A note on isodual constacyclic codes

Chen, Bocong; Dinh, Hai Q.


2014

http://hdl.handle.net/10220/20362

© 2014 Elsevier. This is the author created version of a work that has been peer reviewed and accepted for publication by Finite Fields and Their Applications, Elsevier. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [http://dx.doi.org/10.1016/j.ffa.2014.04.006].
A note on isodual constacyclic codes

Bocong Chen¹, Hai Q. Dinh²

1. Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore
2. Department of Mathematical Sciences, Kent State University, 4314 Mahoning Avenue, Warren, OH 44483, USA

Abstract

This short note gives a counterexample of Theorem 20 in the paper [T. Blackford, Isodual constacyclic codes, Finite Fields Appl., 24(2013), 29-44]. The counterexample shows that [2, Theorem 20] is incorrect. Furthermore, we provide corrections to the above result.

Keywords: Constacyclic code, duadic code, multiplier, finite field.

2010 Mathematics Subject Classification: 94B15; 11T71

1 Introduction

Let \( F_q \) be a finite field of order \( q \) and \( \lambda \) a nonzero element of \( F_q \). A linear code \( C \) of length \( n \) over \( F_q \) is called \( \lambda \)-constacyclic if \((a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C \) for every \((a_0, a_1, \ldots, a_{n-1}) \in C \). It is well known that a \( \lambda \)-constacyclic code of length \( n \) over \( F_q \) can be identified as an ideal in the quotient ring \( R_{n,\lambda} = F_q[X]/(X^n - \lambda) \) (e.g., see [7, Proposition 2.1]). The class of constacyclic codes has received a lot of attention (e.g., see [1]-[7]).

Hereafter, we always assume that \( n \) is a positive integer relatively prime to the characteristic of \( F_q \) and \( r \) is a positive divisor of \( q - 1 \). Recently, Blackford in [2] studied constacyclic codes of length \( n \) over \( F_q \) that are isometric to their dual via a multiplier. We refer to [2] for background and further references. For completeness, we reproduce the definition of Type I duadic splitting of \( n \) over \( F_q \) respect to \( r \) as follows.

**Definition 1.1.** (see [2]) Let \( \theta_{r,n} = \{ j \mid 0 \leq j < rn, j \equiv 1 \pmod{r} \} \). Let \( s \) be a positive integer relatively prime to \( rn \). We say \( s \) is a multiplier for a Type I duadic splitting of \( n \) over \( F_q \) with respect to \( r \) if there is a subset \( T \) of \( \theta_{r,n} \) such that

1. \( T \) is a union of \( q \)-cyclotomic cosets modulo \( rn \).
2. \( T \bigcup sT = \theta_{r,n} \) is a partition of \( \theta_{r,n} \).

*E-Mail addresses: bocong.chen@yahoo.com (B. Chen), hdinh@kent.edu (H. Q. Dinh).
Blackford obtained the following result.

**Theorem 1.2.** (see [2, Theorem 15]) If \( r = 2^a r' \) and \( n = 2^b n' \) with \( a \geq 1, b \geq 1 \) and \( r', n' \) odd, and if \( \gcd(s, rn) = 1 \) with \( s \equiv 1(\text{mod } r) \), then \( s \) is a multiplier for a Type I duadic splitting of \( n \) over \( \mathbb{F}_q \) with respect to \( r \) if and only if \( s \not\equiv \langle q \rangle \) modulo \( 2^a + b \).

In [2, Theorem 20(1)], Blackford states that: Assume \( q \equiv -1(\text{mod } 4) \), with \( q = -1 + 2^v \) for some \( c \geq 2 \) and some odd \( v \). Let \( r = 2^r \) and \( n = 2^b n' \), with \( r', n' \) odd and \( b \geq 2 \). Then \( 1 + 2^r n' \) is a multiplier for a Type I duadic splitting of \( n \) over \( \mathbb{F}_q \) with respect to \( r \) if and only if \( 1 + r' n' \not\equiv 2c - 1(\text{mod } 2^c) \).

Unfortunately, this result is not always true. For example, take \( b = 2, c = 4, r' = 3, n' = 1 \) and \( v = 5 \). Clearly, \( 1 + r' n' = 4 \) and \( 4 \not\equiv 8(\text{mod } 16) \). It follows from [2, Theorem 20(1)] that \( 1 + 2^r n' = 7 \) is a multiplier for a Type I duadic splitting of \( 4 \) over \( \mathbb{F}_{79} \) with respect to 6. But from Theorem 1.2 and the fact \( 1 + 2^r n' = 7 \equiv 79 \equiv 7(\text{mod } 8) \), we know that 7 is not a multiplier for a Type I duadic splitting of \( 4 \) over \( \mathbb{F}_{79} \) with respect to 6. This example shows that [2, Theorem 20(1)] is incorrect in general.

Using Theorem 1.2, we correct [2, Theorem 20(1)] as follows.

**Theorem 1.3.** Assume \( q \equiv 3(\text{mod } 4) \), with \( q = -1 + 2^v \) for some \( c \geq 2 \) and some odd \( v \). Let \( r = 2^r \) and \( n = 2^b n' \), with \( r', n' \) odd and \( b \geq 2 \). Then \( 1 + 2^r n' \) is a multiplier for a Type I duadic splitting of \( n \) over \( \mathbb{F}_q \) with respect to \( r \) if and only if one of the following conditions holds:

(i) \( c > b \) and \( 1 + r' n' \not\equiv 0(\text{mod } 2^c) \).

(ii) \( c \leq b \) and \( 1 + r' n' \not\equiv 2c - 1(\text{mod } 2^c) \).

2 Proof of Theorem 1.3

We need the results [2, Lemma 6]-[2, Theorem 9]. Let \( v \) be an odd integer and \( c \geq 2 \) a positive integer. We claim that \( \langle -1 + 2^v \rangle_{2^{c+b}} = \langle -1 + 2^0 \rangle_{2^{c+b}} \), where \( \langle -1 + 2^v \rangle_{2^{c+b}} \) and \( \langle -1 + 2^0 \rangle_{2^{c+b}} \) denote the cyclic subgroups of \( \mathbb{Z}_{2^{c+b}} \) generated by \( \langle -1 + 2^v \rangle_{2^{c+b}} \) and \( \langle -1 + 2^0 \rangle_{2^{c+b}} \), respectively. There is nothing to prove if \( c > b \). Thus, we assume that \( c \leq b \). By [2, Theorem 9(2)], we know that \( \langle -1 + 2^v \rangle_{2^{c+b}} = \langle -1 + 2^0 \rangle_{2^{c+b}} \), and hence an integer \( j_0 \) can be found such that \( 1 - 2^c = (1 - 2^v)j_0 \). From [2, Lemma 8], \( j_0 \) must be odd since \( 1 - 2^v \) and \( 1 - 2^c \) have the same order in \( \mathbb{Z}_{2^{c+b}} \). Then \( 1 + 2^c = (1 - 1 - 2^c) = (1 - 2^v)j_0 = (1 - 2^v)j_0 = (1 + 2^v)j_0 \). This implies that \( \langle -1 + 2^c \rangle_{2^{c+b}} \subseteq \langle -1 + 2^v \rangle_{2^{c+b}} \), which forces \( \langle -1 + 2^c \rangle_{2^{c+b}} = \langle -1 + 2^v \rangle_{2^{c+b}} \).

**Proof.** Observe that \( \gcd(1 + 2^r n', rn) = 1 \) and \( 1 + 2^r n' \equiv 1(\text{mod } r) \). We see that \( 1 + 2^r n' \in \langle q \rangle_{2^{c+b}} \) if and only if an integer \( j_0 \) can be found such that \( 1 + 2^r n' \equiv q^{j_0}(\text{mod } 2^{b+1}) \). In this case, we claim that \( j_0 \) must be odd. This is simply because \( q^2 \equiv 1(\text{mod } 4) \) but \( 1 + 2^r n' \equiv 1(\text{mod } 4) \).
Assume that (i) holds. It follows from $q = -1 + 2^c v$ and $c > b$ that $\langle q \rangle_{2^{1+b}} = (-1)_{2^{1+b}}$. Suppose otherwise that $1 + 2r' n'$ is not a multiplier for any Type I duadic splitting of $n$ over $F_q$ with respect to $r$. We then know from Theorem 1.2 that $1 + 2r' n' \in (-1)_{2^{1+b}}$, which implies that $1 + 2r' n' \equiv (-1)^{j_0} \pmod{2^{b+1}}$ for some odd integer $j_0$. This gives $1 + r' n' \equiv 0 \pmod{2^b}$, a contradiction.

Assume that (ii) holds. If $1 + 2r' n' \in \langle q \rangle_{2^{1+b}}$, then $1 + 2r' n' \equiv (-1 + 2^c v)^{j_0} \pmod{2^{b+1}}$ for some odd integer $j_0$. It follows from [2, Lemma 8] that an odd integer $v'$ can be found such that $1 + 2r' n' \equiv -1 + 2^c v' \pmod{2^{b+1}}$. We then have $1 + r' n' \equiv 2^{c-1} v' \pmod{2^b}$. Now by the assumption $b \geq c$, we obtain $1 + r' n' \equiv 2^{c-1} \pmod{2^b}$. This is a contradiction.

Conversely, suppose that $1 + 2r' n'$ is a multiplier for a Type I duadic splitting of $n$ over $F_q$ with respect to $r$, i.e., $1 + 2r' n' \not\in \langle q \rangle_{2^{1+b}}$ by Theorem 1.2.

If $c > b$, then $\langle q \rangle_{2^{1+b}} = \langle -1 + 2^c v \rangle_{2^{1+b}} = (-1)_{2^{1+b}}$. We need to prove that $1 + r' n' \not\equiv 0 \pmod{2^b}$. Otherwise, $2 + 2r' n' \equiv 0 \pmod{2^{b+1}}$. This leads to $1 + 2r' n' \equiv -1 \pmod{2^{b+1}}$, a contradiction.

If $c \leq b$, we assert that $1 + r' n' \not\equiv 2^{c-1} \pmod{2^b}$. Otherwise, there exists some integer $k$ such that $1 + r' n' - 2^{c-1} = k 2^b$, which gives $1 + 2r' n' = -1 + 2^c (2k + 1)$. Letting $u = 2k + 1$, we then have $1 + 2r' n' \equiv -1 + 2^c u \pmod{2^{b+1}}$. On the other hand, we know that $\langle -1 + 2^c u \rangle_{2^{b+1}} = \langle -1 + 2^c \rangle_{2^{b+1}} = \langle -1 + 2^c v \rangle_{2^{b+1}} = \langle q \rangle_{2^{b+1}}$. It follows that $-1 + 2^c u \in \langle -1 + 2^c u \rangle_{2^{b+1}} = \langle q \rangle_{2^{b+1}}$. This gives $1 + 2r' n' \in \langle q \rangle_{2^{b+1}}$, a contradiction. \hfill \Box

References