(14.8.92 Preprint of paper submitted to *Discrete Mathematics*)

# The Necessary and Sufficient Condition for a Cyclic Code to Have a Complementary Dual

Xiang Yang and James L. Massey
Signal and Information Processing Laboratory
Swiss Federal Institute of Technology
CH-8092 Zurich, Switzerland

*Abstract:* A linear code with a complementary dual (an LCD code) is a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = \{ \mathbf{0} \}$. It is shown that the necessary and sufficient condition for a cyclic code C of length n to be an LCD code is that the generator polynomial g(x) of C be self-reciprocal and all the monic irreducible factors of g(x) have the same multiplicity in g(x) as in $x^n - 1$.

## 1. Introduction

A *linear code with a complementary dual* (an *LCD code*) was defined in [3] to be a linear code C whose dual code $C^{\perp}$ satisfies $C \cap C^{\perp} = \{ \mathbf{0} \}$. It was shown in [3] that asymptotically good LCD codes exist and that LCD codes have certain other attractive properties. In the following, we give the necessary and sufficient condition for a cyclic code to be an LCD code.

## 2. Results

Let C be a q-ary cyclic code of block length $n = \tilde{n} \cdot p^e$ where p is the characteristic of GF(q), $e \geq 0$, and $\gcd(p, \tilde{n}) = 1$, where here and hereafter "gcd" denotes "greatest common divisor." All monic irreducible factors of

$x^n - 1$ in GF(q)[x] have multiplicity exactly $p^e$, as follows immediately from the facts that

$$x^n - 1 = x^{\tilde{n}\, p^e} - 1 = (x^{\tilde{n}} - 1)^{p^e}$$

and that the polynomial $x^{\tilde{n}} - 1$ in GF(q)[x] has no repeated irreducible factors since $\gcd(p, \tilde{n}) = 1$. Suppose that f(x) is a monic (i.e., leading coefficient 1) polynomial of degree d with $f(0) = c \neq 0$. Then by the *monic reciprocal polynomial* of f(x) we mean the polynomial $\tilde{f}(x) = c^{-1} x^d f(x^{-1})$.

*Lemma:* If g(x) is a generator polynomial for an (n, k) cyclic code C of block length $n = \tilde{n} \cdot p^e$ where p is the characteristic of GF(q), $e \geq 0$ and $\gcd(p, \tilde{n}) = 1$, then C is an LCD code if and only if $\gcd(g(x), \tilde{h}(x)) = 1$, where $\tilde{h}(x)$ is the monic reciprocal polynomial of $h(x) = (x^n - 1)/g(x)$.

*Proof:* The dual code $C^\perp$ of C is the cyclic code whose generator polynomial is $\tilde{h}(x)$, cf. [2, pp. 72-73]. The polynomial $g^*(x) = \mathrm{lcm}(g(x), \tilde{h}(x))$ is of course the generator polynomial of the cyclic code $C \cap C^\perp$, where "lcm" here and hereafter denotes "least common multiple." We first note that $C \cap C^\perp = \{ \mathbf{0} \}$ if and only if $g^*(x)$ has degree n. But $x^n - 1$ is divisible by g(x) and by $\tilde{h}(x)$, $\deg[g(x)] = n - k$, and $\deg[\tilde{h}(x)] = k$. Therefore, $\deg[g^*(x)] = n$ if and only if $\gcd(g(x), \tilde{h}(x)) = 1$. ❑

*Theorem:* If g(x) is the generator polynomial of a q-ary (n, k) cyclic code C of block length n, then C is an LCD code if and only if g(x) is self -reciprocal (i.e., $\tilde{g}(x) = g(x)$) and all the monic irreducible factors of g(x) have the same multiplicity in g(x) and in $x^n - 1$.

*Proof:* Let p be the characteristic of GF(q) and let $n = \tilde{n} \cdot p^e$ where

$\gcd(p, \tilde{n}) = 1$.

Suppose now that C is an LCD code, i.e., (by the Lemma) that $\gcd(g(x), \tilde{h}(x)) = 1$. Then, because

$$x^n - 1 = g(x) \cdot h(x) = \tilde{g}(x) \cdot \tilde{h}(x), \tag{1}$$

it follows that g(x) must divide $\tilde{g}(x)$ and hence that $g(x) = \tilde{g}(x)$, i.e., g(x) is self-reciprocal. Thus $\gcd(g(x), \tilde{h}(x)) = 1$ implies that $\gcd(\tilde{g}(x), \tilde{h}(x)) = 1$ and hence that $\gcd(g(x), h(x)) = 1$. Because

$$x^n - 1 = g(x) \cdot h(x) = (x^{\tilde{n}} - 1)^{p^e}, \tag{2}$$

it follows that all the irreducible factors of g(x) must have multiplicity $p^e$.

Conversely, suppose first that g(x) is not self-reciprocal, i.e., that g(x) does not divide $\tilde{g}(x)$. It follows then from (1) that $\gcd(g(x), \tilde{h}(x)) \neq 1$ and hence, by the Lemma, that C is not an LCD code. Suppose finally that g(x) is self-reciprocal, as hence so also is $h(x) = (x^n - 1)/g(x)$, but that some monic irreducible factor of g(x) has multiplicity less than $p^e$. Because of (2), it follows that $1 \neq \gcd(g(x), h(x)) = \gcd(g(x), \tilde{h}(x))$, and hence by the Lemma that C is not an LCD code. ❏

A *reversible code* is a code such that reversing the order of the components of a codeword gives always again a codeword. It was shown in [4] that a cyclic code is reversible if and only if its generator polynomial is self-reciprocal, which immediately establishes the following corollary that covers the cyclic codes of greatest interest, namely those whose generator polynomials have no repeated factors, cf. [1].

*Corollary:* A q-ary cyclic code, whose length n is relatively prime to the characteristic p of GF(q), is an LCD code if and only if it is a reversible code.

## Acknowledgement

The first author gratefully acknowledges helpful discussions with Dr. Thomas Mittelholzer.

## References

[1] G. Castagnoli, J. L. Massey, P. A. Schoeller and N. Seemann,"On Repeated-Root Cyclic Codes," *IEEE Transactions on Information Theory* (1991) 337-342.

[2] J. H. van Lint, *Introduction to Coding Theory* (Springer, New York, 1982).

[3] J. L. Massey, "Linear codes with complementary duals," to appear in *Discrete Mathematics* (1992).

[4] J. L. Massey, "Reversible codes," *Information & Control* (1964) 369-380.