Aus der Algebra: Die Teiler von $x^n - 1$.

Generalvoraussetzung: $(n, q) = 1$

Dann: $x^n - 1$ zerfällt in t (unter verschiedene) irreduzible Polynome $x^n - 1 = f_1 \cdots f_t$.

[D.h. es gibt 2^t zyklische Code der Länge n über $\mathbb{F}_q$].

Bew.: Die Ableitung f' von $f(x) = x^n - 1$ ist $f'(x) = n x^{n-1}$. Da $(n, q) = 1$ ist, ist $n \in \mathbb{F}_q - \{0\}$. Also haben f und f' in keinem Erweiterungskörper von $\mathbb{F}_q$ eine gemeinsame NST. Also hat f keine mehrfachen Nullstellen. ☒

Bsp: Zerlegung von $x^n - 1 \in \mathbb{F}_2[x]$ in irreduzible Faktoren:

$$x^3 - 1 = (x-1)(x^2 + x + 1)$$
$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$
$$x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$$
$$x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

Sei K der Zerfällungskörper von $X^n - 1$ über $\mathbb{F}_q$.

In K bilden die Nullstellen von $X^n - 1$ eine zyklische Gruppe der Ordnung n; diese heißt die n-ten Einheitswurzeln über $\mathbb{F}_q$.

Was ist K? K hat Charakteristik p $(q = p^r)$.
Also ist $K = \mathbb{F}_{p^{r'}}$ für geeignetes r'. Da $\mathbb{F}_q \subseteq K$ muss gelten $q \mid p^{r'}$, d.h. $K = \mathbb{F}_{q^m}$ für geeignetes m.
Dabei ist $m = m(n) = \min\{m : n \mid q^m - 1\}$, weil $\mathbb{F}_{q^m}^*$ zyklisch der Ordnung $q^m - 1$ ist und die n-ten Einheitswurzeln enthalten muss.

Also $K = \mathbb{F}_{q^m}$ mit $m = \min\{m : n \mid q^m - 1\}$.

Die Galoisgruppe der Körpererweiterung $\mathbb{F}_{q^m} \mid \mathbb{F}_q$ wird erzeugt von dem (Frobenius-) Automorphismus $\alpha \longmapsto \alpha^q$. Die Galoisgruppe operiert transitiv auf den Nullstellen von jedem f_i der irreduziblen Zerlegung

$$X^n - 1 = f_1 \cdots f_t.$$

Sei $\alpha \in \mathbb{F}_{q^m}$ eine primitive n-te Einheitswurzel ($\operatorname{ord} \alpha = n$). Sei α^{m_i} eine Nullstelle von f_i, dann ist

$$f_i(x) = (x - \alpha^{m_i})(x - \alpha^{m_i q})(x - \alpha^{m_i q^2}) \cdots,$$

wobei $m_i q^k \bmod n$ gerechnet wird.

Also: Um Information (Anzahl, Grad) über f_i zu gewinnen, muss man $\mathbb{Z}/n\mathbb{Z}$ in Äquivalenzklassen bzgl. Multiplikation mit q einteilen.

$$\mathbb{Z}/n\mathbb{Z} = \mathcal{Z}_1 \dot\cup \ldots \dot\cup \mathcal{Z}_t.$$

Bsp.: $x^n - 1 \in \mathbb{F}_2[x]$

$$\mathbb{Z}/3\mathbb{Z} = \{0\} \dot\cup \{1, 2\}$$

$$\mathbb{Z}/5\mathbb{Z} = \{0\} \dot\cup \{1, 2, 4, 3\}$$

$$\mathbb{Z}/7\mathbb{Z} = \{0\} \dot\cup \{1, 2, 4\} \dot\cup \{3, 6, 5\}$$

$$\mathbb{Z}/9\mathbb{Z} = \{0\} \dot\cup \{1, 2, 4, 8, 7, 5\} \dot\cup \{3, 6\}$$

Also: Jeder zyklische Code $C \subseteq \mathbb{F}_q^n$ ist von der Form

$$C = \{ f \in R_{q,n} : f(\alpha_1) = \ldots = f(\alpha_t) = 0 \},$$

wobei $\alpha_1, \ldots, \alpha_t$ n-te Einheitswurzeln über $\mathbb{F}_q$ sind.

Das Erzeugerpolynom von C ist

$$g = kgV(p_{\alpha_1}, \ldots, p_{\alpha_t}),$$

wobei $p_{\alpha_i} \in \mathbb{F}_q[x]$ das Minimalpolynom von α_i ist.

BCH - Codes

Def.: Für $\delta, l \in \mathbb{N}$ mit $2 \leq \delta \leq n$ und $1 \leq l \leq n+1-\delta$ definiere

$$BCH(q,n,\delta,l) = \{ f \in R_{q,n} : f(\alpha^l) = f(\alpha^{l+1}) = \ldots = f(\alpha^{l+\delta-2}) = 0 \},$$

Wobei α eine primitive n-te Einheitswurzel über $\mathbb{F}_q$ ist.

BCH $\hat{=}$ Bose - Chaudhuri - Hocquenghem (1960)