§4 Zyklische Codes

In diesem Unterkapitel wird es sich als günstig erweisen Vektoren $x \in \mathbb{F}_q^n$ als $x = (x_0, x_1, \dots, x_{n-1})$ zu schreiben.

Def.: Ein linearer Code $C \subseteq \mathbb{F}_q^n$ heisst **zyklisch**, falls für alle $x = (x_0, \dots, x_{n-1}) \in C$ gilt:

$(x_{n-1}, x_0, \dots, x_{n-2}) \in C$.

D.h. $\sigma = (0\ 1 \dots n-1) \in \mathrm{Aut}(C)$.

Um zyklische Codes algebraisch zu beschreiben werden wir die folgendere Identifikation vornehmen:

$$\begin{array}{ccc} \mathbb{F}_q^n & \cong & \mathbb{F}_q[x]/(x^n-1) \qquad (\text{als } \mathbb{F}_q\text{-VR}) \\ \downarrow & & \downarrow \\ (a_0, \dots, a_{n-1}) & \longmapsto & a_0 + a_1 x + \dots + a_{n-1} x^{n-1}. \end{array}$$

Multiplikation mit x entspricht einem Rechtsschift:

$$x(a_0 + a_1 x + \dots + a_{n-1} x^{n-1}) = a_0 x + a_1 x^2 + \dots + a_{n-2} x^{n-1} + a_{n-1}$$

Satz Ein linearer Code $C \subseteq \mathbb{F}_q^n$ ist zyklisch genau dann wenn C ein Ideal in $\mathbb{F}_q[x]/(x^n-1)$ ist.

[C Ideal: C UVR von $\mathbb{F}_q[x]/(x^n-1)$ und $fC \subseteq C$ für alle $f \in \mathbb{F}_q[x]/(x^n-1)$].

Bew.: "$\Rightarrow$": Weil C linear ist, ist C UVR von $\mathbb{F}_q[x]/(x^n-1)$.

Weil C zyklisch ist, gilt $xc \in C$ für alle $c \in C$.

Genauso $x^i c \in C$ für alle $i \in \mathbb{N}$, $c \in C$. Genauso, wegen der Linearität, ist $fc \in C$ für alle $f \in \mathbb{F}_q[x]/(x^n-1)$ und $c \in C$.

"$\Leftarrow$": Falls C ein Ideal ist, gilt für jeden $c \in C$:

$xc \in C$ und $xc = (c_{n-1}, c_0, \dots, c_{n-2})$. ☒

Etwas Algebra Generalvoraussetzung ab jetzt $(n,q) = 1$, d.h. n, q sind teilerfremd.

- $\mathbb{F}_q[x]/(x^n-1)$ ist ein Hauptidealring, d.h. jedes Ideal I wird von einem Element erzeugt:

$$I = (g) \text{ für ein } g \in \mathbb{F}_q[x]/(x^n-1).$$

Satz Sei $C \subseteq \mathbb{F}_q[x]/(x^n-1)$ ein Ideal mit $C \neq \{0\}$. (D.h. C ist ein zyklischer Code der Länge n). Dann gilt:

(a) Es gibt ein eindeutiges, normiertes Polynom g in C, was minimalen Grad r besitzt.

(b) $C = (g)$, g heißt das Erzeugerpolynom von C.

(c) $g \mid x^n - 1$.

(d) Jedes Codewort $c \in C$ kann man eindeutig schreiben als $c = fg$, wobei $\deg f < n-r$. D.h. $\dim C = n-r$.

(e) Falls $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$. Dann ist

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & & 0 \\ & g_0 & g_1 & \cdots & g_{r-1} & g_r & \\ 0 & & \ddots & & & & \ddots \\ & & & g_0 & & & g_r \end{bmatrix} \in \mathbb{F}_q^{(n-r)\times n}$$

eine Erzeugermatrix von C; G ist eine zyklische Matrix.

Bew.: (a) Ang. $\exists f, g \in C$, $\deg f = \deg g = r$. Dann ist $f - g \in C$. Da $\deg f - g < r$ und r minimal ist, folgt $f - g = 0$.

(b) Sei $c \in C$. Division mit Rest liefert

$c = qg + p$ mit $\deg p < r$. Nun ist

$p = c - qg \in C$. Also $p = 0$, weil r minimal.

Also $c \in (g)$.

(c). Wieder Division mit Rest

$x^n - 1 = qg + p$, $\deg p < r$.

Wieder $p = -qg \in \mathbb{F}_q[x]/(x^n-1)$, also $p \in C$, also $p = 0$.

(d) - (e): Folgt aus (b), weil

$$g, xg, x^2g, \ldots, x^{n-r-1}g$$

eine Basis von C ist. ☒

(e) Zeigt, warum zyklische Codes in der Praxis wichtig sind: Man kann z.B. sehr effizient codieren; Laufzeit $O(n \log n)$ mit Hilfe der schnellen Fouriertransformation (FFT)

Def.: Sei C ein zyklischer Code mit Erzeugerpolynom g. Dann heißt $h = (x^n - 1)/g$ das **Kontrollpolynom** von C.

Falls $c = fg \in C$, dann ist $ch = fgh = 0$ in $\mathbb{F}_q[x]/(x^n - 1)$.

Sei $k = n - \deg g = n - r$, und

$$h = h_0 + h_1 x + \cdots + h_{k-1} x^{k-1} + h_k x^k$$

Dann ist

$$H = \begin{bmatrix} 0 & & h_k & \cdots & h_2 & h_1 & h_0 \\ & h_k & h_{k-1} & \cdots & h_1 & h_0 & \\ \ddots & & & & & & \\ h_k & \cdots & & h_0 & & 0 & \end{bmatrix} \in \mathbb{F}_q^{r \times n}$$

eine Kontrollmatrix von C,

Satz Der zu C duale Code $C^\perp$ ist zyklisch und besitzt Erzeugerpolynom

$$g^\perp(x) = x^k h(x^{-1}).$$

Bew.: → Aufgabe.