren mit exakt i nicht-0-Einträgen beläuft sich also logischerweise auf

$$|M| \cdot (|K| \setminus \{0\})^i = |M| \cdot (|K|-1)^i = \binom{n}{i}(|K|-1)^i$$

~~Ei~~ Diese Menge ist also endlich, jede endliche ~~Ve~~ Vereinigung daher auch. □ ✓ // (1)

* Unter Missbrauch der Notation fassen wir nach DS WiSe 16/17 Vektoren als Familien und diese als Folgen mit einem entsprechenden Intervall als Indexmenge auf.

Es gilt also die Gleichheit und $B_r(a)$ ist endlich.
QED

4 b) Sei C ein Blockcode der Länge n über K. ✓

Zu zeigen: Es gilt:

$$|K|^n \geq |C| \cdot \sum_{\substack{j \in [0,n] \\ j < \frac{d(C)}{2}}} \binom{n}{j} \cdot (|K|-1)^j =: A$$

und $|K^n| = A$ genau dann wenn C perfekt ist.

Beweis:

$\forall a,b \in C$ mit $a \neq b$ gilt: $d(a,b) = d(0, a-b) \geq d(C)$

Also gilt: $B_{\frac{d(C)}{2}}(a) \cap B_{\frac{d(C)}{2}}(b) = \emptyset$ ✓ Δ

$$|C| \cdot \sum_{\substack{j \in [0,n] \\ j < \frac{d(C)}{2}}} \binom{n}{j} (|K|-1)^j \overset{(a)}{=} \sum_{c \in C} |B_{\frac{d(C)}{2}}(c)|$$ // 2

$$\overset{(\Delta)}{=} \left| \dot\bigcup_{c \in C} B_{\frac{d(C)}{2}}(c) \right|$$ ✓ // 1

Falls C perfekt ist folgt die Gleichheit zu $|K|^n = |K^{n \times 1}|$ direkt aus der Definition der Perfektheit. $\square$ ✓

Andernfalls kann die Menge $B := \dot\bigcup_{c \in C} B_{\frac{d(C)}{2}}(c)$ nur weniger Elemente als $K^{n \times 1}$ besitzen, da sie dann eine echte Teilmenge ist $(B \subsetneq K^{n \times 1})$. ~~Die Behauptung gilt also erst~~

Also gilt:

$$|K^{n \times 1}| \geq |B| \;\square$$ ✓ // 1

Die Behauptung wurde also gezeigt

QED

1 c) Zu zeigen: Jeder lineare $[11,6,5]$-Code über $\mathbb{F}_3$ ist perfekt.

Beweis: Sei $\mathcal{L}$ ein linearer $[11,6,5]$-Code über $\mathbb{F}_3$. Per Def. gilt:
▷ $\mathcal{L} \subseteq \mathbb{F}_3^{11 \times 1}$ sorry, hab da erst eine „2" gelesen.
▷ $\dim \mathcal{L} = 6$
▷ $d(\mathcal{L}) = 5$

$$\mathbb{F}_3^{11 \times 1} \overset{!}{=} \bigcup_{c \in C} B_{2.5}(c) \overset{(\Delta)}{=} \dot\bigcup_{c \in C} B_{2.5}(c)$$

Wir wissen, dass $\mathcal{L}$ die Dimension 6 hat, daher hat $\mathcal{L}$ $3^6 = 729$ ~~Ele~~ (distinktive) Elemente. ✓

Ferner wissen wir, dass $|B_{2.5}(a)| = \sum_{\substack{j \in [0,11] \\ j < 2.5}} \binom{11}{j} (|\mathbb{F}_3|-1)^j$
$= \sum_{\substack{j \in [0,11] \\ j < 2.5}} \binom{11}{j} 2^j$
$= 11 \cdot 2 + 55 \cdot 4 = 243$ $= 3^{11}$ (✓)

Das ist ein bisschen zu schwammig, man kann $|\mathbb{F}_3|^{11} = 3^{11}$ $= |C| \cdot \Sigma$ — nicht verwenden. $\forall a \in C$ gilt. −1

Also gilt $|\mathbb{F}_3^{11 \times 1}| \overset{3^{11}}{=} \sum_{c \in C} |B_{2.5}(c)| = |\dot\bigcup_{c \in C} B_{2.5}(c)|$ ~~≠ ...~~ ($|C| = 729$)

2 Da $B := \dot\bigcup_{c \in C} B_{2.5}(c)$ ~~⊊~~ $\subseteq \mathbb{F}_3^{11 \times 1}$ und $|B| = |\mathbb{F}_3^{11 \times 1}|$ gilt, muss $B = \mathbb{F}_3^{11 \times 1}$ gelten, also ist $\mathcal{L}$ perfekt. QED

Aufgabe 40 366511

(a) Es sei $A \in \mathbb{F}_3^{6\times 4}$ gegeben durch $A = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&1&2&2 \\ 2&1&1&2 \end{pmatrix}$ und es sei C der lineare Code über $\mathbb{F}_3$ mit der Erzeugermatrix A.

2 (a)

Zu bestimmen: Kontrollmatrix B von C

Mit Beispiel 4.27 und 3.56/3.57:

Für die ~~Die~~ Kontrollmatrix B von C gilt: $C = Sol(B, 0)$

Nach 3.57 lässt sich B nun wie folgt berechnen:

Wir bestimmen $Sol(A^{tr}, 0)$:

$$Sol(A^{tr}, 0) = Sol\left(\begin{pmatrix} 1&0&0&0&1&2 \\ 0&1&0&0&1&1 \\ 0&0&1&0&2&1 \\ 0&0&0&1&2&2 \end{pmatrix}, 0\right)$$

$$= \mathbb{F}_3 \begin{pmatrix} -1 \\ -1 \\ -2 \\ -2 \\ 1 \\ 0 \end{pmatrix} + \mathbb{F}_3 \begin{pmatrix} -2 \\ -1 \\ -1 \\ -2 \\ 0 \\ 1 \end{pmatrix}$$

$$= \left\langle \begin{pmatrix} -1 \\ -1 \\ -2 \\ -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ -1 \\ -1 \\ -2 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

$$= Col\left(\begin{pmatrix} -1 & -2 \\ -1 & -1 \\ -2 & -1 \\ -2 & -2 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = Col(B^{tr}$$

$$\overset{3.56/3.57}{\Longrightarrow} B = \begin{pmatrix} -1&-1&-2&-2&1&0 \\ -2&-1&-1&-2&0&1 \end{pmatrix}$$ ✓ // 2

Zu Bestimmen: Die Anführer aller Syndrome bzg. B.

Es folgt aus 4.31, dass die Syndrome alle $x \in \mathbb{F}_3^{2\times 1}$ sind.

Nach 4.34 muss nun für alle Anfürer $e \in \mathbb{F}_3^{6\times 1}$

$wt(e) = \min\{ wt(x) \mid x \in \mathbb{F}_3^{6\times 1}$ so, dass x das Syndrom y hat $\}$
und $B\, y = z$ mit $z \in \mathbb{F}_3^{2\times 1}$, z ist Syndrom
gelten.

Es ergibt sich folgende Tabelle (in Anlehnung an 4.38).

$$B = \begin{pmatrix} -1 & -1 & -2 & -2 & 1 & 0 \\ -2 & -1 & -1 & -2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 1 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}$$

Syndrom	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}2\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}0\\2\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$	$\begin{pmatrix}1\\2\end{pmatrix}$	$\begin{pmatrix}2\\1\end{pmatrix}$	$\begin{pmatrix}2\\2\end{pmatrix}$
Anführer	$\begin{pmatrix}0\\0\\0\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\0\\1\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\1\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\0\\0\\1\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\0\\0\\2\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\1\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\\0\\0\\0\end{pmatrix}$

f (-1) f (-1) 1 fehlt hier (-1) //0

Obige Tabelle folgt offensichtlich aus der Kontrollmatrix und 4.34.

(b) (2)

Seien $[n, k, d]$ die Parameter von C. Dann folgt mit 4.19 und 4.22 durch A, dass $k = 4$ ist. Es folgt weiterhin auch mit 4.19 und A, dass $n = 6$ ist.

Für d gilt mit 4.30, dass $d = d(C)$ //1

$= \max\{ r \in \mathbb{N} \mid$ es gibt $j_1, \dots, j_{r-1} \in [1, n]$ mit $j_1 < \dots < j_{r-1}$ so, dass $(B_{-,j_1}, \dots, B_{-,j_{r-1}})$ linear unabhängig ist $\}$

~~Für alle $j_1, j_2 \in [1,6]$ mit $j_1 < j_2$ und~~

Es lässt sich offensichtlich an den Spalten 5 und 6 von B ~~aber~~ ablesen, dass maximal 2 Spalten linear unabh. sind. Daraus folgt mit 4.30, dass $d(C) = 2 = d$ ist.

//1

Wir erhalten also $[6, 4, 2]$ als Parameter für C.

(C) Es seien $x_1, x_2, x_3 \in \mathbb{F}_3^{6\times 1}$ gegeben durch

(a)

$$x_1 = \begin{pmatrix}1\\0\\1\\2\\0\\2\end{pmatrix},\quad x_2 = \begin{pmatrix}0\\2\\1\\1\\0\\2\end{pmatrix},\quad x_3 = \begin{pmatrix}1\\2\\2\\1\\0\\1\end{pmatrix}$$

Wir decodieren x_i für $i \in [1,3]$ nach 4.38.

Es ist $B x_1 = \begin{pmatrix}-1-2-2\\-2-1-2+2\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$

Der Anführer von $\begin{pmatrix}1\\0\end{pmatrix}$ ist $\begin{pmatrix}0\\0\\0\\0\\1\\0\end{pmatrix}$

Es wird x_1 also nach 4.38 zu $\begin{pmatrix}1\\0\\1\\2\\0\\2\end{pmatrix} - \begin{pmatrix}0\\0\\0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\1\\2\\\cancel{2}\,2\\2\end{pmatrix}$ decodiert.

f x_1 hat keinen eind. Anführer (-1)

Es ist $B x_2 = \begin{pmatrix}-2-2-2\\-2-1-2+2\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$

Der Anführer von $\begin{pmatrix}0\\0\end{pmatrix}$ ist $(0\ 0\ 0\ 0\ 0\ 0)^{tr}$.

Es wird x_2 also zu $(0\ 2\ 1\ 1\ 0\ 2)^{tr}$ decodiert.

✓ (1)

Es ist $B x_3 = \begin{pmatrix}-1-2-4-2\\-2-2-2-2+1\end{pmatrix} = \begin{pmatrix}0\\2\end{pmatrix}$

Der Anführer von $\begin{pmatrix}0\\2\end{pmatrix}$ ✓ ist nicht eindeutig bestimmt und könnte $(0\,0\,0\,0\,0\,2)^{tr}$ oder $(1\ 0\ 0\ 1\ 0\ 0)^{tr}$ sein. x_3 kann also nicht eindeutig zu einem Codewort decodiert werden.

Anführer!

f (-1)

Der Anführer ist eind.