Satz $d(BCH(q,n,\delta,\ell)) \geq \delta$.

Bew.: Betrachte die Matrix

$$H = \begin{bmatrix} 1 & \alpha^{\ell} & \alpha^{2\ell} & \cdots & \alpha^{(n-1)\ell} \\ 1 & \alpha^{\ell+1} & \alpha^{2(\ell+1)} & \cdots & \alpha^{(n-1)(\ell+1)} \\ \vdots & \vdots & \vdots & & \\ 1 & \alpha^{\ell+\delta-2} & \alpha^{2(\ell+\delta-2)} & \cdots & \alpha^{(n-1)(\ell+\delta-2)} \end{bmatrix}.$$

Dann gilt $c \in BCH(q,n,\delta,\ell) \iff H c^T = 0$, weil

$c = (c_0, \ldots, c_{n-1}) \in BCH(q,n,\delta,\ell)$

$$\iff c_0 + c_1 \alpha^{\ell} + c_2 (\alpha^{\ell})^2 + \cdots + c_{n-1} (\alpha^{\ell})^{n-1} = 0$$

$$\vdots$$

$$c_0 + c_1 \alpha^{\ell+\delta-2} + c_2 (\alpha^{\ell+\delta-2})^2 + \cdots + c_{n-1} (\alpha^{\ell+\delta-2})^{n-1} = 0.$$

Ang. $\exists\, c \in BCH(q,n,\delta,\ell)$ mit $w(c) = d \leq \delta - 1$.
Wähle quadratische Teilmatrix von H mit Spalten $j_1, j_2, \ldots, j_d \in \{0, \ldots, d\}$, $c_{j_i} \neq 0$ und den ersten d Zeilen:

$$H' = \begin{bmatrix} \alpha^{j_1 \ell} & \alpha^{j_2 \ell} & \cdots & \alpha^{j_d \ell} \\ \alpha^{j_1(\ell+1)} & & & \\ \vdots & & \ddots & \vdots \\ \alpha^{j_1(\ell+d-1)} & & & \end{bmatrix}.$$

Dann ist $H'(c')^T = 0$, $c' = (c_{j_1}, \dots, c_{j_d})$, aber die Determinante von H' ist eine Vandermondsche-Determinante, die $\neq 0$ ist, weil die α^i's paarweise verschieden sind, und weil α eine primitive n-te Einheitswurzel ist. ☒

Satz $\dim BCH(q, n, \delta, \ell) \geq n - m(\delta - 1)$

Bew.: → Aufgabe 5.4.

Effiziente Decodierung von BCH-Codes (mögl. Seminarthema)

z.B. mittels Berlekamp-Massey-Algorithmen;
Ideen ähnlich wie beim Weld-Berlekamp-Algorithmus für RS-Codes.

Beziehung zwischen BCH und RS:

Satz $RS_{q,q-1,q-1-\delta+1} = BCH(q, q-1, \delta, 1)$

Bew.: Sei α eine primitive $(q-1)$-te Einheitswurzel über $\mathbb{F}_q$. D.h. α ist primitives Element der multiplikativen Gruppe $\mathbb{F}_q^*$. Dann hat der BCH-Code $BCH(q, q-1, \delta, 1)$ das Erzeugerpolynom

$$g(x) = (x-\alpha^1)(x-\alpha^2)\cdots(x-\alpha^{\delta-1}).$$

Es zerfällt über $\mathbb{F}_q$ in Linearfaktoren. Die Minimaldistanz des BCH-Codes ist $\geq \delta$ und seine Dimension ist $= q-1-\deg g = q-1-\delta+1$. Also ist $BCH(q, q-1, \delta, 1)$ ein MDS-Code.

Deswegen genügt es z.z., dass

$$RS_{q, q-1, q-1-\delta+1} \subseteq BCH(q, q-1, \delta, 1)$$

gilt.

Zur Erinnerung

$$RS_{q, q-1, q-1-\delta+1} = \{(f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{q-2})) : f \in \mathbb{F}_q[x], \deg f \leq q-1-\delta\},$$

Wobei wir eine Basis des RS-Codes haben, wenn wir $f = 1, x, x^2, \dots, x^{q-1-\delta}$ wählen.

D.h. es ist

$$\sum_{j=0}^{q-2} f(\alpha^j)(\alpha^k)^j = 0 \quad \text{für} \quad f = x^i, \; i = 0, \dots, q-1-\delta$$
$$k = 1, \dots, \delta - 1$$

Zu zeigen:

Das stimmt tatsächlich (geometrische Reihe):

$$\sum_{j=0}^{q-2} (\alpha^j)^i (\alpha^k)^j = \sum_{j=0}^{q-2} (\alpha^{i+k})^j = \frac{(\alpha^{i+k})^{q-1} - 1}{\alpha^{i+k} - 1} = 0,$$

weil $i + k \neq 0, q-1$.

$\boxtimes$