MDP Faltungscodes

Julia Lieb

Institut für Mathematik
Universität Würzburg

Motivation/Prinzip der Kodierungstheorie

1. Nachricht als Vektor mit Einträgen aus einem endlichen Körper: $u = \begin{pmatrix} u_0 \\ \vdots \\ u_{k-1} \end{pmatrix} \in \mathbb{F}^k$

Motivation/Prinzip der Kodierungstheorie

1. Nachricht als Vektor mit Einträgen aus einem endlichen Körper: $u = \begin{pmatrix} u_0 \\ \vdots \\ u_{k-1} \end{pmatrix} \in \mathbb{F}^k$
2. Durch Hinzufügen redundanter Information erhält man aus der Nachricht u das Kodewort $v \in \mathbb{F}^n$ mit $n > k$.

Motivation/Prinzip der Kodierungstheorie

1. Nachricht als Vektor mit Einträgen aus einem endlichen Körper: $u = \begin{pmatrix} u_0 \\ \vdots \\ u_{k-1} \end{pmatrix} \in \mathbb{F}^k$
2. Durch Hinzufügen redundanter Information erhält man aus der Nachricht u das Kodewort $v \in \mathbb{F}^n$ mit $n > k$.
3. v wird an Empfänger gesendet; je nach Kanal können verschiedene Arten von Fehlern auftreten (Auslöschungen, Vertauschungen, falsche Symbole)

Motivation/Prinzip der Kodierungstheorie

1. Nachricht als Vektor mit Einträgen aus einem endlichen Körper: $u = \begin{pmatrix} u_0 \\ \vdots \\ u_{k-1} \end{pmatrix} \in \mathbb{F}^k$
2. Durch Hinzufügen redundanter Information erhält man aus der Nachricht u das Kodewort $v \in \mathbb{F}^n$ mit $n > k$.
3. v wird an Empfänger gesendet; je nach Kanal können verschiedene Arten von Fehlern auftreten (Auslöschungen, Vertauschungen, falsche Symbole)
4. Dekodierung: Rekonstruktion von u aus (fehlerhaftem) v

Beispiel: ISBN-Nummern

ISBN-Nummer:
9 Stellen mit Information $z_1, \ldots, z_9$,
letzte Stelle $z_{10} := \sum_{i=1}^{9} i \cdot z_i \mod 11$ ist Prüfziffer

Beispiel: ISBN-Nummern

ISBN-Nummer:
9 Stellen mit Information $z_1, \ldots, z_9$,
letzte Stelle $z_{10} := \sum_{i=1}^{9} i \cdot z_i \mod 11$ ist Prüfziffer

Beispiel: 074755442-0 (Harry Potter and the Goblet of Fire)

1. $u = (z_1, \ldots, z_9)^\top = (0, 7, 4, 7, 5, 5, 4, 4, 2)^\top \in \mathbb{F}_{11}^9$

Beispiel: ISBN-Nummern

ISBN-Nummer:
9 Stellen mit Information $z_1, \ldots, z_9$,
letzte Stelle $z_{10} := \sum_{i=1}^{9} i \cdot z_i \mod 11$ ist Prüfziffer

Beispiel: 074755442-0 (Harry Potter and the Goblet of Fire)

1. $u = (z_1, \ldots, z_9)^\top = (0, 7, 4, 7, 5, 5, 4, 4, 2)^\top \in \mathbb{F}_{11}^9$
2. $z_{10} = 187 \equiv 0 \mod 11$,
   $v = (z_1, \ldots, z_{10})^\top = (0, 7, 4, 7, 5, 5, 4, 4, 2, 0)^\top \in \mathbb{F}_{11}^{10}$

Beispiel: ISBN-Nummern

ISBN-Nummer:
9 Stellen mit Information $z_1, \ldots, z_9$,
letzte Stelle $z_{10} := \sum_{i=1}^{9} i \cdot z_i \mod 11$ ist Prüfziffer

Beispiel: 074755442-0 (Harry Potter and the Goblet of Fire)

1. $u = (z_1, \ldots, z_9)^\top = (0, 7, 4, 7, 5, 5, 4, 4, 2)^\top \in \mathbb{F}_{11}^9$
2. $z_{10} = 187 \equiv 0 \mod 11$,
   $v = (z_1, \ldots, z_{10})^\top = (0, 7, 4, 7, 5, 5, 4, 4, 2, 0)^\top \in \mathbb{F}_{11}^{10}$

Erkannt wird, wenn

- eine Ziffer falsch ist
- zwei aufeinanderfolgende Ziffern vertauscht werden

Lineare Blockcodes

Definition

Ein linearer (n, k) **Blockcode** $\mathcal{C}$ ist ein k dimensionaler Unterraum des Vektorraumes $\mathbb{F}^n$. Es existiert $G \in \mathbb{F}^{n \times k}$ mit vollem Rang, so dass $\mathcal{C} = \{v \in \mathbb{F}^n \mid v = Gu \text{ für ein } u \in \mathbb{F}^k\}$. G heißt **Generatormatrix** und $\frac{k}{n}$ **Rate** von $\mathcal{C}$.

Lineare Blockcodes

Definition

Ein linearer (n, k) **Blockcode** $\mathcal{C}$ ist ein k dimensionaler Unterraum des Vektorraumes $\mathbb{F}^n$. Es existiert $G \in \mathbb{F}^{n \times k}$ mit vollem Rang, so dass $\mathcal{C} = \{v \in \mathbb{F}^n \mid v = Gu \text{ für ein } u \in \mathbb{F}^k\}$. G heißt **Generatormatrix** und $\frac{k}{n}$ **Rate** von $\mathcal{C}$.

Beispiel (ISBN): $G = \begin{pmatrix} & & & & I_9 & & & & \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \in \mathbb{F}^{10 \times 9}$

Lineare Blockcodes

Definition

Ein linearer (n, k) **Blockcode** $\mathcal{C}$ ist ein k dimensionaler Unterraum des Vektorraumes $\mathbb{F}^n$. Es existiert $G \in \mathbb{F}^{n \times k}$ mit vollem Rang, so dass $\mathcal{C} = \{v \in \mathbb{F}^n \mid v = Gu \text{ für ein } u \in \mathbb{F}^k\}$. G heißt **Generatormatrix** und $\frac{k}{n}$ **Rate** von $\mathcal{C}$.

Beispiel (ISBN): $G = \begin{pmatrix} & & & & I_9 & & & & \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \in \mathbb{F}^{10 \times 9}$

Definition

Das **Hamming-Gewicht** von $v = (v_1, \ldots, v_n)^\top \in \mathbb{F}^n$ ist die Anzahl der Einträge mit $v_i \neq 0$. Der **Minimalabstand** von $\mathcal{C}$ ist $d_{\min} := \min_{v, \hat{v} \in \mathcal{C}, v \neq \hat{v}} wt(v - \hat{v}) = \min_{v \in \mathcal{C}, v \neq 0} wt(v)$.

Lineare Blockcodes

Definition

Ein linearer (n, k) **Blockcode** $\mathcal{C}$ ist ein k dimensionaler Unterraum des Vektorraumes $\mathbb{F}^n$. Es existiert $G \in \mathbb{F}^{n \times k}$ mit vollem Rang, so dass $\mathcal{C} = \{v \in \mathbb{F}^n \mid v = Gu \text{ für ein } u \in \mathbb{F}^k\}$. G heißt **Generatormatrix** und $\frac{k}{n}$ **Rate** von $\mathcal{C}$.

Beispiel (ISBN): $G = \begin{pmatrix} & & & & I_9 & & & & \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \in \mathbb{F}^{10 \times 9}$

Definition

Das **Hamming-Gewicht** von $v = (v_1, \ldots, v_n)^\top \in \mathbb{F}^n$ ist die Anzahl der Einträge mit $v_i \neq 0$. Der **Minimalabstand** von $\mathcal{C}$ ist $d_{\min} := \min_{v, \hat{v} \in \mathcal{C}, v \neq \hat{v}} wt(v - \hat{v}) = \min_{v \in \mathcal{C}, v \neq 0} wt(v)$.

Beispiel (ISBN): $d_{min} = 2$

Lineare Blockcodes

Definition

Ein linearer (n, k) **Blockcode** $\mathcal{C}$ ist ein k dimensionaler Unterraum des Vektorraumes $\mathbb{F}^n$. Es existiert $G \in \mathbb{F}^{n \times k}$ mit vollem Rang, so dass $\mathcal{C} = \{v \in \mathbb{F}^n \mid v = Gu \text{ für ein } u \in \mathbb{F}^k\}$. G heißt **Generatormatrix** und $\frac{k}{n}$ **Rate** von $\mathcal{C}$.

Beispiel (ISBN): $G = \begin{pmatrix} & & & & I_9 & & & & \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} \in \mathbb{F}^{10 \times 9}$

Definition

Das **Hamming-Gewicht** von $v = (v_1, \ldots, v_n)^\top \in \mathbb{F}^n$ ist die Anzahl der Einträge mit $v_i \neq 0$. Der **Minimalabstand** von $\mathcal{C}$ ist $d_{\min} := \min_{v, \hat{v} \in \mathcal{C}, v \neq \hat{v}} wt(v - \hat{v}) = \min_{v \in \mathcal{C}, v \neq 0} wt(v)$.

Beispiel (ISBN): $d_{min} = 2$

Theorem (Singleton-Schranke)

$d_{\min} \leq n - k + 1$

Faltungscodes

Definition

Sei $G \in \mathbb{F}[z]^{n \times k}$ von vollem Spaltenrang. Dann heißt

$$\mathfrak{C} = \{v \in \mathbb{F}[z]^n \mid v(z) = G(z)u(z) \text{ für ein } u \in \mathbb{F}[z]^k\}.$$

Faltungscode der **Rate** k/n. Die **Generatormatrix** G von $\mathfrak{C}$ ist eindeutig bis auf Multiplikation mit einer unimodularer Matrix $U \in GL_k(\mathbb{F}[z])$.

Nachricht: $u_0, u_1, \ldots \quad \Rightarrow u(z) = \begin{pmatrix} u_0 \\ \vdots \\ u_{k-1} \end{pmatrix} + \begin{pmatrix} u_k \\ \vdots \\ u_{2k-1} \end{pmatrix} \cdot z + \cdots$

Codewort: $v(z) = G(z)u(z) = \begin{pmatrix} v_0 \\ \vdots \\ v_{n-1} \end{pmatrix} + \begin{pmatrix} v_n \\ \vdots \\ v_{2n-1} \end{pmatrix} \cdot z + \cdots$

$\Rightarrow v_0, v_1, \ldots$

Faltungscodes

Definition

Eine **Minore** einer rechteckigen Matrix ist die Determinante einer quadratischen Teilmatrix.

Definition

Der **Grad** δ von $\mathfrak{C}$ ist definiert als der maximale Grad der $k \times k$-Minoren, d.h. der Minoren maximaler Größe, von G. Seien $\delta_1, \ldots, \delta_k$ die Grade der Spalten von G. Dann gilt $\delta \leq \delta_1 + \cdots + \delta_k$ und falls $\delta = \delta_1 + \cdots + \delta_k$, nennt man G **minimale** Generatormatrix.

Faltungscodes

Definition

Eine **Minore** einer rechteckigen Matrix ist die Determinante einer quadratischen Teilmatrix.

Definition

Der **Grad** δ von $\mathfrak{C}$ ist definiert als der maximale Grad der $k \times k$-Minoren, d.h. der Minoren maximaler Größe, von G. Seien $\delta_1, \ldots, \delta_k$ die Grade der Spalten von G. Dann gilt $\delta \leq \delta_1 + \cdots + \delta_k$ und falls $\delta = \delta_1 + \cdots + \delta_k$, nennt man G **minimale** Generatormatrix.

Definition

Falls G rechtsprim ist, d.h. falls $G(z)$ für alle $z \in \overline{\mathbb{F}}$ vollen Spaltenrang besitzt, existiert eine sog. **Kontrollmatrix** $H \in \mathbb{F}[z]^{(n-k)\times n}$ von vollem Rang, so dass

$$\mathfrak{C} = \{v \in \mathbb{F}[z]^n \mid H(z)v(z) = 0 \in \mathbb{F}[z]^{n-k}\}.$$

MDP Faltungscodes

Definition

Für $j \in \mathbb{N}_0$ ist der **j-te Spaltenabstand** von $\mathfrak{C}$ definiert als

$$d_j^C(\mathfrak{C}) := \min \left\{ \sum_{t=0}^{j} wt(\vec{v}_t) \mid v \in \mathfrak{C} \text{ und } v \not\equiv 0 \right\}.$$

MDP Faltungscodes

Definition

Für $j \in \mathbb{N}_0$ ist der **j-te Spaltenabstand** von $\mathfrak{C}$ definiert als

$$d_j^C(\mathfrak{C}) := \min\left\{ \sum_{t=0}^{j} wt(\vec{v}_t) \mid v \in \mathfrak{C} \text{ und } v \not\equiv 0 \right\}.$$

Theorem (GRS 2006)

$$d_j^C(\mathfrak{C}) \leq (n-k)(j+1)+1$$

Definition

Ein Faltungscode $\mathfrak{C}$ mit Rate k/n und Grad δ heißt **MDP** falls

$$d_j^C(\mathfrak{C}) = (n-k)(j+1)+1 \quad \text{für } j = 0, \ldots, L := \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor$$

GRS 2006: H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. IEEE Trans. Inform. Theory, 52(2):584–598, 2006.

MDP Faltungscodes

Theorem (GRS 2006)

$G(z) = \sum_{i=0}^{\mu} G_i z^i \in \mathbb{F}[z]^{n\times k}$ und $H(z) = \sum_{i=0}^{\nu} H_i z^i \in \mathbb{F}[z]^{n-k\times n}$ seien Generator- bzw. Kontrollmatrix von $\mathfrak{C}$. Äquivalent sind:

(i) $\mathfrak{C}$ ist MDP.

(ii) Jede Minore maximaler Größe von $\mathcal{G}_L := \begin{bmatrix} G_0 & & 0 \\ \vdots & \ddots & \\ G_L & \dots & G_0 \end{bmatrix}$

mit $G_i \equiv 0$ für $i > \mu$, die nicht trivialerweise Null ist, d.h. Null für jede Wahl von $G_1, \dots, G_L$, ist ungleich Null.

(iii) Jede Minore maximaler Größe von $\mathcal{H}_L := \begin{bmatrix} H_0 & & 0 \\ \vdots & \ddots & \\ H_L & \dots & H_0 \end{bmatrix}$

mit $H_i \equiv 0$ für $i > \nu$, die nicht trivialerweise Null ist, ist ungleich Null. Diese Minoren ergeben sich durch Auswahl von Spalten mit Indizes $1 \le j_1 < \dots < j_{(j+1)(n-k)}$ so dass $j_{s(n-k)} \le sn$ für $s = 1, \dots, L$.

Reversible MDP Faltungscodes

Definition (H 2008)

Sei $\mathfrak{C}$ ein (n, k, δ) Faltungscode mit minimaler Generatormatrix G. Setze $\overline{g_{ij}(z)} := z^{\delta_j} g_{ij}(z^{-1})$. Dann ist der Code $\overline{\mathfrak{C}}$ mit Generatormatrix $\overline{G}$ ebenfalls ein (n, k, δ) Faltungscode, der **invertierter Code** zu $\mathfrak{C}$ genannt wird.
Es gilt: $v_0 + \cdots + v_d z^d \in \overline{\mathfrak{C}} \Leftrightarrow v_d + \cdots + v_0 z^d \in \mathfrak{C}$

Definition (TRS 2012)

Sei $\mathfrak{C}$ ein MDP Faltungscode. Wenn $\overline{\mathfrak{C}}$ ebenfalls MDP ist, so nennt man $\mathfrak{C}$ einen **reversiblen MDP** Faltungscode.

H 2008: R. Hutchinson. The existence of strongly MDS convolutional codes. SIAM J. Control Optim., 47(6):2812–2826, 2008.

TRS 2012: V. Tomas, J. Rosenthal and R. Smarandache. Decoding of Convolutional Codes Over the Erasure Channel. IEEE Trans. Inf. Theory 58(1), 2012.

Reversible MDP Faltungscodes

Bemerkung

Falls $(n-k) \mid \delta$ *und* $H(z) = H_0 + \cdots + H_\nu z^\nu$ *eine Kontrollmatrix des MDP Codes* $\mathfrak{C}$ *ist, hat der invertierte Code* $\overline{\mathfrak{C}}$ *die Kontrollmatrix* $\overline{H(z)} = H_\nu + \cdots + H_0 z^\nu$. *Folglich ist* $\mathfrak{C}$ *genau dann reversibel MDP wenn jede Minore maximaler Größe der Matrix*

$$\mathfrak{H}_L := \begin{bmatrix} H_\nu & \cdots & H_{\nu-L} \\ & \ddots & \vdots \\ 0 & & H_\nu \end{bmatrix}$$

gebildet aus Spalten mit Indizes $j_1, \ldots, j_{(L+1)(n-k)}$ *so dass* $j_{s(n-k)+1} > sn$ *für* $s = 1, \ldots, L$ *ungleich Null ist.*

Vollständige MDP Faltungscodes

Definition (TRS 2012)

Seien $k < n$, $(n-k) \mid \delta$ und
$H(z) = H_0 + H_1 z + \cdots H_\nu z^\nu \in \mathbb{F}[z]^{(n-k)\times n}$ eine Kontrollmatrix des Faltungscodes $\mathfrak{C}$ mit Rate k/n und Grad δ. Dann heißt

$$\mathfrak{H} := \begin{pmatrix} H_\nu & \cdots & H_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & H_\nu & \cdots & H_0 \end{pmatrix} \in \mathbb{F}^{(L+1)(n-k)\times(\nu+L+1)n}$$

partielle Kontrollmatrix des Codes. Desweiteren heißt $\mathfrak{C}$ ein **vollständiger MDP** Faltungscode, falls für die partielle Kontrollmatrix gilt, dass jede Minore maximaler Größe, die nicht trivialerweise gleich Null ist, ungleich Null ist.
Diese Bedingung kann nur erfüllt sein, falls $(n-k) \mid \delta$.

Vollständige MDP Faltungscodes

Bemerkung (TRS 2012)

Eine Minore maximaler Größe von $\mathfrak{H}$ gebildet aus den Spalten $j_1, \ldots, j_{(L+1)(n-k)}$ ist genau dann nicht trivialerweise Null wenn

(i) $j_{2s+1} > sn$

(ii) $j_{2s} \leq sn + \nu n$

für $s = 1, \ldots, L$.

Bemerkung (TRS 2012)

Jeder vollständige MDP Faltungscode ist ein reversibler MDP Faltungscode, da die Matrizen $\mathcal{H}_L$ und $\mathfrak{H}_L$ Teilmatrizen von $\mathfrak{H}$ mit identischer Zeilenzahl sind.

Existenz von MDP Faltungsodes

Theorem (TRS 2012)

Seien $n, k, \delta \in \mathbb{N}$ mit $k < n$. Dann existiert ein reversibler MDP (n, k, δ) Faltungscode, falls der zugrundeliegende Körper hinreichend groß ist.

Existenz von MDP Faltungsodes

Theorem (TRS 2012)

Seien $n, k, \delta \in \mathbb{N}$ mit $k < n$. Dann existiert ein reversibler MDP (n, k, δ) Faltungscode, falls der zugrundeliegende Körper hinreichend groß ist.

Theorem (L 2017)

Seien $n, k, \delta \in \mathbb{N}$ mit $k < n$ und $(n - k) \mid \delta$. Dann existiert ein vollständiger MDP (n, k, δ) Faltungscode, falls der zugrundeliegende Körper hinreichend groß ist.

Superreguläre Matrizen

Definition

Eine Toeplitz-Matrix der Form $\begin{pmatrix} a_1 & & 0 \\ \vdots & \ddots & \\ a_r & \cdots & a_1 \end{pmatrix} \in \mathbb{F}^{r \times r}$ heißt **superregulär**, falls alle ihre Minoren, die nicht trivialerweise Null sind, ungleich Null sind.

Bemerkung

Man kann den Begriff der Superregularität für Matrizen beliebiger Strukturen definieren, deren Minoren, die nicht trivialerweise Null sind, ungleich Null sind.

Konstruktion von vollständigen MDP Faltungscodes

Lemma (GRS 2006)

Für $a, b \in \mathbb{N}$ mit $b < a$ sei

$$X_a^b := \begin{bmatrix} 1 & & & & & 0 \\ \binom{b}{1} & \ddots & & & & \\ \vdots & \ddots & & & & \\ \binom{b}{b-1} & & & & & \\ 1 & \ddots & & & & \\ & \ddots & & & & \\ 0 & & 1 & \binom{b}{b-1} & \cdots & \binom{b}{1} \quad 1 \end{bmatrix} \in \mathbb{Z}^{a \times a}.$$

und $\hat{X} := (X_a^b)_{j_1,\ldots,j_r}^{i_1,\ldots,i_r}$ sei gebildet aus den Zeilen $1 \leq i_1 < \cdots < i_r \leq a$ und Spalten $1 \leq j_1 < \cdots < j_r \leq a$ von X^b. Dann gilt $\det(\hat{X}) \geq 0$ und $\det(\hat{X}) > 0 \Leftrightarrow j_l \in \{i_l - b, \ldots, i_l\}$ für $l = 1, \ldots, r$.

Konstruktion von vollständigen MDP Faltungscodes

Theorem (L 2017)

Seien $n, k, \delta \in \mathbb{N}$ mit $k < n$ und $(n-k) \mid \delta$.

1. *Setze $\nu = \delta/(n-k)$, $a := (\nu + L + 1)n$ sowie $b := \nu n + k$.*
2. *Berechne X_a^b.*
3. *Streiche die ersten $\nu n + k$ Zeilen von X_a^b.*
4. *Abwechselnd wähle $n-k$ Zeilen von X_a^b und streiche k Zeilen von X_a^b.*

Die resultierende Matrix ist eine partielle Kontrollmatrix eines vollständigen MDP (n, k, δ) Faltungscodes, falls die Charakteristik des zugrundeliegenden Körpers größer als $\binom{\nu n+k}{\lfloor 1/2(\nu n+k) \rfloor}^{(n-k)(L+1)} \cdot ((n-k)(L+1))^{1/2(n-k)(L+1)}$ ist.

Bemerkung

Für die Charakteristik: Die Determinante einer $A \times A$-Matrix mit größtem Eintrag gleich B ist höchstens $B^A \cdot A^{A/2}$.

Konstruktion von vollständigen MDP Faltungscodes

Beispiel

Konstruktion eines vollständigen MDP $(3, 1, 4)$ *Faltungscodes:* $\nu = 2, L = 4$ *und* $\nu n + k = 7$. *Man erhält die Kontrollmatrix* $H(z) = H_0 + H_1 z + H_2 z^2$ *mit* $H_2 = \begin{bmatrix} 1 & 7 & 21 \\ 0 & 1 & 7 \end{bmatrix}$, $H_1 = \begin{bmatrix} 35 & 35 & 21 \\ 21 & 35 & 35 \end{bmatrix}$ *und* $H_0 = \begin{bmatrix} 7 & 1 & 0 \\ 21 & 7 & 1 \end{bmatrix}$ *über einem Körper mit Charakteristik größer als* $\binom{7}{3}^{2 \cdot 7} (2 \cdot 7)^7 \approx 4,36 \cdot 10^{29}$.

Konstruktion von vollständigen MDP Faltungscodes

Proposition (ANP 2016)

Sei α ein primitives Element des endlichen Körpers $\mathbb{F} = \mathbb{F}_{p^N}$ und $B = [b_{i,l}]$ eine Matrix über $\mathbb{F}$ mit den folgenden Eigenschaften:

1. *falls $b_{i,l} \neq 0$, dann $b_{i,l} = \alpha^{\beta_{i,l}}$ für eine natürliche Zahl $\beta_{i,l}$*
2. *falls $b_{i,l} = 0$, dann $b_{i',l} = 0$ für alle $i' > i$ oder $b_{i,l'} = 0$ für alle $l' < l$*
3. *falls $l < l'$, $b_{i,l} \neq 0$ und $b_{i,l'} \neq 0$, dann $2\beta_{i,l} \leq \beta_{i,l'}$*
4. *falls $i < i'$, $b_{i,l} \neq 0$ und $b_{i',l} \neq 0$, dann $2\beta_{i,l} \leq \beta_{i',l}$.*

Sei N größer als jeder Exponent von α, der als nichttrivialer Summand bei der Berechnung einer beliebigen Minore von B auftritt. Dann ist B superregulär, d.h. alle Minoren, die nicht trivialerweise Null sind, sind ungleich Null.

ANP 2016: P.J. Almeida, D. Napp and R. Pinto. Superregular matrices and applications to convolutional codes. Linear Algebra and its Applications 499, 1-25, 2016.

Konstruktion von vollständigen MDP Faltungscodes

Theorem (L 2017)

Seien $n, k, \delta \in \mathbb{N}$ mit $k < n$ und $(n-k) \mid \delta$ und sei α ein primitives Element des endlichen Körpers $\mathbb{F} = \mathbb{F}_{p^N}$ mit $N > (L+1) \cdot 2^{(\nu+2)n-k-1}$. Dann ist $H(z) = \sum_{i=0}^{\nu} H_i z^i$ mit

$$H_i = \begin{bmatrix} \alpha^{2^{in}} & \dots & \alpha^{2^{(i+1)n-1}} \\ \vdots & & \vdots \\ \alpha^{2^{(i+1)n-k-1}} & \dots & \alpha^{2^{(i+2)n-k-2}} \end{bmatrix} \text{ für } i = 0, \dots, \nu = \frac{\delta}{n-k}$$

eine Kontrollmatrix eines vollständigen MDP (n, k, δ) Faltungscodes.

Konstruktion von vollständigen MDP Faltungscodes

Beispiel

Konstruktion eines vollständigen MDP $(3, 1, 4)$ *Faltungscodes* $(\nu = 2, L = 4)$*: Setze* $H(z) = H_0 + H_1 z + H_2 z^2$ *mit*

$$H_0 = \begin{bmatrix} \alpha & \alpha^2 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha^8 \end{bmatrix}, H_1 = \begin{bmatrix} \alpha^8 & \alpha^{16} & \alpha^{32} \\ \alpha^{16} & \alpha^{32} & \alpha^{64} \end{bmatrix},$$

$$H_2 = \begin{bmatrix} \alpha^{64} & \alpha^{128} & \alpha^{256} \\ \alpha^{128} & \alpha^{256} & \alpha^{512} \end{bmatrix}$$ *und wähle* $N > 7 \cdot 2^{10} \approx 2^{13}$.

Im Gegensatz zur vorherigen Konstruktion kann die Charakteristik des zugrundeliegenden Körpers beliebig klein gewählt werden, allerdings ist die Kardinalität des Körpers selbst mindestens $2^{7 \cdot 2^{10}} = 2^{7168}$*, was deutlich größer ist als zuvor.*

Notwendige Größe des Körpers für die Existenz von MDP Faltungscodes

Theorem (HST 2008)

Seien $B_r := \frac{1}{2}\left(\frac{1}{r}\binom{2(r-1)}{r-1} + \binom{r-1}{\lfloor\frac{r-1}{2}\rfloor}\right)$ *und* $|\mathbb{F}| > B_r$. *Dann existiert eine* $r \times r$ *superreguläre Toeplitz-Matrix über* $\mathbb{F}$.
Es gelte $(n-k) \mid \delta$ *und* $|\mathbb{F}| > B_{(L+1)(n-1)}$. *Dann existiert ein MDP* (n, k, δ) *Faltungscode über* $\mathbb{F}$.

Vermutung (GRS 2006)

Für $l \geq 5$ *existiert eine superreguläre* $l \times l$*-Toeplitz-Matrix über* $\mathbb{F}_{2^{l-2}}$.

HST 2008: R. Hutchinson, R. Smarandache, J. Trumpf. On superregular matrices and MDP convolutional codes. Lin Alg Appl 428, 2585-2596.

MDP Faltungscodes mit Rate $1/n$ und Grad 1

Theorem (L 2017)

Ein MDP $(2, 1, 1)$ *Faltungscode über* $\mathbb{F}$ *existiert genau dann wenn* $|\mathbb{F}| \geq 3$.
Außerdem gilt in diesem Fall: MDP $\Leftrightarrow$ *vollständig MDP*

Theorem (L 2017)

Für $n \geq 3$ *existiert ein MDP* $(n, 1, 1)$ *Faltungscode über* $\mathbb{F}$ *genau dann wenn* $|\mathbb{F}| \geq n$.
Außerdem gilt in diesem Fall: MDP $\Leftrightarrow$ *reversibel MDP*

$(n, n-1, 1)$ MDP Faltungscodes für $n \geq 3$

Bemerkung

Die MDP $(n, n-1, 1)$ *Faltungscodes sind dual zu den MDP* $(n, 1, 1)$ *Faltungscodes, d.h. es gilt dieselbe Schranke für die Größe des Körpers, nämlich n.*
Für einen vollständigen MDP $(n, n-1, 1)$ *Faltungscode benötigt man* $|\mathbb{F}| \geq n+1$.

$(n, n-1, 1)$ MDP Faltungscodes für $n \geq 3$

Bemerkung

Die MDP $(n, n-1, 1)$ *Faltungscodes sind dual zu den MDP* $(n, 1, 1)$ *Faltungscodes, d.h. es gilt dieselbe Schranke für die Größe des Körpers, nämlich n.*
Für einen vollständigen MDP $(n, n-1, 1)$ *Faltungscode benötigt man* $|\mathbb{F}| \geq n+1$.

Bemerkung

Die erforderliche Größe des Körpers für einen MDP $(n, n-1, 1)$ *Faltungscode ist deutlich geringer als die erforderliche Größe des Körpers für eine superreguläre Toeplitz-Matrix, aus der man einen solchen MDP Faltungscode konstruieren kann.*

$(n, n-1, 1)$ MDP Faltungscodes für $n \geq 3$

Bemerkung

Die MDP $(n, n-1, 1)$ *Faltungscodes sind dual zu den MDP* $(n, 1, 1)$ *Faltungscodes, d.h. es gilt dieselbe Schranke für die Größe des Körpers, nämlich n.*
Für einen vollständigen MDP $(n, n-1, 1)$ *Faltungscode benötigt man* $|\mathbb{F}| \geq n+1$.

Bemerkung

Die erforderliche Größe des Körpers für einen MDP $(n, n-1, 1)$ *Faltungscode ist deutlich geringer als die erforderliche Größe des Körpers für eine superreguläre Toeplitz-Matrix, aus der man einen solchen MDP Faltungscode konstruieren kann.*
Beispiel: ein MDP $(5, 1, 1)$ *Faltungscode existiert über* $\mathbb{F}_5$*, während eine* $(L+1)(n-1) \times (L+1)(n-1)$ *superreguläre Toeplitz-Matrix für* $n = 5$ *und* $L = 1$ *erst über* $\mathbb{F}_{31}$ *existiert.*

$(n, n-1, \delta)$ MDP Faltungscodes für $n \geq \delta + 2$

Theorem (L 2017)

Falls $\delta \leq n-2$, d.h. $k > \delta$ und $L = \nu = \delta$, sowie $|\mathbb{F}| > (e-1) \cdot n^L \cdot L!$, dann existiert ein $(n, n-1, \delta)$ MDP Faltungscode über $\mathbb{F}$.

$(n, n-1, \delta)$ MDP Faltungscodes für $n \geq \delta + 2$

Theorem (L 2017)

Falls $\delta \leq n-2$, d.h. $k > \delta$ und $L = \nu = \delta$, sowie $|\mathbb{F}| > (e-1) \cdot n^L \cdot L!$, dann existiert ein $(n, n-1, \delta)$ MDP Faltungscode über $\mathbb{F}$.

Bemerkung

Für $2 \leq \delta \leq n-2$ liefert diese Schranke ein besseres Ergebnis als wenn man die vermutete Schranke $2^{(L+1)(n-1)-2}$ für superreguläre Toeplitz-Matrizen verwendet.

$(n, n-1, 2)$ MDP Faltungscodes für $n \geq 4$

In diesem Fall gilt $\nu = \delta = 2$ und $L = 2$.

Theorem (L 2017)

Für einen MDP Faltungscode mit diesen Parametern liegt die erforderliche Mindestgröße des zugrundeliegenden Körpers zwischen $2n-1$ *und* $1/2(n-1)(3n-2)+1$.

$(n, n-1, 2)$ MDP Faltungscodes für $n \geq 4$

In diesem Fall gilt $\nu = \delta = 2$ und $L = 2$.

Theorem (L 2017)

Für einen MDP Faltungscode mit diesen Parametern liegt die erforderliche Mindestgröße des zugrundeliegenden Körpers zwischen $2n-1$ *und* $1/2(n-1)(3n-2)+1$.

Bemerkung

(i) Für $n = 4$ *ist* $|\mathbb{F}| \geq 9$ *notwendig und* $|\mathbb{F}| \geq 16$ *hinreichend. Beispiel für einen MDP* $(4, 3, 2)$ *Faltungscode über* $\mathbb{F}_{13}$*:*
$H_0 = (1, 1, 1, 1)$, $H_1 = (1, 2, 3, 4)$ *und* $H_2 = (0, 0, 5, 11)$.
Die notwendige Größe des Körpers für eine entsprechende superreguläre Toeplitz-Matrix wäre 59.

$(n, n-1, 2)$ MDP Faltungscodes für $n \geq 4$

In diesem Fall gilt $\nu = \delta = 2$ und $L = 2$.

Theorem (L 2017)

Für einen MDP Faltungscode mit diesen Parametern liegt die erforderliche Mindestgröße des zugrundeliegenden Körpers zwischen $2n-1$ *und* $1/2(n-1)(3n-2)+1$.

Bemerkung

(i) Für $n = 4$ *ist* $|\mathbb{F}| \geq 9$ *notwendig und* $|\mathbb{F}| \geq 16$ *hinreichend. Beispiel für einen MDP* $(4, 3, 2)$ *Faltungscode über* $\mathbb{F}_{13}$*:*
$H_0 = (1, 1, 1, 1)$, $H_1 = (1, 2, 3, 4)$ *und* $H_2 = (0, 0, 5, 11)$.
Die notwendige Größe des Körpers für eine entsprechende superreguläre Toeplitz-Matrix wäre 59.
(ii) Hinreichend für reversibel: $|\mathbb{F}| \geq 3n^2 - 3n + 2$
Hinreichend für vollständig: $|\mathbb{F}| \geq 5n^2 - 3n + 2$