Codierungstheorie

Reinhold Hübl

Herbst 2021 / 4. Vorlesung

endliche Körper

Übung

Wir betrachten den Körper $\mathbb{F}_8$ mit der Relation $\alpha^3 = \alpha + 1$. Berechnen Sie

- $(\alpha + 1) \cdot \alpha^2$.
- $(\alpha^2 + 1) \cdot (\alpha^2 + \alpha)$.

endliche Körper

Es kann mehrere Relationen geben, die den Körper $\mathbb{F}_q$ beschreiben, aber nicht jede Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

ist eine definierende Relation.

Beispiel

Die Relation $\alpha^3 = \alpha^2 + \alpha + 1$ beschreibt den Körper $\mathbb{F}_8$ nicht.

endliche Körper

Definition

Ist $\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$ eine definierende Relation von $\mathbb{F}_q$, so heißt

$$F(X) = X^l - r_{l-1} \cdot X^{l-1} - r_{l-2} \cdot X^{l-2} - \cdots - r_1 \cdot X - r_0 \in \mathbb{F}_p[X]$$

Minimalpolynom von $\mathbb{F}_q$.

Satz

Ein Polynom $F(X) = X^l + r_{l-1} \cdot X^{l-1} + \cdots + r_1 \cdot X + r_0 \in \mathbb{F}_p[X]$ ist genau dann ein Minimalpolyonom von $\mathbb{F}_q$ (mit $q = p^l$) wenn es **keine** *Polynome $h(X)$ und $g(X)$ vom Grad mindestens 1 gibt, sodass*

$$F(X) = g(X) \cdot h(X)$$

endliche Körper

Für Körpererweiterungen kleinen Grades kann das leicht überprüft werden.

Bemerkung

Ist $l = 2$, so ist $F(X) = X^2 + r_1 \cdot X + r_0$ genau dann ein Minimalpolynom vn $\mathbb{F}_q$, wenn $F(X)$ keine Nullstelle in $\mathbb{F}_p$ hat.
Ist $l = 3$, so ist eine $F(X) \in \mathbb{F}_p[X]$ genau dann ein Minimalpolynom von $\mathbb{F}_q$, wenn $F(X)$ keine Nullstelle in $\mathbb{F}_p$ hat.

Beispiel

Das Polynom $F(X) = X^2 + X + 1$ ist ein Minimalpolynom von $\mathbb{F}_4$, denn

$$F(0) = 1 \neq 0, \quad F(1) = 1 \neq 0$$

also definiert $\alpha^2 = -\alpha - 1 = \alpha + 1$ den Körper $\mathbb{F}_4$.
Das Polynom $F(X) = X^2 + 1$ ist kein Minimalpolynom von $\mathbb{F}_4$, denn

$$F(1) = 0.$$

endliche Körper

Übung

Überprüfen Sie, welche der Polynome $F(X) = X^3 + X^2 + 1$ und $G(X) = X^3 + X^2 + X + 1$ Minimalpolynome von $\mathbb{F}_8$ sind.

endliche Körper

Bemerkung

Ist $l = 4$ oder $l = 5$, so ist ein Polynom $F(X) \in \mathbb{F}_p[X]$ vom Grad l genau dann ein Minimalpolynom von $\mathbb{F}_q$ ($q = p^l$), wenn $F(X)$ keine Nullstelle in $\mathbb{F}_p$ hat und wenn es kein Polynom $g(X) \in \mathbb{F}_p[X]$ vom Grad 2 gibt, dass selbst keine Nullstelle hat und das $F(X)$ teilt.

Beispiel

Das Polynom $F(X) = X^4 + X^3 + X + 1$ ist kein Minimalpolynom von $\mathbb{F}_{16}$, denn $F(1) = 0$.

Das Polynom $F(X) = X^4 + X + 1$ ist ein Minimalpolynom von $\mathbb{F}_{16}$, denn

$$F(0) = 1 \neq 0, \quad F(1) = 1 \neq 0$$

und

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

endliche Körper

Übung

Überprüfen Sie, ob das Polynom $F(X) = X^5 + X^4 + 1$ ein Minimalpolynom von $\mathbb{F}_{32}$ ist.

endliche Körper

Für die Division in endlichen Körpern gibt es keine definierende Formel.

Das Inverse $\frac{1}{a}$ eines $a \in \mathbb{F}_q \setminus \{0\}$ kann durch Ausprobieren und über die Multplikationstafel bestimmt werden.

Beispiel

In $\mathbb{F}_8$, definiert durch $\alpha^3 = \alpha + 1$ gilt

$(\alpha+1)\cdot\alpha = \alpha^2+\alpha$, $(\alpha+1)\cdot(\alpha+1) = \alpha^2+1, \cdots, (\alpha+1)\cdot(\alpha^2+\alpha) = 1$

also gilt

$$\frac{1}{\alpha+1} = \alpha^2+\alpha$$

endliche Körper

Wie im Fall von $\mathbb{F}_p$ kann auch für $\mathbb{F}_q$ das Inverse eines Elements $a \neq 0$ mithilfe des euklidischen Algorithmus bestimmt werden.
Dazu nehmen wir an, dass $\mathbb{F}_q$ durch eine Relation $\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$ und damit das Minimalpolynon

$$F(X) = X^l - r_{l-1} \cdot X^{l-1} - r_{l-2} \cdot X^{l-2} - \cdots - r_1 \cdot X - r_0 \in \mathbb{F}_p[X]$$

definiert wird.
Ist $a = a_n \cdot \alpha^n + \cdots + a_1 \cdot \alpha + a_0$ (mit $n < l$) ein Element von $\mathbb{F}_q$, so schreibe

$$a(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0$$

Da $F(X)$ keine echten Teiler hat, sind $a(X)$ und $F(X)$ teilerfremd,

$$\mathrm{ggT}(a(X), F(X)) = 1$$

endliche Körper

Der euklidische Algorithmus ermittel $\frac{1}{a}$ nun wie folgt:

- Bestimme $\operatorname{ggT}(a(X), F(X)) = 1$ mithilfe des euklidischen Algorithmus (mit Polynomdivision mit Rest statt ganzzahliger Division mit Rest).
- Durch Rückwärtsrechnen finde eine Darstellung

$$1 = g(X) \cdot a(X) + h(X) \cdot F(X)$$

  mit Polynomen $g(X), h(X) \in \mathbb{F}_p[X]$.
- Es ist

$$\frac{1}{a} = g(\alpha)$$

endliche Körper

Beispiel

Im Körper $\mathbb{F}_8$ gegeben durch $\alpha^3 = \alpha + 1$ (also mit $F(X) = X^3 + X + 1$ betrachte $a = \alpha + 1$, also $a(X) = X + 1$.

- $(X^3 + X + 1) = (X^2 + X) \cdot (X + 1) + 1.$
- $X + 1 = (X + 1) \cdot 1 + 0 \quad \longrightarrow$ STOPP.

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

also

$$\frac{1}{\alpha + 1} = \alpha^2 + \alpha$$

endliche Körper

Satz

Der Körper $\mathbb{F}_q$ kann beschrieben werden durch ein α mit definierender Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

so dass

$$\mathbb{F}_q \setminus \{0\} = \{\alpha, \alpha^2, \ldots, , \alpha^{q-2}, \alpha^{q-1} = 1\}$$

Ist dann $a \in \mathbb{F}_q \setminus \{0\}$, so gibt es ein $s \in \{1, \ldots, q-1\}$ mit

$$a = \alpha^s$$

und damit gilt

$$\frac{1}{a} = \alpha^{q-1-s}$$

denn

$$a \cdot \alpha^{q-1-s} = \alpha^s \cdot \alpha^{q-1-s} = \alpha^{q-1} = 1$$

endliche Körper

Beispiel

Ist $\mathbb{F}_8$ gegeben durch die Relation $\alpha^3 = \alpha + 1$, so gilt

$$\begin{array}{rcl@{\qquad}rcl}
\alpha & = & \alpha & \alpha^5 & = & \alpha^2+\alpha+1 \\
\alpha^2 & = & \alpha^2 & \alpha^6 & = & \alpha^2+1 \\
\alpha^3 & = & \alpha+1 & \alpha^7 & = & 1 \\
\alpha^4 & = & \alpha^2+\alpha & \alpha^8 & = & \alpha
\end{array}$$

Damit gilt

$$\frac{1}{\alpha^2+1} = \frac{1}{\alpha^6} = \alpha^1 = \alpha$$

oder

$$\frac{\alpha^2+\alpha}{\alpha^2+\alpha+1} = \frac{\alpha^4}{\alpha^5} = \frac{1}{\alpha} = \alpha^6 = \alpha^2+1$$

endliche Körper

Übung

Betrachten Sie $\mathbb{F}_8$ gegeben durch die Relation $\alpha^3 = \alpha^2 + 1$. Prüfen Sie ob,

$$\mathbb{F}_8 \setminus \{0\} = \{\alpha, \alpha^2, \ldots, \alpha^7\}$$

und bestimmen Sie

$$\frac{1}{\alpha^2 + 1}$$

endliche Körper

Der wichtigste Körper für die digitale Datenverarbeitung ist der Körper $\mathbb{F}_{256}$ mit $2^8 = 256$ Elementen. Er wird definiert durch die Relation

$$\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$$

Hierfür gilt

$$\mathbb{F}_{256} \setminus \{0\} = \{\alpha, \alpha^2, \dots, \alpha^{254}, \alpha^{255} = 1\}$$

Ein Element $x \in \mathbb{F}_{256}$ wird als 8–Tupel

$$x = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) \in \mathbb{F}_2^8$$

gespeichert; das entspricht dem Element

$$x = b_7\alpha^7 + b_6\alpha^6 + \cdots + b_1\alpha + b_0$$

Damit lassen sich Bytes multplizieren und dividieren.

endliche Körper

Beispiel

Für die beiden Elemente $x, y \in \mathbb{F}_{256}$ mit

$$x = (1,0,0,1,0,0,0,1), \quad y = (0,0,1,0,1,1,0,0)$$

gilt

$$\begin{aligned} x \cdot y &= (1,0,0,1,0,0,0,1) \cdot (0,0,1,0,1,1,0,0) \\ &= (\alpha^7 + \alpha^4 + 1) \cdot (\alpha^5 + \alpha^3 + \alpha^2) \\ &= \alpha^6 + \alpha^4 + \alpha^2 \\ &= (0,1,0,1,0,1,0,0) \end{aligned}$$

endliche Körper

Über beliebigen endlichen Körpern können lineare Gleichungssysteme betrachtet und nach dem Eliminationsverfahren gelöst werden.

Beispiel

Über $\mathbb{F}_8$, gegeben durch $\alpha^3 = \alpha + 1$ betrachte das lineare Gleichungssystem

$$\begin{array}{rcrcrcl} \alpha \cdot x_1 & + & \alpha^2 \cdot x_2 & + & (\alpha^2+1) \cdot x_3 & = & 0 \\ \alpha^2 \cdot x_1 & + & (\alpha^2+\alpha) \cdot x_2 & + & (\alpha+1) \cdot x_3 & = & 0 \end{array}$$

$$v = r \cdot (\alpha^2, \alpha^2, 1)$$

Die Lösung $v_1 = (\alpha^2, \alpha^2, 1)$ ist die Grundlösung des Gleichungssystems.

lineare Codes

Betrachte einen endlichen Körper $k = \mathbb{F}_q$ und eine Teilmenge $U \subseteq k^n$.

Definition

U heißt **Untervektorraum** von k^n, wenn gilt

- $U \neq \emptyset$.
- Ist $u \in U$ und $r \in k$, so ist $r \cdot u \in U$.
- Sind $u, v \in U$, so ist auch $u + v \in U$.

lineare Codes

Definition

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

Bemerkung

Ein linearer $[n, k]_q$–Code ist ein $[n, k]_q$–Code im Sinne der ursprünglichen Definition, also ein Code der Länge n und der logarithmischen Kardinalität k.

Beispiel

$C = \{(0, 0, 0, 0,), (1, 0, 1, 0), (0, 1, 0, 1), (1, 1, 1, 1)\}$ ist ein linearer $[4, 2]_2$–Code.

lineare Codes

Definition

Ist $C \subseteq \mathbb{F}_q^n$ ein lineare Code und $c = (c_1, \ldots, c_n) \in C$, so heißt

$$w(c) = d(c, 0) = |\{i \in \{1, \ldots, n\} | \, c_i \neq 0\}|$$

das **Gewicht** von c.

Beispiel

Für $C = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}$ ist

$$\begin{array}{rcl} w((0,0,0)) & = & 0 \\ w((1,0,1)) & = & 2 \\ w((0,1,1)) & = & 2 \\ w((1,1,0)) & = & 2 \end{array}$$

lineare Codes

Satz

Ist $C \subseteq \mathbb{F}_q^n$ ein linearer $[n,k]_q$–Code, so gilt

$$d(C) = min\{w(c) \mid c \in C \setminus \{0\}\}$$

Folgerung

Ist C ein linearer $[n,1]_q$–Code und bildet der Vektor v eine Basis von C, so gilt

$$d(C) = w(v)$$

Beispiel

Der lineare $[n,1]_q$–Code

$$C = \{(r, r, \ldots, r, r) \mid r \in \mathbb{F}_q\}$$

hat Minimalabstand $d(C) = n$.

lineare Codes

Übung

Berechnen Sie $d(C)$ für den linearen $[6,2]_2$–Code $C \subseteq \mathbb{F}_2^6$ mit Basis

$$v_1 = (1,1,1,1,1,1), \quad v_2 = (1,1,0,1,1,0)$$

Erzeugermatrix

Jeder $[n,k]_q$–Code $C \subseteq \mathbb{F}_q^n$ besitzt eine Basis $g_1, \dots, g_k$, bestehend aus k Vektoren.
Ist

$$g_i = (g_{i,1}, g_{i,2}, \dots, g_{i,n}) \qquad (i = 1, \dots, k)$$

so heißt

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \ddots & \vdots & \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

Erzeugermatrix von C.

lineare Codes

Beispiel

Der $[5,2]_2$–Code

$$C = \{(0,0,0,0,0),(1,0,1,0,1),(0,1,0,1,1),(1,1,1,1,0)\}$$

hat Erzeugermatrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

aber auch

$$G' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Die Erzeugermatrix eines Codes ist also nicht eindeutig bestimmt.

Erzeugermatrix

Übung

Bestimmen Sie eine Erzeugermatrix G des linearen $[3,2]_7$–Codes

$$C = \{(x,y,z) \mid x + 2y + 4z = 0\}$$

Paritätsprüfmatrix

Ein Ergebnis der linearen Algebra besagt, dass jeder Untervektorraum von $\mathbb{F}_q^n$ als Lösungsmenge eines homogenen Gleichungssystems geschrieben werden kann.

Satz

Ist $C \subseteq \mathbb{F}_q^n$ ein $[n, k]_q$–Code, so gibt es eine $(n-k) \times n$–Matrix H vom Rang $n-k$ mit

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

Die Matrix H heißt **Paritätsprüfmatrix** von C.

Paritätsprüfmatrix

Beispiel

Der $[5,2]_2$–Code

$$C = \{(0,0,0,0,0),(1,0,1,0,1),(0,1,0,1,1),(1,1,1,1,0)\}$$

hat Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

aber auch

$$H' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Die Paritätsprüfmatrix eines Codes ist also nicht eindeutig bestimmt.

Paritätsprüfmatrix

Beispiel

Der erste systematische fehlerkorrigierende Code (aus der zweiten Vorlesung) war ein lineare $[7,5]_{11}$–Code mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Paritätsprüfmatrix

Übung

Bestimmen Sie eine Paritätsprüfmatrix H des linearen $[3,1]_7$–Codes

$$C = \{(r, 3r, 6r) \mid r \in \mathbb{F}_7\}$$