Codierungstheorie

Reinhold Hübl

Vorlesung 6 - WS 2022/23

lineare Codes

Ein linearer $[n, k]_q$–Code ist ein k–dimensionaler Untervektorraum $C \subseteq \mathbb{F}_q^n$.

Ein linearer Code kann beschreiben werden durch eine Erzeugermatrix, also eine $k \times n$–Matrix G, deren Zeilen eine Basis von C bilden.

Ein linearer Code kann beschrieben werden durch eine Paritätsprüfmatrix, also eine $(n-k) \times n$–Matrix H, für die gilt:

$$C = \{c \in \mathbb{F}_q^n \mid H \cdot \overrightarrow{c} = \overrightarrow{0}\}$$

Bemerkung

Das Dualitätsprinzip der linearen Algebra liefert Algorithmen zur Berechnung einer Erzeugermatrix G eines Codes C aus einer Paritätsprüfmatrix H und zur Berechnung einer Paritätsprüfmatrix H aus einer Erzeugermatrix G.

spezielle lineare Codes

Beispiel

Der n–**fache Wiederholungscode** $C \subseteq \mathbb{F}_q^n$ ist der $[n, 1, n]_q$–Code

$$C = \{(r, r, \ldots, r) \in \mathbb{F}_q^n | \; r \in \mathbb{F}_q\}$$

Beispiel

Der **Paritätsprüfcode** $C \subseteq \mathbb{F}_q^n$ der Länge n ist der $[n, n-1, 2]_q$–Code

$$C = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \mid \sum_{i=1}^{n} x_i = 0\}$$

spezielle lineare Codes

Bemerkung

Der n–fache Wiederholungscode hat Erzeugermatrix

$$G = (1 \ 1 \ \ldots \ 1)$$

und der Paritätsprüfcode der Länge n hat die Paritätsprüfmatrix

$$H = (1 \ 1 \ \ldots \ 1)$$

Die beiden Codes sind also dual zueinander.

spezielle lineare Codes

Übung

Bestimmen Sie eine Paritätsprüfmatrix des 5–fachen Wiederholungscodes über $\mathbb{F}_7$.

spezielle lineare Codes

Wir betrachen ein n von der Form $n = 2^k - 1$ und alle möglichen k–Tupel $v = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ mit $a_i \in \{0, 1\}$ ohne das Nulltupel $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Hiervon gibt es genau n Stück $v_1, \ldots, v_n$. Wir betrachten die $k \times n$–Matrix

$$H = (v_1 \ \ldots \ v_n)$$

mit den v_i als Spalten.

Satz

Die Matrix H ist die Paritätsprüfmatrix eines vollkommenen $[n, n-k]_2$–Codes C mit $d(C) = 3$.

Definition

Dieser Code C heißt **Hammingcode**

spezielle lineare Codes

Übung

Bestimmen Sie eine Paritätsprüfmatrix und eine Erzeugermatrix für den $[7, 4, 3]_2$–Hamming–Code

zyklische Codes

Definition

Ein linearer $[n,k]_q$–Code $C \subseteq \mathbb{F}_q^n$ heißt **zyklisch**, wenn gilt:
Ist $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in C$, so ist auch
$\widetilde{c} = (c_n, c_1, c_2, \ldots, c_{n-1}) \in C$.

Beispiel

Der lineare $[6,2]_2$–Code

$$C = \{(0,0,0,0,0,0), (1,0,1,0,1,0), (0,1,0,1,0,1), (1,1,1,1,1,1)\} \subseteq \mathbb{F}_2^6$$

ist zyklisch.

zyklische Codes

Für ein $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in \mathbb{F}_q^n$ bezeichnen wir mit $c^{[1]} = (c_n, c_1, c_2, \ldots, c_{n-1})$ das Element von $\mathbb{F}_q^n$, das dadurch entsteht, dass wir alle Komponenten um eine Stelle nach rechts verschieben.

Regel

Ein linearer $[n, k]_q$–Code C ist genau dann zyklisch, wenn gilt

$$c \in C \Longrightarrow c^{[1]} \in C$$

Satz

Ist $\mathbf{g_1}, \ldots, \mathbf{g_k}$ Basis eines $[n, k]_q$–Codes C, so ist C genau dann zyklisch, wenn $\mathbf{g_1}^{[1]}, \ldots, \mathbf{g_k}^{[1]} \in C$.

zyklische Codes

Übung

Überprüfen Sie, ob der lineare $[4,2]_7$–Code C mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 3 & 1 & 3 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

zyklisch ist.

zyklische Codes

Ein **Polynom** über $\mathbb{F}_q$ ist ein Ausdruck der Form

$$f(X) = a_0 + a_1 \cdot X + a_2 \cdot X^2 + \cdots + a_n \cdot X^n$$

mit $a_0, \ldots, a_n \in \mathbb{F}_q$ und mit einer Unbekannten X.
Die Zahlen $a_i \in \mathbb{F}_q$ heißen die **Koeffizienten** des Polynoms $f(X)$.
Ist $a_n \neq 0$, so heißt $\deg(f) = n$ der **Grad** von $f(X)$.
Mit $\mathbb{F}_q[X]$ bezeichnen wir die Menge der Polynome über $\mathbb{F}_q$.

Beispiel

$f(X) = 2X^6 + 7X^2 + 4X + 3 \in \mathbb{F}_{11}[X]$ ist ein Polynom vom Grad 6.

Regel

$\mathbb{F}_q[X]$ *ist (zusammen mit der Polynommultiplikation) ein Ring.*

zyklische Codes

Satz

Ist C ein zyklischer $[n,k]_q$–Code, so gibt es Elemente $g_0,\ldots,g_{n-k}\in\mathbb{F}_q$ und $h_0,\ldots,h_k\in\mathbb{F}_q$ mit den folgenden Eigenschaften

1. $\left(g_0+g_1X+\cdots+g_{n-k}X^{n-k}\right)\cdot\left(h_0+h_1X+\cdots+h_kX^k\right)=X^n-1$ *über* $\mathbb{F}_q$.
2. *Die Matrix*

$$G=\begin{pmatrix} g_0 & g_1 & \cdots & & \cdots & g_{n-k} & 0 & 0 & \cdots & 0\\ 0 & g_0 & \cdots & & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0\\ \vdots & & & \ddots & & & & & & \vdots\\ 0 & 0 & & g_0 & & & & & & g_{n-k}\end{pmatrix}$$

mit n Spalten und k Zeilen ist eine Erzeugermatrix von C.

zyklische Codes

Satz

1. *Die Matrix*

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & \dots & & \dots & h_1 & h_0 & 0 & \dots & 0 \\ \vdots & & & \ddots & & & & & & \vdots \\ 0 & 0 & & h_k & & & & & & h_0 \end{pmatrix}$$

mit n Spalten und $n-k$ Zeilen ist eine Paritätsprüfmatrix von C.

Umgekehrt definieren auch zwei Polynome

$$G(X) = g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}, \quad H(X) = h_0 + h_1 X + \cdots + h_k X^k$$

mit $G(X) \cdot H(X) = X^n - 1$ über $\mathbb{F}_q$ einen zyklischen $[n,k]_q$–Code (mit Erzeuger– und Paritätsprüfmatrix wie oben beschrieben).

zyklische Codes

Definition

Das Polynom $G(X)$ aus dem Satz heißt **Erzeugerpolynom** des Codes C, das Polynom $H(X)$ heißt **Paritätsprüfpolynom** von C.

Beispiel

Für den zyklischen $[4,2]_2$–Code
$C = \{(0,0,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\}$ gilt:

$$G(X) = X^2 + 1, \quad H(X) = X^2 + 1$$

Beachten Sie dabei, dass über Körpern der Charakteristik 2 gilt

$$X^n - 1 = X^n + 1$$

zyklische Codes

Beispiel

Das Polynom $G(X) = X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$ definiert einen zyklischen $[6, 2]_2$–Code.

$$(X^6 + 1) \div (X^4 + X^3 + X + 1) = X^2 + X + 1$$

Beispiel

Das Polynom $G(X) = X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ definiert keinen zyklischen $[6, 3]_2$–Code.

$$(X^6 + 1) \div (X^3 + X^2 + X + 1) = X^3 + X^2 \quad \text{Rest } X^2 + 1$$

$G(X)$ ist also kein Teiler von $X^6 + 1$.

zyklische Codes

Beispiel

Das Polynom $G(X) = X^3 + 3X^2 + 6X + 4 \in \mathbb{F}_7[X]$ ist Erzeugerpolynom eines zyklischen $[6, 3]_7$–Codes.
Das Paritätsprüfpolynom hierzu ist

$$H(X) = X^3 + 4X^2 + 3X + 5$$

zyklische Codes

Übung

Überprüfen Sie, ob $G(X) = X^2 + 4 \in \mathbb{F}_5[X]$ Erzeugerpolynom eines zyklischen $[4, 2]_5$–Codes C ist.

zyklische Codes

Übung

Wie viele zyklische $[5, 3]_2$–Codes gibt es?

zyklische Codes

Regel

Für ein $n \in \mathbb{N}$ und ein $1 \leq k \leq n-1$ sind die folgenden Aussagen äquivalent:

- *Es gibt einen zyklischen $[n,k]_q$–Code.*
- *Das Polynom $X^n - 1$ hat einen Teiler vom Grad k in $\mathbb{F}_q[X]$.*
- *Es gibt einen zyklischen $[n,n-k]_q$–Code.*
- *Das Polynom $X^n - 1$ hat einen Teiler vom Grad $n-k$ in $\mathbb{F}_q[X]$.*

zyklische Codes

Beispiel

Es gibt genau zwei zyklische $[6,2]_2$–Codes. Einer mit

$$G_1(X) = X^4 + X^2 + 1, \qquad H_1(X) == X^2 + 1$$

und einer mit

$$G_2(X) = X^4 + X^3 + X + 1 \qquad H_2(X) = X^2 + X + 1$$

Weitere zyklische $[6,2]_2$–Codes gibt es nicht.

zyklische Codes

Jedes Polynom $G(X) \in \mathbb{F}_q[X]$ vom Grad $n-k$ mit

$$G(X)|(X^n-1)$$

definiert einen zyklischen $[n,k]_q$–Code mit zugehörigem Paritätsprüfpolynom

$$H(X) = (X^n-1) \div G(X)$$

Unterschiedliche zyklische $[n,k]_q$–Codes führen zu unterschiedlichen Erzeugerpolynomen $G(X)$ (und unterschiedlichen Paritätsprüfpolynomen $H(X)$).
Unterschiedliche Teiler $G(X)|(X^n-1)$ können jedoch denselben zyklischen $[n,k]_q$–Code definieren.

zyklische Codes

Regel

Sind $G_1(X)$ und $G_2(X)$ zwei Polynome in $\mathbb{F}_q[X]$ vom Grad $n-k$, die X^n-1 teilen, und gilt

$$G_1(X) = r \cdot G_2(X)$$

für ein $r \in \mathbb{F}_q \setminus \{0\}$, so definieren $G_1(X)$ und $G_2(X)$ denselben zyklischen $[n,k]_q$–Code.

Beispiel

Das Polynom $G_1(X) = X^2 + 5X + 6 \in \mathbb{F}_7[X]$ definiert einen zyklischen $[6,4]_7$–Code mit Paritätsprüfpolynom

$$H_1(X) = X^4 + 2X^3 + 5X^2 + 5X + 1$$

Derselbe Code wird definiert durch $G_2(X) = 5X^2 + 4X + 2$ $(= 5 \cdot G_1(X))$ mit Paritätsprüfpolynom $H_2(X) = 3X^4 + 6X^3 + X^2 + X + 3$ $(= 3 \cdot H_1(X))$.

zyklische Codes

Regel

Sind $G_1(X)$ und $G_2(X)$ zwei Polynome in $\mathbb{F}_q[X]$ vom Grad $n-k$, die X^n-1 teilen, und gilt **nicht**

$$G_1(X) = r \cdot G_2(X)$$

für ein $r \in \mathbb{F}_q \setminus \{0\}$, so definieren $G_1(X)$ und $G_2(X)$ unterschiedliche zyklische $[n,k]_q$–Codes.

Bemerkung

Das Erzeugerpolynom $G(X)$ eines zyklischen $[n,k]_q$–Codes kann immer normiert gewählt werden, dh. so, dass

$$G(X) = X^{n-k} + g_{n-k-1} \cdot X^{n-k-1} + \cdots + g_1 \cdot X + g_0$$

Dadurch ist das Erzeugerpolynom eindeutig bestimmt. In diesem Fall ist auch das Paritätsprüfpolynome eindeutig.

zyklische Codes

Übung

Überprüfen Sie, ob

$$G_1(X) = 3X^3 + X^2 + X + 5, \quad G_2(X) = 5X^3 + 4X^2 + 3X + 2 \in \mathbb{F}_7[X]$$

zyklische $[6, 3]_7$–Codes definieren. Falls das der Fall ist, überprüfen Sie, ob die beiden Codes übereinstimmen.

zyklische Codes

Zyklische Codes können nicht nur über Körpern $\mathbb{F}_p$ betrachtet werden sondern über beliebigen endlichen Körpern.

Beispiel

Wir betrachten den Körper $\mathbb{F}_4$, gegeben durch die Relation $\alpha^2 = \alpha + 1$.
Das Polynom $G(X) = X^3 + X^2 + \alpha \cdot X + \alpha$ definiert einen zyklischen $[6, 3]_4$–Code:
Es ist

$$(X^6 + 1) \div G(X) = X^3 + X^2 + (\alpha + 1) \cdot X + \alpha + 1 \qquad \text{Rest } 0$$

Damit ist also

$$H(X) = X^3 + X^2 + (\alpha + 1) \cdot X + \alpha + 1$$

das Paritätsprüfpolynom für diesen Code.

zyklische Codes

Übung

Wir betrachten wieder $\mathbb{F}_4$, gegeben durch $\alpha^2 = \alpha + 1$.
Zeigen Sie, dass $G(X) = X^4 + \alpha \cdot X^2 + \alpha + 1$ das Erzeugerpolynom eines zyklischen $[6, 2]_4$–Codes ist und bestimmen Sie das zugehörige Paritätsprüfpolynom.

zyklische Codes

Wir betrachten den Körper $\mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha + 1$. Dann können auch über $\mathbb{F}_8$ zyklische Codes betrachtet werden.

Beispiel

Das Polynom $G(X) = X^3 + (\alpha^2 + \alpha + 1) \cdot X^2 + (\alpha^2 + 1) \cdot X + \alpha + 1$ ist das Erzeugerpolynom eines zyklischen $[7, 4]_8$–Codes.

$$(X^7+1) \div G(X) = X^4+(\alpha^2+\alpha+1)\cdot X^3+(\alpha^2+\alpha)\cdot X^2+X+\alpha^2+\alpha \quad \text{Rest } 0$$

Also ist

$$H(X) = X^4 + (\alpha^2 + \alpha + 1) \cdot X^3 + (\alpha^2 + \alpha) \cdot X^2 + X + \alpha^2 + \alpha$$

das zugehörige Paritätsprüfpolynom.

zyklische Codes

Übung

Wir betrachten den Körper $\mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha + 1$. Zeigen Sie, dass das Polynom

$$G(X) = X^3 + (\alpha^2 + \alpha + 1) \cdot X^2 + \alpha^2 \cdot X + \alpha^2 + \alpha + 1$$

einen zyklischen $[7, 4]_8$–Code definiert und bestimmen Sie das zugehörige Paritätsprüfpolynom.

Codierung bei zyklischen Codes

Nachrichten können bei zyklischen Codes direkt mithilfe des Erzeugerpolynoms codiert werden.
Wir betrachtenen einen zyklischen $[n, k]_q$–Code C mit Erzeugerpolynom $G(X)$ und eine Nachricht $m = (m_0, m_1, \ldots, m_{k-1}) \in \mathbb{F}_q^k$.

- Bilde $m(X) = m_0 + m_1 \cdot X + \cdots + m_{k-1} \cdot X^{k-1}$.
- Berechne $c(X) = m(X) \cdot G(X)$.
- Schreibe $c(X) = c_0 + c_1 X + \cdots + c_{n-1} \cdot X^{n-1}$.
- Setze $c = (c_0, c_1, \ldots, c_{n-1})$.

Codierung bei zyklischen Codes

Beispiel

Wir betrachten den zyklischen $[6,4]_2$–Code mit Erzeugerpolynom $G(X) = X^2 + X + 1$ und die Nachricht $m = (1,0,1,1)$.

- $m(X) = 1 + X^2 + X^3$.
- $$\begin{aligned} c(X) &= (1 + X^2 + X^2) \cdot (1 + X + X^2) \\ &= 1 + X + X^5 \end{aligned}$$
- $c = (1,1,0,0,0,1)$.

Codierung bei zyklischen Codes

Übung

Wir betrachten den zyklischen $[6,3]_7$–Code mit Erzeugerpolynom $G(X) = X^3 + 6X^2 + 4X + 6$.
Codieren Sie die Nachricht $m = (3,5,2)$

Codierung bei zyklischen Codes

Beispiel

Wir betrachten den Körper $\mathbb{F}_8$ mit der Relation $\alpha^3 = \alpha + 1$ und den zyklischen $[7,4]_8$–Code mit Erzeugerpolynom

$$G(X) = X^3 + (\alpha^2 + 1) \cdot X^2 + \alpha \cdot X + \alpha^2 + 1$$

und die Nachricht $m = (\alpha^2, \alpha^2 + 1, \alpha, \alpha + 1)$.

- $m(X) = \alpha^2 + (\alpha^2 + 1) \cdot X + \alpha \cdot X^2 + (\alpha + 1) \cdot X^3$.
- $$\begin{aligned} c(X) &= G(X) \cdot m(X) \\ &= \alpha + \alpha^2 \cdot X + \alpha \cdot X^2 + (\alpha + 1) \cdot X^3 + \alpha \cdot X^4 \\ &\quad + (\alpha^2 + \alpha) \cdot X^5 + (\alpha + 1) \cdot X^6 \end{aligned}$$
- $c = (\alpha, \alpha^2, \alpha, \alpha + 1, \alpha, \alpha^2 + \alpha, \alpha + 1)$.

Codierung bei zyklischen Codes

Übung

Wir betrachten den zyklischen $[7,3]_8$–Code mit Erzeugerpolynom

$$G(X) = X^4 + (\alpha^2+1)\cdot X^3 + (\alpha^2+1)\cdot X^2 + (\alpha+1)\cdot X + \alpha$$

Codieren Sie die Nachricht $m = (\alpha, \alpha+1, \alpha^2)$