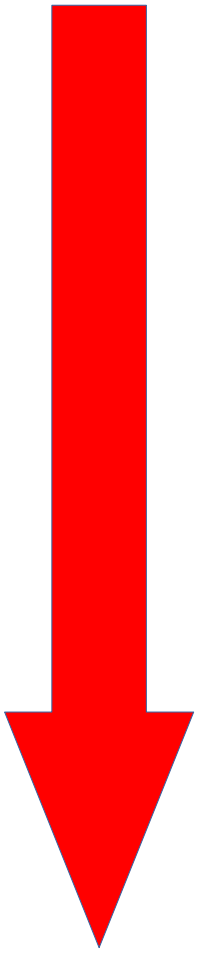
Proseminar Kodierungstheorie
Abschnitt 7:

Dualer Code, Paritätsprüf-Matrix und Syndrom-Dekodierung

Von: Gedeon Prosch
Ort/Datum: Düsseldorf den 31.05.2021

Gliederung:

Start



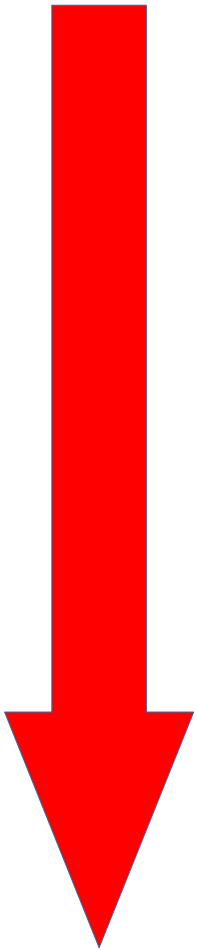
Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Hier steht immer, was wir im Detail betrachten werden.

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Wiederholung

- Inneres Produkt
  Lemma 7.1 [Rechenregeln des Inneren Produkts]

- Generator Matrix
  Rückblick auf Bsp 5.6

Das Innere Produkt

Das innere Produkt $\boldsymbol{u}\cdot\boldsymbol{v}$ *, mit den Vektoren:* $u=(u_1 u_2 \ldots u_n)$ *und* $v=(v_1 v_2 \ldots v_n)\in V(n,q)$
ist Definiert als der Skalar:

$$u\cdot v = u_1 v_1 + u_2 v_2 + \ldots + u_n v_n$$

Beispiele des $V(4,2)$: $(1001)\cdot(1101)=0$ $(1111)\cdot(1110)=1$
Beispiele des $V(4,3)$: $(2011)\cdot(1210)=0$ $(1212)\cdot(2121)=2$

Falls $\boldsymbol{u}\cdot\boldsymbol{v}=0$ *gilt, nennt man* $\boldsymbol{u}$ *und* $\boldsymbol{v}$ *orthogonal*

Lemma 7.1 [Rechenregeln des Inneren Produkts]:

Seien $\boldsymbol{u}$, $\boldsymbol{v}$ *und* $\boldsymbol{w}$ *aus* $V(n,q)$ *und* $\lambda, \mu \in GF(q)$, *dann gilt:*
$(i)\ \boldsymbol{u}\cdot\boldsymbol{v}=\boldsymbol{v}\cdot\boldsymbol{u}$
$(ii)\ (\lambda\boldsymbol{u}+\mu\boldsymbol{v})\cdot\boldsymbol{w}=\lambda(\boldsymbol{u}\cdot\boldsymbol{w})+\mu(\boldsymbol{v}\cdot\boldsymbol{w})$

Lemma 7.1 [Rechenregeln des Inneren Produkts]:

Seien $\boldsymbol{u}, \boldsymbol{v}$ *und* $\boldsymbol{w}$ *aus* $V(n,q)$ *und* $\lambda, \mu \in GF(q)$, *dann gilt*:

$(i)\ \boldsymbol{u}\cdot\boldsymbol{v} = \boldsymbol{v}\cdot\boldsymbol{u}$

$(ii)\ (\lambda\boldsymbol{u} + \mu\boldsymbol{v})\cdot\boldsymbol{w} = \lambda(\boldsymbol{u}\cdot\boldsymbol{w}) + \mu(\boldsymbol{v}\cdot\boldsymbol{w})$

Die Generator Matrix

Wiederholungen
(Siehe Bsp. 5.6)

$$\begin{bmatrix}1&1&1&1&1&1&1\\1&0&0&0&1&0&1\\1&1&0&0&0&1&0\\0&1&1&0&0&0&1\end{bmatrix} \xrightarrow[r_3 \to r_3 - r_1]{r_2 \to r_2 - r_1} \begin{bmatrix}1&1&1&1&1&1&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&1&1&0&0&0&1\end{bmatrix} \xrightarrow[r_4 \to r_4 - r_2]{r_3 \to r_3 - r_2} \begin{bmatrix}1&0&0&0&1&0&1\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\\0&0&0&1&0&1&1\end{bmatrix}$$

$$\xrightarrow{r_2 \to r_2 - r_3} \begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&1&1&0&1\\0&0&0&1&0&1&1\end{bmatrix} \xrightarrow{r_3 \to r_2 - r_4} \begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix}$$

Das Tolle an einer Erzeugendenmatrix:

Sei $\boldsymbol{u}$ *ein beliebiges Codewort aus* C,

dann können wir $\boldsymbol{u}$ *schreiben als:* $\boldsymbol{u} = \sum_{i=1}^{k} \lambda_i \boldsymbol{r}_i$,

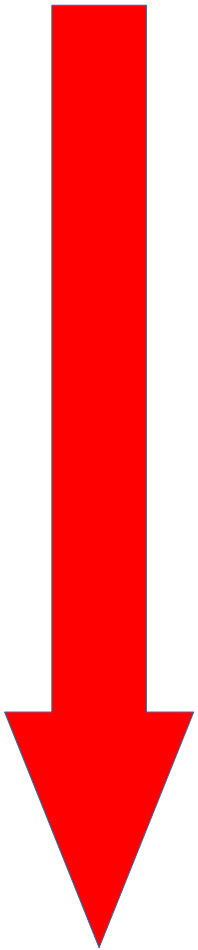
wobei λ_i *Skalare sind*

wobei die $\boldsymbol{r}_i$ die Reihen der Matrix sind:

$$\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix} = \begin{bmatrix}r_1\\r_2\\r_3\\r_4\end{bmatrix}$$

Gliederung:

Start



Ende

- Wiederholung
- 
  Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Einleitung

Generelle Informationen zum Vortrag

Einleitung

Ziel des Vortrags

- Vermittlung der 3 Begriffe „dualer Code“, „Paritätsprüf-Matrix“ und „Syndrom decodierung“
- Anwenden der Begriffe auf ein großes Beispiel. (ISBN code)
- Festigung des gelernten Wissens
- Das Vortragen Üben

Stil des Vortrags

- Offen, Interaktiv, wie eine Übungsgruppe oder ein kleingruppen Tutorium
- Fragen und Fehlerkorrektur jederzeit erwünscht
- Zusammenfassung im Plenum, anstelle als Folie

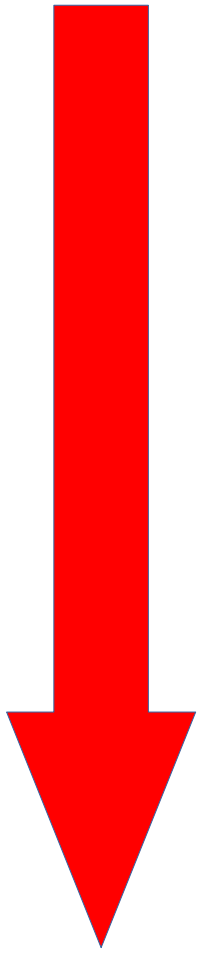
Aufgabe als Zuschauer

Pro Begriff zwei Abschnitte aufschreiben:

(i) Wie ist der Begriff definiert und was versteht ihr darunter?
(ii) Welche Eigenschaften/Folgerungen haben wir über den Begriff gelernt?

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Dualer Code
- Definition

- Beispiel 7.2
  [Beispiele für duale Codes]
- Lemma 7.3
[Dualer Code und Erzeugermatrix]

- Satz 7.5
  [dualer Code von dualem Code]

Dualer Code

Sei C ein linearer $[n, k]-$code.
Wir definieren $C^{\perp}$ als:
Die Menge der zu jedem Codewort orthogonalen Vektoren aus $V(n, q)$.
Der duale code von C ist definiert als ebendiese Menge. Geschrieben:

$$C^{\perp} \stackrel{\text{def}}{=} \{ \boldsymbol{v} \in V(n, q) \mid \boldsymbol{v} \cdot \boldsymbol{u} = 0 \quad \text{für alle } \boldsymbol{u} \in C \}$$

Beispiel 7.2 [Beispiele für dualen Code]:
Es ist einfach zu sehen, dass

(i) Wenn

$$C = \begin{Bmatrix} 0000 \\ 1100 \\ 0011 \\ 1111 \end{Bmatrix}, \text{ dann ist } C^{\perp} = C.$$

(ii) Wenn

$$C = \begin{Bmatrix} 000 \\ 110 \\ 011 \\ 101 \end{Bmatrix}, \text{ dann ist } C^{\perp} = \begin{Bmatrix} 000 \\ 111 \end{Bmatrix}.$$

Lemma 7.3 [Dualer Code und Erzeugendenmatrix]

Angenommen C ist ein $[n, k]$*–Code mit der* Erzeugenden-Matrix G.
Dann ist ein Vektor v aus $V(n, q)$ *genau dann* $\in C^{\perp}$, *wenn* $\boldsymbol{v}$ *orthogonal zu jeder reihe von G ist*.
d. h. $\boldsymbol{v} \in C^{\perp} \Leftrightarrow \boldsymbol{v} G^{T} = 0$, *wobei* G^{T} *die Transponierte Matrix von G ist*.

Beweis:
$(\Rightarrow)$ *Die Reihen von G sind Codewörter, d. h.* $v \in C^{\perp} \Rightarrow \boldsymbol{v} G^{T} = 0$ *folgt direkt aus der Defintion*.
$(\Leftarrow)$ *Wir nehmen an* $\boldsymbol{v}\,\boldsymbol{r}_i = 0$, *wobei* $\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_k$ *die Reihen von G seien*.

Sei $\boldsymbol{u}$ *ein beliebiges Codewort aus C, dann können wir* $\boldsymbol{u}$ *schreiben als*: $\boldsymbol{u} = \sum_{i=1}^{k} \lambda_i \boldsymbol{r}_i$.

Daraus ergibt sich:

$$\boldsymbol{v} \cdot \boldsymbol{u} \overset{\text{nutze Erzeugendenmatrix}}{=} \boldsymbol{v} \cdot \sum_{i=1}^{k} \lambda_i \boldsymbol{r}_i \overset{\text{Lemma } 7.1(ii)}{=} \sum_{i=1}^{k} \lambda_i (\boldsymbol{v} \cdot \boldsymbol{r}_i) \overset{\text{dualer code}}{=} \sum_{i=1}^{k} \lambda_i 0 = 0.$$

Lemma $7.1(ii)$: $(\lambda \boldsymbol{u} + \mu \boldsymbol{v}) \cdot \boldsymbol{w} = \lambda (\boldsymbol{u} \cdot \boldsymbol{w}) + \mu (\boldsymbol{v} \cdot \boldsymbol{w})$

(B) Lemma 7.4 [Dualer Code ist Linearer [n,n-k]-Code]

C sei ein $[n, k]-$ *Code über* $GF(q)$.
Dann ist der duale code $C^{\perp}$ *von C ein linearer* $[n, n-k]-$ *Code*.

Beweis $[C^{\perp}$ *ist linearer Code*]:
Angenommen wir haben $\boldsymbol{v}_1, \boldsymbol{v}_2 \in C^{\perp}$ *und* $\lambda, \mu \in GF(q)$.
Dann gilt für alle $u \in C$,

$$(\lambda \boldsymbol{v}_1 + \mu \boldsymbol{v}_2)\cdot \boldsymbol{u} \overset{Lemma 7.1}{=} \lambda(\boldsymbol{v}_1 \cdot \boldsymbol{u}) + \mu(\boldsymbol{v}_2 \cdot \boldsymbol{u})$$
$$= \lambda 0 + \mu 0 = 0.$$

Also ist $\lambda \cdot \boldsymbol{v}_1 + \mu \cdot \boldsymbol{v}_2 \in C^{\perp}$, *wodurch* $C^{\perp}$ *nach Beispiel* 4.1 *linear ist*.

(B) Beweis Fortsetzung [(dim (C^⊥) = n-k]

Sei $G=[g_{ij}]$ *eine Erzeugendenmatrix für* C.

Nach Lemma 7.2 sind die Elemente von $C^{\perp}$ *die Vektoren* $\boldsymbol{v}=v_1 v_2 \cdots v_n$, *die die Gleichung*

$$\sum_{j=1}^{n} g_{ij} v_j = 0 \text{ für } i=1,2,\ldots,k \text{ erfüllen}.$$

Dies ist ein System von k unabhängiger gleichartiger Gleichungen in n unbekannten.

Durch die Lineare Algebra wissen wir:
Die Lösungsmenge davon hat dim $(n-k)$.
Also sind wir hier eigentlich schon fertig.
Wir machen hier jedoch ein kleines Alternatives Beweisende.

(B) Beweis Fortsetzung [(dim (C^⊥) = n-k]

Sei $G=[g_{ij}]$ *eine Erzeugendenmatrix für* C.

Wenn C_1 *und* C_2 *äquivalent sind , dann sind dies natürlich auch* $C_1^{\perp}$ *und* $C_2^{\perp}$.

Dementsprechend reicht es $\dim(C^{\perp})=n-k$ *für folgenden Fall zu Zeigen*:

C habe eine Standartform ErzeugendenMatrix

$$G=\begin{bmatrix} 1 & \cdots & 0 & a_{11} & \cdots & a_{1,n-k} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & a_{k1} & \cdots & a_{k,n-k} \end{bmatrix},$$

$$C^{\perp}=\left\{(\nu_1,\nu_2,\ldots,\nu_n)\in V(n,q)\,\middle|\quad \nu_i+\sum_{j=1}^{n-k} a_{ij}=0,\ i=1,2,\ldots,k\right\}.$$

dann existiert für alle q^{n-k} *Möglichkeiten aus* $(\nu_{k+1},\nu_2,\ldots,\nu_n)$

ein unabhängiger Vektor $(\nu_1,\nu_2,\ldots,\nu_n)$ *in* $C^{\perp}$.

Das Bedeutet $|C^{\perp}|=q^{n-k}$ *und letztenendes dann* $\dim(C^{\perp}=n-k)$.

Platz zum Malen(nur bei Bedarf)

Satz 7.5 [dualer Code von dualem Code]

Für jeden $[n, k]-$*code* C*, ist gilt* $(C^{\perp})^{\perp} = C$.

Beweis:

(i) $C \subseteq (C^{\perp})^{\perp}$:

Da jeder Vektor $\in C$ *orthogonal zu jedem Vektor* $\in C^{\perp}$ *ist, folgt* (i).

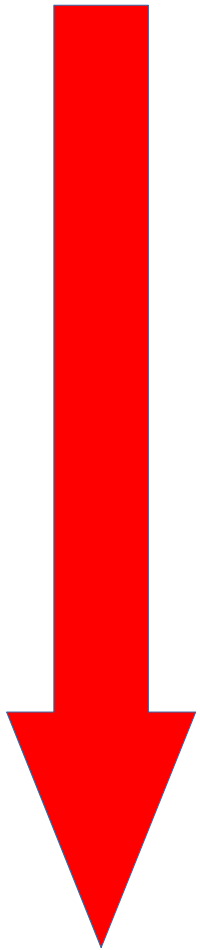
(ii) $(C^{\perp})^{\perp} \subseteq C$:

Durch Lemma 7.4*, gilt:* $\dim((C^{\perp})^{\perp}) = n - (n-k) = k = \dim C$*, daraus folgt* (ii)

Insgesamt folgt Satz 7.5.

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Paritätsprüf-Matrix

- Definition

- Satz 7.6 [Erzeugung der P.p.M]

- Beispiel 7.7[Erzeugung der P.p.M]

- Definition [standartform der P.p.M]

Definition Paritätsprüf-Matrix

Eine Paritätsprüf-Matrix H für einen $[n,k]-$Code ist eine Erzeugendenmatrix von $C^{\perp}$.

Das bedeutet, H ist eine $(n-k)\times n$ Matrix,

welche die Gleichung $GH^T=\mathbf{0}$ erfüllt.

(Wobei H^T die Transponierte von H und $\mathbf{0}$ die Nullmatrix ist.)

Aus Lemma 7.2 und Satz 7.5 folgt:

Wenn H eine Paritätsprüf-Matrix von C ist, dann ist

$$C=\{\boldsymbol{x}\in V(n,q)\,|\,\boldsymbol{xH^T}=\mathbf{0}\}.$$

Auf diese Art lässt sich jeder lineare code vollständig durch eine Paritätsprüf-Matrix beschreiben.

In Beispiel 7.4 (i), ist $\begin{bmatrix}1100\\0011\end{bmatrix}$ *eine* Erzeugenden-Matrix ***und*** *eine* Paritätsprüf-Matrix,

wohingegen in (ii), $[111]$ nur eine Paritätsprüf-Matrix ist.

(B) Erklärung Paritätsprüf-Matrix

*Die **Reihen** einer Paritätsprüf-Matrix sind Paritätsprüfungen der Codewörter .*
Sie sagen aus ,
dass bestimmte Linearkombinationen der Position jedes Codewortes null sind .
Ein Beispiel : wenn ,

$$H = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix},$$

dann ist C der code :

$$\{(x_1, x_2, x_3, x_4) \in V(4,2) \mid x_1 + x2 = 0 , x_3 + x_4 = 0\}.$$

Die Gleichungen $x_1 + x_2 = 0$ und $x_3 + x_4 = 0$, werden Paritätsprüf – Gleichungen genannt .
Wenn $H = [111]$, dann besteht C aus jenen Vektoren $\in V(3,2)$,
deren Position sich zu 0 (mod2) aufsummiert.

Allgemein gesagt , kann der in *Aufgabe* 5.2 *auftauchende uniform gewichtete Code E_n*
als die Menge aller Vektoren $(x_1 x_2 \ldots x_n)$ aus $V(n,2)$, welche die Paritätsprüf – Gleichung

$$x_1 + x_2 + \ldots + x_n = 0 \text{ erfüllt .}$$

Satz 7.6 [erzeugen einer Paritätsprüf-Matrix]

Sei $G=[I_k|A]$ *die Generatormatrix eines* $[n,k]-$*codes* C, *in Standartform.*
Dann ist eine paritätsprüf-Matrix für C *duch* $H=[-A^T|I_{n-k}]$ *gegeben.*

Beweis: *Seien*

$$G=\left[\begin{array}{ccc|ccc} 1 & & 0 & a_{11} & \cdots & a_{1,n-k} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & a_{k1} & \cdots & a_{k,n-k} \end{array}\right],\ \text{und}\ H=\left[\begin{array}{ccc|ccc} -a_{11} & \cdots & -a_{k1} & 1 & & 0 \\ \vdots & & \vdots & & \ddots & \\ -a_{1,n-k} & \cdots & -a_{k,n-k} & 0 & & 1 \end{array}\right],$$ *wie beschrieben.*

Dann hat H *die benötigte Größe einer Paritätsprüf-Matrix und linear unabhängige Reihen.*

Daher reicht es nun zu Zeigen, dass jede Reihe von H *orthogonal zu jeder Reihe von* G *ist.*
Das Innere Produkt der $i-$*ten Reihen von* G *mit der* $j-$*ten Reihe von* H *ist jedoch*

$$0+\cdots+0+(-a_{ij})+0+\cdots+0+a_{ij}+0+\cdots+0=0.$$

Wodurch direkt Satz 7.6 Folgt.

Beispiel7.7 [erzeugen einer Paritätsprüf-Matrix]

Wir betrachen die Erzeugendenmatrix aus Beispiel $5.6(ii)$*, die in Standartform vorliegt* .

$$G=\left[\begin{array}{c|ccc} & 1 & 0 & 1 \\ I_4 & 1 & 1 & 1 \\ & 1 & 1 & 0 \\ & 0 & 1 & 1 \end{array}\right],$$

mit Satz 7.5 *wäre die Paritätsprüf-Matrix dann*:

$$H=\left[\begin{array}{cccc|c} 1 & 1 & 1 & 0 & \\ 0 & 1 & 1 & 1 & I_3 \\ 1 & 1 & 0 & 1 & \end{array}\right]$$

$(Die\ Minuszeichen\ sind\ im\ Binärfall\ hinfällig)$

Definition [Standardform der Paritätsprüf-Matrix]

Eine Praritätsprüf-Matrix ist in Standardform, wenn $H = [\, B \,|\, I_{n-k} \,]$ *gilt.*

Der Beweis von Satz 7.6 gilt in beide Richtungen, d.h.
wenn ein Code durch eine Paritätsprüfmatrix in Standartform

$$H = [\, B \,|\, I_{n-k} \,]$$

beschrieben ist,
dann ist

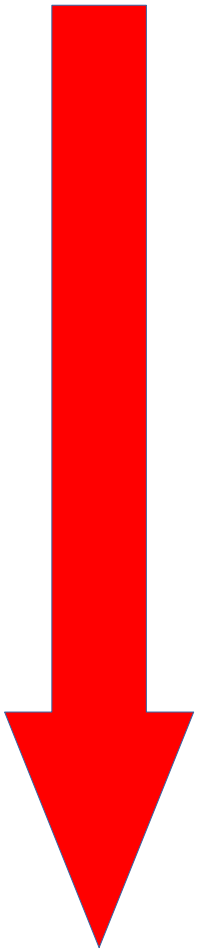
$$G = [\, I_k \,|\, -B^T \,]$$

eine Erzeugendenmatrix des Codes.

Wenn ein Code durch eine Paritätsprüfmatrix H beischrieben ist, welche nicht in Standardform vorligt, kann man H auf die selbe Art auf Standardform bringen, wie eine Erzeugendenmatrix.

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
-  Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Syndrom
- Definition

- Eigenschaften

Definition Syndrom

Angenommen H ist eine Paritätsprüf-Matrix eines $[n,k]-$*Codes.*
Für jeden Vektor $\boldsymbol{y}\in V(n,q)$ *bezeichnet man den* $1\,x\,(n-k)$ *Vektor*

$$S(\boldsymbol{y})=\boldsymbol{H}^{T},$$

als das syndrom von $\boldsymbol{y}$.

Anmerkungen:

(i) : *Wenn wir die Reihen von H mit* $\boldsymbol{h}_1,\boldsymbol{h}_2,\ldots,\boldsymbol{h}_{n-k}$ *bezeichnen, dann ist das syndrom*

$$S(y)=(\boldsymbol{y}\cdot\boldsymbol{h}_1,\boldsymbol{y}\cdot\boldsymbol{h}_2,\ldots,\boldsymbol{y}\cdot\boldsymbol{h}_{n-k}).$$

(ii) : $S(\boldsymbol{y})=0\Leftrightarrow\boldsymbol{y}\in C$.

(iii): *Alternativ kann man das syndrom von* $\boldsymbol{y}$ *auch mit dem Spaltenvektor* $H\,\boldsymbol{y}^{T}$ *definieren.* (*Dieser ist dann der zu unserer Definition tranponierte Vektor*)

Lemma 7.8 [syndrom und Nebenklasse]

Zwei Vektoren $\boldsymbol{u}$ *und* $\boldsymbol{v}$ *sind genau dann in der selben Nebenklasse von* C *, wenn sie die selben syndrome haben .*

Beweis :

$\boldsymbol{u}$ *und* $\boldsymbol{v}$ *sind in der selben Nebenklasse*

$$\Leftrightarrow \boldsymbol{u}+C=\boldsymbol{v}+C \quad \Leftrightarrow \quad \boldsymbol{u}-\boldsymbol{v}\in C \quad \Leftrightarrow \quad (\boldsymbol{u}-\boldsymbol{v})H^T=0$$

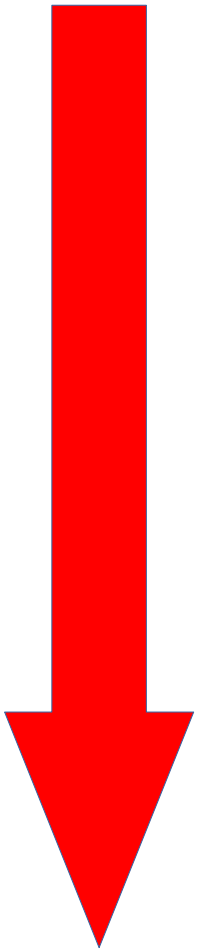
$$\Leftrightarrow \boldsymbol{u}H^T=\boldsymbol{v}H^T \quad \Leftrightarrow \quad S(\boldsymbol{u})=S(\boldsymbol{v})$$

Lemma 7.9:

Syndrom und Nebenklasse stehen in einer Eins zu Eins Beziehung .

Gliederung:

Start



Ende

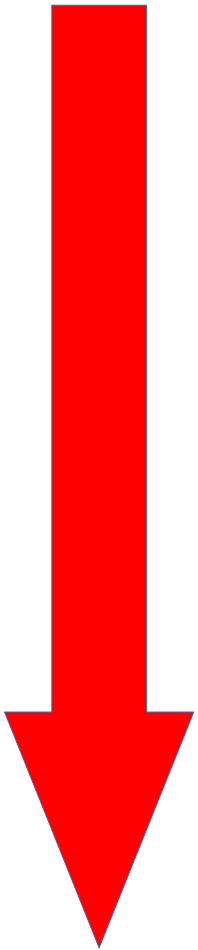
- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom

- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Pause :D (5 -10 Minuten)
Fragen klären, Aufs Klo Gehen
Oder Kurz an die Frische Luft ;)

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
-  Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Syndromdekodierung
- Dekodierungsalgorithmus

- Beispiel 7.10

Syndromdekodierung

In der herkömmlichen array decodierung, ist es für kleine n leicht den eingegangenen Vektor $\boldsymbol{y} \in$ dem Decodierungsarray zu finden.

Bei großen n können wir uns allerdings eine menge Zeit spaaren,
wenn wir mithilfe des syndroms die Nebenklasse bestimmen, die $\boldsymbol{y}$ enthält.
Damit erhalten wir nähmlich auch die Reihe im dekodierungsarray, in der $\boldsymbol{y}$ steht.

Das erreichen wir folgendermaßen:
Wir berechnen das syndrom $S(\boldsymbol{e})$ für die Hauptvektoren $\boldsymbol{e}$ jeder Nebenklasse.
Anschließend erweitern wir das herkömmliche Decodierungarray um eine Extra spalte,
indem wir die berechneten syndrome dazu auflisten.

Dekodierungalgorithmus

Das Hinzufügen der Syndromspalte ermöglicht es uns also, den Decodierungsalgorithmus zu berbessern:

Der Verbesserte Algorithmus ist jetzt:

Schritt 1: *Beim erhalten eines Vektors* $\boldsymbol{y}$, *berechne* $S(\boldsymbol{y}) = \boldsymbol{y}\boldsymbol{H}^{\boldsymbol{T}}$.

Schritt 2: *Finde* $\boldsymbol{y} \in$ *der zu dem syndrom gehörigen Zeile*

Schritt 3: *Dekodiere* $\boldsymbol{y}$ *als das Codewort in der obersten Zeile der gefundenen Spalte*

Beispiel 7.10 [Anwendung syndromdekodierun]

Schritt 1: *Beim erhalten eines Vektors* $\boldsymbol{y}$, *berechne* $S(\boldsymbol{y}) = \boldsymbol{y}\boldsymbol{H}^T$.
Schritt 2: *Finde* $\boldsymbol{y} \in$ *der zu dem syndrom gehörigen Zeile*
Schritt 3: *Dekodiere* $\boldsymbol{y}$ *als das Codewort in der obersten Zeile der gefundenen Spalte*

In Beispiel 6.5, $G = \begin{bmatrix} 1011 \\ 0101 \end{bmatrix}$, *wodurch mit Theorem* 7.6, $H = \begin{bmatrix} 1010 \\ 1101 \end{bmatrix}$ *eine Paritätsprüfmatrix davon ist*.

Dementsprechend sind die syndrome der Hauptvektoren der Untervekorräume:
$S(0000) = 00$, $S(1000) = 11$, $S(0100) = 01$, $S(0010) = 10$.
Das standart dekodierungarray wird dann:

Hauptvektoren				*syndrome*
0000	1011	0101	1110	00
1000	0011	1101	0110	11
0100	1111	0001	1010	01
0010	1001	0111	1100	10

Sei jetzt $\boldsymbol{y} = 1111$, *dann ist* $S(1111) = 01$, *suche daher* $1111 \in$ *Reihe* 3, *also spalte* 1.
Wir decodieren 1111 *also als* 1011.

Beispiel 7.10 (Fortsetzung)

Hauptvektoren				*syndrome*
0000	1011	0101	1110	00
1000	0011	1101	0110	11
0100	1111	0001	1010	01
0010	1001	0111	1100	10

Wird zu:

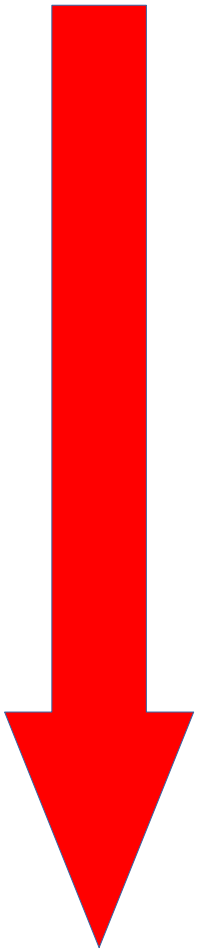
Hauptvektoren	*syndrome*
0000	00
1000	11
0100	01
0010	10

Dekodierungsalgorithmus:

$Codewort = y - Hauptvektor_{s(y)}$

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
-  Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Unvollständiges dekodieren
- Erklärung

- Beispiel 7.11
[Bsp Unvollständiges dekodiern]

Unvollständiges Dekodieren

Wenn wir ein Dekodierungsschema haben können wir mit der syndromdekodierung
eine Fallunterscheidung machen , bis zu welchem Fehlergrad dekodiert werden soll
und ab welchem Fehlergrad nicht mehr .
Genaugenommen können wir bei einem Code mit $d(C)=2t+1$ *oder* $2t$ *,*
für die Korrektur aller fehler vom grad $\leq t$ *garantieren und*
in manchen fällen auch fehler die größer als t sind finden .

Hierzu etwickeln wir folgendes Schema :
Ordne die Hauptvektoren der Nebenklassen wie gewöhnlich mit zunehmender Gewichtung an .
Teile das entstandene Array in Ober – und Unterseite auf :
Zur Oberseite zählen alle Zeilen deren Hauptvektoren Gewicht $\leq t$ *haben .*
Zur Unterseite zählen alle Zeilen deren Hauptvektoren bzw . Nebenklassen Gewicht $> t$ *haben .*
Wenn ein erhaltener Vektor $\boldsymbol{y}$ *nun ein syndrom im oberen Teil hat , decodieren wir ihn .*
Wenn ein erhaltener Vektor $\boldsymbol{y}$ *das syndrom im unteren Teil hat , forden wir ihn neu an .*

Beispiel 7.11 [Bsp. Unvollständiges Dekodieren]

$$\text{Sei } H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Nachdem wir die syndrome der Nebenklassen mit $S(\boldsymbol{y}) = \boldsymbol{y}\boldsymbol{H}^T$ *berechnet haben, erhalten wir:*

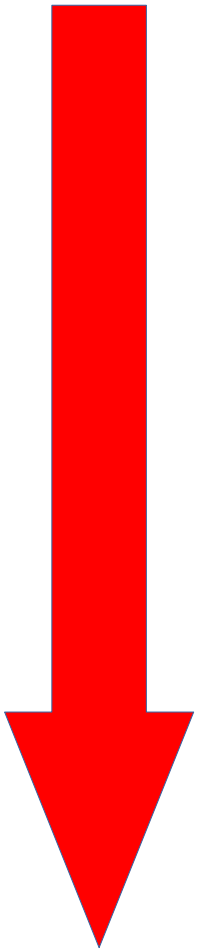
hauptvektor $f(z)$	*syndrome* z
00000	000
10000	110
01000	011
00100	100
00010	010
00001	001
.....	.....
11000	101
10001	111

(i) *wenn* $\boldsymbol{y} = 11111$, *dann ist* $S(\boldsymbol{y}) =$
$(11111 \cdot 10101 = 1, 11111 \cdot 11010 = 1, 11111 \cdot 01001 = 0)$
und das Codewort ist $11111 - 00010 = 11101.$

(ii) *wenn* $\boldsymbol{y} = 10011$, *dann ist* $S(\boldsymbol{y}) = 101$,
welches nicht in der Oberen Seite auftaucht.
d.h., dass mindestens 2 Fehler aufgetaucht sind.

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
-  Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Das ISBN Beispiel
- Erklärung

- Beispiel 7.11
[Bsp Unvollständiges dekodiern]

Beispiel 7.12 [Finde ISBN-10 Prüf-Algorithmus]

Wir wollen einen syndrom Dekodierungsalgorithmus für einen linearen $[10,8]$ *– Code über* $GF(11)$.
Hierfür sei unsere Paritäts-Prüf-Matrix

$$H=\begin{bmatrix}1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\end{bmatrix}.$$

Sei C nun der 10 *er – Code, den wir aus diesem* 11 *er – Code erhalten,*
*indem wir alle Codewörter loswerden, die eine '*10*' enthalten.*

In anderen Worten heißt das:
C besteht aus allen 10 *stelligen Dezimalzahlen* $\boldsymbol{x}=x_1x_2\ldots x_{10}$,
die die beiden Paritätsprüf – Gleichungen:

$$\sum_{i=1}^{10} x_i \equiv 0 \pmod{11}, \qquad \text{und} \qquad \sum_{i=1}^{10} i x_i \equiv 0 \pmod{11} \qquad \text{erfüllt.}$$

Eine schöne Übungsaufgabe für das Einschluss – Ausschluss – Verfahren ist es zu Zeigen,
dass C in diesem Fall, 82 644 629 *Codewörter hat.*
Wir nehmen hier allerdings an, dass diese Tatsache bereits Bewiesen ist.

Beispiel 7.12 [Finde ISBN-10 Prüf-Algorithmus]

Die Codewörter von C mit einer Erzeugenden-Matrix beschrieben werden.
Die finden wir, indem wir H auf Standartform bringen:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix} \xrightarrow{r_1 \to r_1 + r_2} \begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix} \xrightarrow{\substack{r_1 \to (-1) r_1 \\ r_2 \to (-1) r_2}}$$

$$\begin{bmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \xrightarrow{r_2 \to r_2 - 2 r_1} \begin{bmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 \end{bmatrix}$$

Mit Satz 7.6 ist dann $G = \left[\, I_8 \;\middle|\; \begin{matrix} 2 & 8 \\ 3 & 7 \\ 4 & 6 \\ 5 & 5 \\ 6 & 4 \\ 7 & 3 \\ 8 & 2 \\ 9 & 1 \end{matrix} \right]$

$$\left[\, I_8 \;\middle|\; \begin{matrix} -9 & -3 \\ -8 & -4 \\ -7 & -5 \\ -6 & -6 \\ -5 & -7 \\ -4 & -7 \\ -4 & -8 \\ -3 & -9 \\ -2 & -10 \end{matrix} \right]$$

Dadurch ist $C = \{(x_1, x_2, \ldots, x_8, 2x_1 + 3x_2 + \cdots + 9x_8, 8x_1 + 7x_2 + \cdots + x_8)\}$,
wobei $x_1, x_2, \ldots, x_8$ *über die Werte* 0,1,2,...,9 *läuft und wir haben keine Nummer '10' in den letzten beiden Spalten stehen.*

Beispiel 7.12 (Fortsetzung)

Beschreiben nun Schema für unvollständigen dekodier Algorithmus:
Angenommen $\boldsymbol{x}=(x_1, x_2, \ldots, x_{10})$ *ist das gesendete Codewort und*
$\boldsymbol{y}=(y_1, y_2, \ldots, y_{10})$ *der ankommende Vektor. Berechnen wir ersmal das syndrom*

$$(A, B)=\boldsymbol{y}\, H^T=\left(\sum_{i=1}^{10} y_i, \sum_{i=1}^{10} i y_i\right) \quad (\text{modulo } 11).$$

$$H^T=\begin{bmatrix} 1 & 1 \\ 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 1 & 5 \\ 1 & 6 \\ 1 & 7 \\ 1 & 8 \\ 1 & 9 \\ 1 & 10 \end{bmatrix}$$

Dann erhalten wir:

$$A=\sum_{i=1}^{10} y_i=\left(\sum_{i=1}^{10} x_i\right)+k \,(\text{mod } 11)$$

$$B=\sum_{i=1}^{10} i y_i=\left(\sum_{i=1}^{10} i\, x_i\right)+jk \,(\text{mod } 11)$$

Also erhalten wir aus A direkt die Fehlerstärke k und
durch BA^{-1} *die Fehler Position j.*

Beispiel 7.12 (Fortsetzung)

Das Schema für das Unvollständige dekodieren ist dann:

Schritt 1*: Berechne* (A, B) *von* $\boldsymbol{y}$

Schritt 2*: Mache Fallunterscheidung:*

(1) *wenn* $(A, B) = (0,0)$*, dann ist* $\boldsymbol{y}$ *Codewort und wir gehen von keinem Fehler aus.*

(2) *wenn* $A \neq 0$ *und* $B \neq 0$*, dann korrigieren wir den Einzelfehler,*
indem wir A *vom* $(BA^{-1})-$*sten wert von* $\boldsymbol{y}$ *abziehen*

(3) *Wenn entweder* $A = 0$ *oder* $B = 0$*, liegen mindestens* 2 *Fehler vor.*

(3) *kommt immer zu tragen, wenn Zwei stellen eines Codewortes Vertauscht wurden.*

Dann ist $A = 0$ *und* $B \neq 0$

$$A = \sum_{i=1}^{10} y_i \qquad B = \sum_{i=1}^{10} i y_i$$

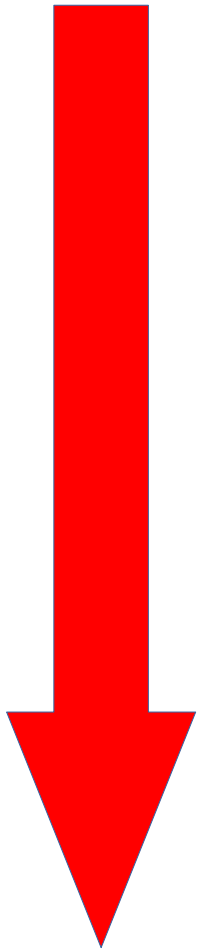
Wenn beispielsweise $\boldsymbol{y} = 0610271355$ *ist, dann sind* $A = 8$ *und* $B = 6.$

Dementsprechend ist $BA^{-1} = 6 * 8^{-1} = 6 * 7 = 42 = 9.$

Also hätte der $9.$ *Eintrag eine* $5 - 8 = -3 = 8$ *sein müssen.*

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
-  Bemerkung zum Beispiel
- Besprechung der Begriffe

Bemerkung zum Beispel

Bemerkungen zum Beispiel

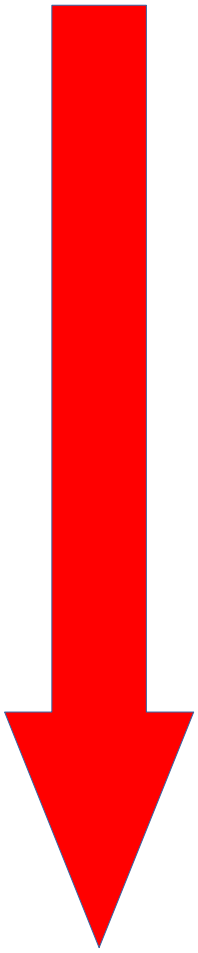
(1) *Habt Ihr bemerkt, wie viel schneller dieses Dekodierungsschema ist, als die brute–force Methode, die den erhaltenen Vektor mit allen Codewörtern vergleicht?*

(2) *Der Fakt, dass wir jeden Einzelfehler korrigieren können ist ein Indirekter Beweis, dass die Minimaldistanz des codes mindestens 3 ist.*
Desweiteren werden wir in Beispiel 8.8 sehen, dass man die Minimaldistanz direkt aus der Paritätsprüf-Matrix H ablesen kann.

(3) *In Kapitel 11 werden noch weitere Dezimal-Codes Thematisiert.*

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel

- Besprechung der Begriffe

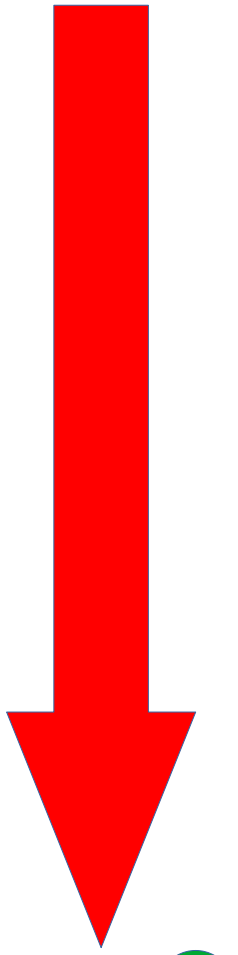
Ist jemand gegen spontanes drannehmen ?

-niemand?

Alles klar :)

Gliederung:

Start



Ende

- Wiederholung
- Einleitung
- Dualer Code
- Paritätsprüf-Matrix
- Syndrom
- Pause
- Syndromdekodierung
- Unvollständiges dekodieren
- Das ISBN- Beispiel
- Bemerkung zum Beispiel
- Besprechung der Begriffe

Ja, auch dieser Vortrag hat ein Ende :)

Ende!

Danke fürs Zuhören!