Zyklische Codes

Sei $C \leq \mathbb{F}_q^n$ mit $n \geq 1$ ein zyklischer Code, d.h. mit $(c_0, ..., c_{n-1})^t \in C$ soll auch $(c_{n-1}, c_0, ..., c_{n-2})^t \in C$ sein. Wir fassen $\mathbb{F}_q^n$ und damit auch C als $\mathbb{F}_q[X]$-Moduln auf mittels

$$X : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n, \quad a = (a_0, \ldots, a_{n-1})^t \longmapsto X \cdot a = X(a) = (a_{n-1}, a_0, \ldots, a_{n-2})^t,$$

und setzen diese Vorschrift auf $\mathbb{F}_q[X]$ fort. Damit operieren die Elemente von $\mathbb{F}_q[X]$ als Endomorphismen des $\mathbb{F}_q[X]$-Moduls $\mathbb{F}_q^n$ mittels $f(X) \cdot a = f(a)$ für alle $f \in \mathbb{F}_q[X]$ und $a \in \mathbb{F}_q^n$. Der $\mathbb{F}_q[X]$-Modul $\mathbb{F}_q^n$ ist zyklisch, da $\mathbb{F}_q^n = \mathbb{F}_q[X]e_1$ gilt mit $X^{l-1}(e_1) = e_l \in \mathbb{F}_q[X]e_1$ $(l = 1, \ldots, n)$, wenn $e_i \in \mathbb{F}_q^n$ den i-ten Einheistvektor bezeichnet. Im Folgendem sei D_{n-1} eine $(n-1) \times (n-1)$-Matrix über $\mathbb{F}_q$ mit Einsen auf der Diagonalen und sonst Nullen. Für das charakteristische Polynom von $f_X(t) \in \mathbb{F}_q[t]$ von X auf $\mathbb{F}_q^n$ erhalten wir damit

$$\text{CharPol } f_X(t) = \det \quad tE_n - \left(\begin{array}{c|c} 0 \cdots 0 & 1 \\ \hline & 0 \\ D_{n-1} & \vdots \\ & 0 \end{array}\right) = t^n - 1$$

und da wir bereits wissen, dass $\mathbb{F}_q^n = \mathbb{F}_q[X]e_1$ gilt, ist $f_X(t)$ sogar das Minimalpolynom von X. Mit dem Hauptsatz für endlich erzeugte Moduln über Hauptidealringen (Satz. 4.30 im AlgebraII-Skript) erhalten wir die Isomorphie

$$\Psi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(X^n - 1), \quad (a_0, \ldots, a_{n-1})^t \longmapsto \sum_{i=0}^{n-1} a_i X^i$$

Wir setzen $R_n := \mathbb{F}_q[X]/(X^n - 1)$ und $\tilde{C} := \Psi(C)$. Da C ein linearer zyklischer Code ist und somit $\mathbb{F}_q[X]C \subset C$ gilt, folgt insbesondere $R_n\tilde{C} \leq \tilde{C}$. Der zu C isomorphe lineare Code $\tilde{C}$ ist also ein Ideal von R_n. Jedes Ideal von R_n ist ein Hauptideal. Betrachten wir nämlich die kanonische Restklassenabbildung $\pi : \mathbb{F}_q[X] \longrightarrow R_n$ und ein Ideal $I \subseteq R_n$, so ist $\pi^{-1}(I) = g\mathbb{F}_q[X]$ mit $g \in \mathbb{F}_q[X]$ geeignet. Aus $(X^n - 1) \subseteq \pi^{-1}(0) \subseteq \pi^{-1}(I)$ folgt dann $g|(X^n - 1)$. Da dann $I = \pi(g\mathbb{F}_q[X]) = \pi(g)R_n$ ist, könnnen wir uns auf solche g mit $\deg\ g < n$ beschränken. Ein Ideal gR_n von R_n mit $\deg g < n$ ist also genau dann nicht-trivial, wenn g ein nicht-trivialer Teiler von $X^n - 1$ ist. Ist $C \leq R_n$ ein zyklischer Code, so nennen wir g mit $gR_n = C$ das Erzeugerpolynom von

C und $h(X) := (X^n - 1)/g(X)$ das Kontrollpolynom von C. Ist $C \subseteq R_n$ ein zyklischer $[n,k]_q$-Code, so können wir auch $C = g(X)R_n =$

$$\langle g(X), Xg(X), \ldots, X^{k-1}g(X)\rangle = \{f \cdot g \mid \deg f < k \text{ und } f, g \in \mathbb{F}_q[X]\}$$

schreiben. Es gilt weiter

Lemma 1. *Ist $C = gR_n$ zyklischer Code mit Erzeugerpolynom $g \in \mathbb{F}_q[X]$. Dann lässt sich C schreiben als*

$$C = \{f \in \mathbb{F}_q[X] \mid f \cdot h \equiv 0 \mod X^n - 1\},$$

wobei h das Kontrollpolynom von C ist.

Beweis. Bezeichne $g \in \mathbb{F}_q[X]$ das Erzeugerpolynom von C. Aus $gh \equiv 0 \mod X^n - 1$ folgt zuerst $ch \equiv 0 \mod X^n - 1$ für ein $c \in C$, da c von der Form $c = gr$ mit $r \in R_n$ geeignet ist. Das zeigt $\subseteq$. Andererseits folgt aus $fh \equiv 0 \mod X^n - 1$, dass gh das Polynom fh teilt, was aber wiederum $g|f$ bedeutet. Dies zeigt die umgekehrte Inklusion und damit folgt die Behauptung. □

Insbesondere sehen wir, dass $\deg g = n - k$ und $\deg h = k$ ist und damit $\sharp C = q^{\deg h}$ und $\dim C = \deg h$ gilt. Letztere Darstellung motiviert auch die Bezeichnung $C = R_n[h]$, d.h. wir sehen die Elemente von C als h-Torsionselemente von R_n an.

Lemma 2. *Sei $C = gR_n$ zyklischer $[n,k]_q$-Code mit Erzeugerpolynom $g \in \mathbb{F}_q[X]$. Dann ist auch $C^\perp$ zyklisch. Ist*

$$h(X) = h_0 + h_1X + \ldots + h_kX^k = g_{C^\perp} \quad (h_k = 1, h_0 \neq 0)$$

das Kontrollpolynom von C, so gilt $h^*(X) := h_0^{-1}(h_k + h_{k-1}X + \ldots + h_0X^k) = g_{C^\perp}$.

Beweis. Aus $h^* = h_0^{-1}X^kh(1/X)$ und $gh = X^n - 1$ erhalten wir als erstes $g(1/X)h(1/X) = \frac{1}{X^n} - 1$ und beide Seiten mit X^n multipliziert ergibt $X^{n-k}g(1/X)X^kh(1/X) = 1 - X^n = -(X^n - 1)$, also $h^*|(X^n - 1)$, da $X^{n-k}g(1/X)$ und $X^kh(1/X)$ beidemale Polynome in $\mathbb{F}_q[X]$ sind. Ausserdem ist $\deg h^* = n - k$ und $h^*R_n =: C^*$ definiert in R_n einen zyklischen Code der Dimension $n - k$ mit Erzeugermatrix (s. Skript von Hauck, S. 87, Folgerung 8.17)

$$G_{C^\star} = h_0^{-1} \begin{pmatrix} h_k & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & \ddots & & \ddots & & \vdots \\ \vdots & & \ddots & & \ddots & \vdots \\ 0 & \cdots & \cdots & h_k & \cdots & h_0 \end{pmatrix} = H_C = G_{C^\perp},$$

woraus dann $C^* = C^\perp$ folgt. □

Für die Syndromabbildung s eines zyklischen Codes $C = gR_n$ erhalten wir

$$s : \mathbb{F}_q[X]/(X^n - 1) \longrightarrow \mathbb{F}_q[X]/(g), \quad f \longmapsto f \mod g.$$

Damit ist also $f \in C = gR_n$ genau dann, wenn $s(f) \equiv 0$ ist, .d.h. $f \equiv 0 \mod g$ oder $f = rg$ mit $r \in \mathbb{F}_q[X]$ geeignet.