Codierungstheorie

Reinhold Hübl

Vorlesung 7 - WS 2022/23

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

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.

Übung

Wir betrachten den Körper $\mathbb{F}_4$, 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 $m = (\alpha, \alpha+1, \alpha^2)$

Decodierung bei zyklischen Codes

Auch bei der Decodierung zyklischer Codes können Polynome eingesetzt werden.

Idee:

- Ist c ein korrektes Codewort, so ist $c(X) = G(X) \cdot m(X)$ mit dem Nachrichtenpolynom $m(x)$.
- Ist also c korrekt, so ist

$$m(X) = c(X) \div G(X)$$

- Ist c korrekt, so kann m aus $c(X)$ durch Polynomdivision gewonnen werden.

Decodierung bei zyklischen Codes

Beispiel

Wir betrachten den zyklischen $[6,4]_2$–Code mit Erzeugerpolynom

$$G(X) = X^2 + X + 1$$

und die empfangene Nachricht $a = (1,1,1,1,1,1)$.
Dann ist $a(X) = 1 + X + X^2 + X^3 + X^4 + X^5$ und

$$a(X) \div G(X) = X^3 + 1 \quad \text{Rest } 0$$

Also ist a ein Codewort, das zur Nachricht

$$m = (1,0,0,1)$$

gehört.

Decodierung bei zyklischen Codes

Beispiel

Wir betrachten den zyklischen $[6,4]_2$–Code mit Erzeugerpolynom

$$G(X) = X^2 + X + 1$$

und die empfangene Nachricht $b = (1,1,0,0,1,1)$.
Dann ist $b(X) = 1 + X + X^4 + X^5$ und

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

Also ist b kein Codewort.

Decodierung bei zyklischen Codes

Übung

Wir betrachten den zyklischen $[6,3]_7$–Code mit Erzeugerpolynom $G(X) = X^3 + 6X^2 + 4X + 6$.
Überprüfen Sie, ob es sich bei den Nachrichten $a = (6,2,3,6,2,4)$ und $b = (4,2,5,2,6,4)$ um korrekt übermittelte Codewörter handelt.

Decodierung bei zyklischen Codes

Beispiel

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

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

und die empfangene Nachricht

$$a = (\alpha + 1, 1, \alpha, \alpha^2, \alpha^2 + \alpha, \alpha^2 + 1, \alpha^2 + \alpha + 1)$$

Dann ist

$$\begin{aligned} a(X) &= \alpha + 1 + X + \alpha \cdot X^2 + \alpha^2 \cdot X^3 + (\alpha^2 + \alpha) \cdot X^4 \\ &\quad + (\alpha^2 + 1) \cdot X^5 + (\alpha^2 + \alpha + 1) \cdot X^6 \end{aligned}$$

Decodierung bei zyklischen Codes

Beispiel

Es gilt

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

Also ist a ein Codewort, das zur Nachricht

$$m = (\alpha^2, \alpha + 1, \alpha^2 + \alpha + 1)$$

gehört.

Decodierung bei zyklischen Codes

Beispiel

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

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

und die empfangene Nachricht

$$a = (\alpha, 1, \alpha, 1, \alpha + 1, \alpha, \alpha)$$

Dann ist

$$\begin{aligned} a(X) &= \alpha + X + \alpha \cdot X^2 + X^3 + (\alpha + 1) \cdot X^4 \\ &\quad + \alpha \cdot X^5 + \alpha \cdot X^6 \end{aligned}$$

Decodierung bei zyklischen Codes

Beispiel

In diesem Fall gilt

$$\begin{aligned} a(X) \div G(X) &= \alpha^2 + \alpha + (\alpha + 1) \cdot X + \alpha \cdot X^2 \\ &\quad \text{Rest } (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1 \end{aligned}$$

Also ist a kein Codewort.

Decodierung bei zyklischen Codes

Übung

Wir betrachten den Körper $\mathbb{F}_8$ mit der Relation $\alpha^3 + 1$ 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 empfangenen Nachrichten

$$a = (1, 0, \alpha, \alpha^2 + 1, \alpha, 0, \alpha)$$

und

$$b = (\alpha^2, 0, 1, \alpha, 0, 1, \alpha^2 + 1)$$

Überprüfen Sie, ob a und b korrekt übertragene Codewörter sind und bestimmen Sie gegebenenfalls die zugehörige Nachrichten.

Decodierung bei zyklischen Codes

Wir betrachten allgemein einen zyklischen $[n, k]_q$–Code C mit Erzeugerpolynom $G(X)$.
Ist $a \in \mathbb{F}_q^n$ kein Codewort, so ergibt die Polynomdivision

$$a(X) = n(X) \cdot G(X) + s(X)$$

mit einem Polynom $s(X) \neq 0$ mit $\deg(s(X)) < n - k = \deg(G(X))$.

Definition

Das Polynom $s(X)$ heißt **Syndrom** oder **Syndrompolynom** von a.

Mithilfe des Syndroms ist für viele zyklische Polynome eine Fehlerkorrektur über Syndromtabellen möglich.

Decodierung bei zyklischen Codes

Beispiel

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

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

In diesem Fall ist bekannt, dass C die Zuverlässigkeit $d = 5$ hat, also bis zu zwei Fehler korrigieren kann.
Wir betrachten wieder $a = (\alpha, 1, \alpha, 1, \alpha + 1, \alpha, \alpha)$.
Dann ist

$$\begin{aligned} a(X) \div G(X) &= \alpha^2 + \alpha + (\alpha + 1) \cdot X + \alpha \cdot X^2 \\ &\quad \text{Rest } (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1 \end{aligned}$$

Decodierung bei zyklischen Codes

Beispiel

Also ist a kein Codewort, wie wir ja schon gesehen haben. Aus dem Syndrom $s(X) = (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1$, das nur an zwei Stellen Einträge hat, lesen wir ab, dass

$$\begin{aligned} c &= a - (\alpha^2 + 1, \alpha^2 + \alpha, 0, 0, 0, 0, 0) \\ &= (\alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha, 1, \alpha + 1, \alpha, \alpha) \end{aligned}$$

ein Codewort ist, dass sich an (höchstens) zwei Stellen von dem übertragenen Wort unterscheidet.
Das liegt in diesem Fall daran, dass das Syndrom nur so viele Terme hat wie durch die Fehlerkorrektur gegeben.
Die dazu passende Nachricht ist $m = (\alpha^2 + \alpha, \alpha + 1, \alpha)$.

Decodierung bei zyklischen Codes

Beispiel

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

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

Wir betrachten diesmal $a = (\alpha^2, \alpha^2, 1, \alpha + 1, \alpha^2 + 1, \alpha + 1, \alpha + 1)$.
Dann ist

$$\begin{aligned} a(X) \div G(X) \quad = \quad & \alpha^2 + \alpha + 1 + (\alpha^2 + \alpha + 1) \cdot X + (\alpha + 1) \cdot X^2 \\ & \text{Rest } (\alpha^2 + \alpha) \cdot X^3 + (\alpha + 1) \cdot X^2 + (\alpha + 1) \cdot X + 1 \end{aligned}$$

Decodierung bei zyklischen Codes

Beispiel

Also ist auch hier a kein Codewort, aber aus dem Syndrom $s(X) = (\alpha^2 + \alpha) \cdot X^3 + (\alpha + 1) \cdot X^2 + (\alpha + 1) \cdot X + 1$ kann diesmal die Fehlerkorrektur nicht direkt abgelesen werden, da in dem Syndrom vier Terme auftreten, also mehr als die Fehlerkorrektur angibt.
Aber es gilt, dass

$$\begin{aligned} c &= a - (0, 0, 0, 0, 0, 0, \alpha^2 + \alpha + 1) \\ &= (\alpha^2, \alpha^2, 1, \alpha + 1, \alpha^2 + 1, \alpha + 1, \alpha^2) \end{aligned}$$

ein Codewort ist, dass sich an höchstens zwei Stellen (hier sogar nur an einer) von dem übertragenen Wort unterscheidet. Das liegt daran, dass

$$(\alpha^2 + \alpha + 1) \cdot X^6 = \Big((\alpha^2 + \alpha + 1) \cdot X^2 + (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1\Big) \cdot G(X) + s(X)$$