A new q-polynomial approach to cyclic and quasi-cyclic codes

Funda Özdemir

İstinye University

funda.ozdemir@istinye.edu.tr

Abstract. A q-polynomial approach to cyclic codes was introduced by Ding and Ling [D-L]. In this work, we present an alternative q-polynomial approach to cyclic and quasi-cyclic codes.

Let $\mathbb{F}_q$ be the finite field with q elements, and $\mathbb{F}_{q^n}$ be the extension field of degree $n > 1$ over $\mathbb{F}_q$. Let $\mathcal{B} = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ be a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for a normal element $\alpha \in \mathbb{F}_{q^n}^*$. The following map is an $\mathbb{F}_q$-linear isomorphism.

$$\begin{aligned} \phi_{\mathcal{B}} : \mathbb{F}_{q^n} &\longrightarrow \mathbb{F}_q^n \\ v_0\alpha + v_1\alpha^q + \cdots + v_{n-1}\alpha^{q^{n-1}} &\mapsto (v_0, v_1, \ldots, v_{n-1}). \end{aligned}$$

We call $V \subseteq \mathbb{F}_{q^n}$ q-invariant if $V = V^q$, i.e. V is mapped onto itself by the Frobenius automorphism. Taking q-th power of $v \in \mathbb{F}_{q^n}$ corresponds to a cyclic shift of $\vec{v} \in \phi_{\mathcal{B}}(V)$. Hence, V is a q-invariant $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$ if and only if $\phi_{\mathcal{B}}(V)$ is a linear cyclic code of length n over $\mathbb{F}_q$.

The following theorem shows our correspondence between q-polynomials and cyclic codes. This is different from Theorem 4.10 in [D-L].

Theorem 0.1.

(i) Let $L(x) \in \mathbb{F}_q[x]$ be a q-polynomial of degree q^k which splits in $\mathbb{F}_{q^n}$ and let $V \subseteq \mathbb{F}_{q^n}$ be the set of roots of $L(x)$. Then $\phi_{\mathcal{B}}(V)$ is a q-ary $[n, k]$-cyclic code.

(ii) For every q-ary $[n, k]$-cyclic code, there exists a q-polynomial of degree q^k over $\mathbb{F}_q$ splitting in $\mathbb{F}_{q^n}$.

Using the relation in the Theorem, we can construct optimal cyclic codes. We also obtain a characterization of linear complementary dual (LCD) cyclic codes in terms of q-polynomials. Let us recall that an LCD code is a linear code which intersects its dual trivially.

Theorem 0.2. *Let $A(x) \in \mathbb{F}_q[x]$ be the q-polynomial, splitting in $\mathbb{F}_{q^n}$, of a q-ary $[n, k]$-cyclic code C and $B(x) \in \mathbb{F}_q[x]$ be the q-polynomial, splitting in $\mathbb{F}_{q^n}$, of $C^\perp$. Assume that $(n, q) = 1$. Then C is LCD if and only if $A(x) \circ B(x) = x^{q^n} - x$.*

We also generalize our results to quasi-cyclic codes.

[D-L] C. Ding and S. Ling, “A q-polynomial approach to cyclic codes”, *Finite Fields Appl.*, vol. 20, 1-14, 2013.

Joint work with Cem Güneri (Sabancı University) and Ferruh Özbudak (Middle East Technical University).