J. Appl. Math. & Informatics Vol. **31**(2013), No. 1 - 2, pp. 179 - 188
Website: http://www.kcam.biz

THE NUMBER OF SOLUTIONS TO THE EQUATION $(x+1)^d = x^d + 1$

JI-MI YIM, SUNG-JIN CHO*, HAN-DOO KIM*, UN-SOOK CHOI AND JI-YOUN CHOI

Abstract. In this paper, we study the number of solutions to the equation $(x+1)^d = x^d + 1$. This equation gives the value of the third power sum equation in case of Niho type exponents and is helpful in finding the distribution of the values $C_d(\tau)$. We provide the number of the solutions using the new method.

AMS Mathematics Subject Classification : 97N70, 11G25, 94A55, 68Q87.
Key words and phrases : Cross-correlation, finite field, decimation, m-sequence.

1. Introduction

Pseudorandom binary sequences of maximal period are widely used in many areas of engineering and sciences due to their randomness but simplicity in their generation. Some well-known applications include Code-Division Multiple-Access(CDMA) mobile communications and stream-cipher system. Especially families of binary sequences with low correlation have important applications in CDMA communication systems and cryptography. Cross-correlation properties of these sequences were studied due to their applications in sequence designs. The cross-correlation between binary sequences lead to difficult problems and is related to exponential sums over finite fields. Cross-correlation functions $C_d(\tau)$ of maximal length sequences have been studied for about fifty years [3, 4]. Niho [8], Helleseth [4] and Rosendahl [9] wrote the powerful theses on the topic. In this paper p will be an arbitrary prime. We denote $q = p^k$ and d satisfies the Niho condition $d \equiv 1(mod\ q-1)$. We study the number of solutions to the equation $(x+1)^d = x^d + 1$, where $x \in GF(q^2)$. Solving this equation gives the value of the third power sum $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^3$ and is helpful in finding the distribution of the values $C_d(\tau)$. In addition, this equation is related to the number of codewords of weight three in certain cyclic codes [7] and nonlinearity

Received September 6, 2012. Accepted November 15, 2012. *Corresponding author.

properties of power functions [1], which is of interest in cryptography. Niho used the result due to Welch to treat the $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^3$. And Rosendahl's work was mathematical throughout, the emphasis being on equations over finite fields. For the theory of finite fields, we refer to [2, 5, 6]. In this paper we solve the equation $(x+1)^d = x^d + 1$ using the new method.

2. Preliminaries

The cross-correlation function $C_d(\tau)$ between the sequences $u(t)$ and $v(t)$, where $v(t) = u(dt)$ $(d = 1, \ldots, p^n - 2)$, is defined for $\tau = 0, 1, \ldots, p^n - 2$ by $C_d(\tau) = \sum_{\tau=0}^{p^n-2}(-1)^{u(t+\tau)+v(t)}$. Let $x \in GF(q^2)$. In analogy with the usual complex conjugation we define $\overline{x} = x^q$. We define the unit circle of $x \in GF(q^2)$ to be the set $S = \{x \in GF(p^n) |\ x\overline{x} = 1\}$. S is the group of $(q+1)$-st roots of unity in $GF(q^2)$. We will use the property of the group S in the proof of next section.

The following theorem is useful in finding the distributions of values $C_d(\tau)$. In particular, finding b in (c) is the main study of this paper. This is provided in section 3.

Theorem 2.1 ([4, 8]). *Let $n = 2k$ and $q = p^k$. For some integer d $(d = 1, \ldots, p^n - 2)$, we have*

(a) $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1) = p^n$.

(b) $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^2 = p^{2n}$.

(c) $\sum_{\tau=0}^{p^n-2}(C_d(\tau)+1)^3 = p^{2n}b$,

where b is the number of $x \in GF(q^2)$ such that $(x+1)^d = x^d + 1$.

3. The number of solutions to the equation $(x+1)^d = x^d + 1$

Lemma 3.1. *Let $q = p^k$, where p is a prime and let $d \equiv 1 (mod\ q-1)$. Then $x \in GF(q^2) \setminus \{0, -1\}$ is a solution to*

$$(x+1)^d = x^d + 1 \tag{3.1.1}$$

if and only if $x^{d-1} = (x+1)^{d-1} = 1$ or $x^{d-q} = (x+1)^{d-q} = 1$.

Proof. Since $(x+1)^d = x^d + 1$,

$$(\overline{x}+1)^d = (x^q+1)^d = (x+1)^{qd} = \{(x+1)^d\}^q = (x^d+1)^q = \overline{x}^d + 1. \tag{3.1.2}$$

Thus

$$(x\overline{x} + x + \overline{x} + 1)^d = (x\overline{x})^d + x^d + \overline{x}^d + 1. \tag{3.1.3}$$

Since $x\overline{x} \in GF(q)$ and $x + \overline{x} \in GF(q)$, $x\overline{x} + x + \overline{x} + 1 \in GF(q)$ and thus $(x\overline{x} + x + \overline{x} + 1)^d = x\overline{x} + x + \overline{x} + 1$ and $(x\overline{x})^d = x\overline{x}$. Therefore we have

$$x\overline{x} + x + \overline{x} + 1 = x\overline{x} + x^d + \overline{x}^d + 1, \tag{3.1.4}$$

i.e.,

$$x + \overline{x} = x^d + \overline{x}^d. \tag{3.1.5}$$

Multiply x^{d-q-1} to the both sides of (3.1.5), then

$$x^{d-q} + x^{d-1} = x^{2d-q-1} + x^{qd+d-q-1}. \tag{3.1.6}$$

Since $d \equiv 1(mod\ q-1)$, there exists an integer s such that $d-1 = (q-1)s$. Since

$$x^{qd+d-q-1} = x^{(q+1)(d-1)} = x^{(q+1)(q-1)s} = 1, \tag{3.1.7}$$

we have

$$x^{2d-q-1} - x^{d-q} - x^{d-1} + 1 = (x^{d-1}-1)(x^{d-q}-1) = 0. \tag{3.1.8}$$

Thus we have $x^d = x$ or $x^d = x^q = \overline{x}$.
(i) $x^d = x$: $(x+1)^d = x^d + 1 = x + 1$ and thus $(x+1)^{d-1} = 1$.
(ii) $x^d = \overline{x}$: We have $(x+1)^d = \overline{x} + 1 = (x+1)^q$. Thus $(x+1)^{d-q} = 1$.
Conversely, let $x^{d-1} = (x+1)^{d-1} = 1$. Then $(x+1)^d = x+1$ and $x^d = x$ and thus $(x+1)^d = x+1 = x^d + 1$. Therefore x is a solution to (3.1.1). And let $x^{d-q} = (x+1)^{d-q} = 1$. Then $(x+1)^d = (x+1)^q = x^q + 1 = x^d + 1$. Therefore x is a solution to (3.1.1). □

Corollary 3.2. *Let $q = p^k$, where p is a prime and let $d \equiv 1(mod\ q-1)$. Then $x \in GF(q^2) \setminus \{0, -1\}$ is a solution to*

$$(x+1)^d = x^d + 1 \tag{3.2.1}$$

Then $(\frac{x+1}{\overline{x}+1})^{d-1} = 1$ or $(\frac{x+1}{\overline{x}+1})^{d+1} = 1$.

Proof. By Lemma 3.1 $x^d = x$ or $x^d = \overline{x}$. Also $x + \overline{x} = x^d + \overline{x}^d$ from (3.1.5).
(i) $x^d = x$: Since $\overline{x}^d = \overline{x}$ from (3.1.5), we have

$$(\frac{x+1}{\overline{x}+1})^d = \frac{x^d+1}{\overline{x}^d+1} = \frac{x+1}{\overline{x}+1}$$

and thus $(\frac{x+1}{\overline{x}+1})^{d-1} = 1$.
(ii) $x^d = \overline{x}$: Since $\overline{x}^d = x$ from (3.1.5), we have

$$(\frac{x+1}{\overline{x}+1})^d = \frac{x^d+1}{\overline{x}^d+1} = \frac{\overline{x}+1}{x+1}$$

and thus $(\frac{x+1}{\overline{x}+1})^{d+1} = 1$. □

Lemma 3.3. *Let $d = (q-1)s+1$ and $e = (q-1)t+1$. Assume that*

$$gcd(s, q+1) = gcd(t, q+1)\ ,\ gcd(s-1, q+1) = gcd(t-1, q+1). \tag{3.3.1}$$

Then $x \in GF(q^2)$ is a solution to (3.1.1) if and only if x satisfies

$$(x+1)^e = x^e + 1. \tag{3.3.2}$$

Proof. Since every $x \in GF(q)$ is a solution to (3.1.1), we may assume that $x \in GF(q^2)\setminus\{0,-1\}$. Let x be a solution to (3.1.1). Then by Lemma 3.1 $x^{d-1} = (x+1)^{d-1} = 1$ or $x^{d-q} = (x+1)^{d-q} = 1$. Since $x^d = x$, $x^d = x^{(q-1)s} \cdot x = x$ and thus $x^{(q-1)s} = 1$. Since $x^{q^2-1} = 1$ and

$$x^{gcd((q-1)t,q^2-1)} = (x^{(q-1)})^{gcd(t,q+1)} = (x^{(q-1)})^{gcd(s,q+1)} = x^{gcd((q-1)s,q^2-1)} = 1,$$

$x^{(q-1)t} = 1$. Thus $x^e = x^{(q-1)t+1} = x^{(q-1)t} \cdot x = x$. Now assume that $x^d = \overline{x}$. Then

$$1 = x^{d-q} = x^{(q-1)(s-1)}. \tag{3.3.3}$$

Since $x^{q^2-1} = 1$ and $x^{gcd((q-1)(s-1)s,q^2-1)} = x^{gcd((q-1)(t-1),q^2-1)}$,
$x^{e-q} = x^{(q-1)(t-1)} = 1$. Thus $x^e = \overline{x}$. Similarly we can prove that $(x+1)^e = x+1$ and $(x+1)^e = (x+1)^q$. Therefore $x^{e-1} = (x+1)^{e-q} = 1$. Thus by Lemma 3.1 x is a solution to (3.3.2). The converse proof for d is the same as the proof for e. This completes the proof. □

Lemma 3.4. *Let $q = p^k$ be odd. Assume that $d = (q-1)s+1$. Let $gcd(s,q+1) \cdot gcd(s-1,q+1) = 2$. Then $gcd(d-1,q+1)|4$ and $gcd(d+1,q+1)|4$.*

Proof.

$$\begin{aligned} gcd(d-1,q+1) &= gcd((q-1)s,q+1) \\ &= gcd((q+1)s-2s,q+1) \\ &= gcd(2s,q+1) \\ gcd(d+1,q+1) &= gcd((q-1)s+2,q+1) \\ &= gcd((q+1)s-2s+2,q+1) \\ &= gcd(2(s-1),q+1) \end{aligned}$$

If $gcd(s,q+1) = 2andgcd(s-1,q+1) = 2$, then $gcd(d-1,q+1) = 2$ or 4 and $gcd(d+1,q+1) = 2$.
If $gcd(s,q+1) = 1andgcd(s-1,q+1) = 2$, then $gcd(d-1,q+1) = 2$ and $gcd(d+1,q+1) = 2$ or 4. □

Lemma 3.5. *Let $x \in GF(q^2)\setminus\{0,-1\}$, where $q = p^k$ is odd and let $x \notin GF(q)$ such that $x^2 = -1$. Then $ord((x+1)^{q-1}) > 2$.*

Proof. Since $x^q \neq x$,

$$\{(x+1)^{q-1}\}^2 = (x^2+2x+1)^{q-1} = 2^{q-1}x^{q-1} = x^{q-1} \neq 1.$$

Thus $ord((x+1)^{q-1}) > 2$. □

Theorem 3.6. *Let $q = p^k$ be odd. Assume that $d \equiv 1(mod\ q-1)$. And let $gcd(s,q+1) \cdot gcd(s-1,q+1) = 2$. Then*

$$\{x \in GF(q^2)|(x+1)^d = x^d+1\} = GF(q). \tag{3.6.1}$$

Proof. We may assume that $x \in GF(q^2) \setminus \{0, -1\}$. By Lemma 3.1 $x^d = x$ or $x^d = \overline{x}$. Let A be the left side of (3.6.1). Since every $x \in GF(q)$ is a solution to (3.1.1), $GF(q) \subset A$. Suppose that $x \in A$ and $x \notin GF(q)$.

(I) $gcd(d-1, q+1) = gcd(d+1, q+1) = 2$: Since $gcd(d \pm 1, q+1) = 2$ and $\frac{x+1}{\overline{x}+1} \in S$ by Corollary 3.2

$$(\frac{x+1}{\overline{x}+1})^2 = 1. \tag{3.6.2}$$

Thus $x^2 + 2x + 1 = \overline{x}^2 + 2\overline{x} + 1$. Therefore $(x - \overline{x})(x + \overline{x} + 2) = 0$. Since $x \neq \overline{x}$,

$$x + \overline{x} = -2. \tag{3.6.3}$$

(i) $x^d = x$: In this case $x^{d-1} = x^{(q-1)s} = 1$.
Thus $(x^{q-1})^{gcd(s,q+1)} = x^{gcd((q-1)s, q^2-1)} = 1$. Since $gcd(s, q+1)|2$, $x^{2(q-1)} = 1$. Thus $\overline{x}^2 = x^{2q} = x^{2(q-1)} \cdot x^2 = x^2$. Therefore $x^2 - \overline{x}^2 = (x - \overline{x})(x + \overline{x}) = 0$. Since $x \notin GF(q)$, $x + \overline{x} = 0$. This is a contradiction to (3.6.3).
(ii) $x^d = \overline{x}$: In this case $x^{d-q} = x^{(q-1)(s-1)} = 1$. Thus $(x^{q-1})^{gcd(s-1,q+1)} = x^{gcd((q-1)(s-1), q^2-1)} = 1$. Since $gcd(s-1, q+1)|2$, $x^{2(q-1)} = 1$. Thus $\overline{x}^2 = x^{2q} = x^{2(q-1)} \cdot x^2 = x^2$. Therefore $x^2 - \overline{x}^2 = (x - \overline{x})(x + \overline{x}) = 0$. Since $x \notin GF(q)$, $x + \overline{x} = 0$. This is a contradiction to (3.6.3). Therefore by (i) and (ii) $x \in GF(q)$.

(II) $gcd(d-1, q+1) = 4$ or $gcd(d+1, q+1) = 4$: Since $gcd(d-1, q+1) = 4$ or $gcd(d+1, q+1) = 4$, by Corollary 3.2

$$(\frac{x+1}{\overline{x}+1})^4 = 1. \tag{3.6.4}$$

(i) $x^d = x$: In this case $x^{d-1} = x^{(q-1)s} = 1$.
Thus $(x^{q-1})^{gcd(s,q+1)} = x^{gcd((q-1)s, q^2-1)} = 1$. Since $gcd(s, q+1)|2$, $x^{2(q-1)} = 1$. Thus $\overline{x}^2 = x^{2q} = x^{2(q-1)} \cdot x^2 = x^2$. Therefore from (3.6.4) we obtain $(x - \overline{x})(x^2 + 1) = 0$. Since $x \notin GF(q)$, $x^2 = -1$. Thus $x^4 = 1$.
(a) If $q \equiv 1 (mod\ 4)$, then $x^{q-1} = 1$ and thus $x^q = x$, i.e., $x \in GF(q)$. This is a contradiction.
(b) If $q \equiv -1 (mod\ 4)$, then $x^{q+1} = 1$. Since $(x+1)^d = (x+1)^{(q-1)s}(x+1) = x+1$, $(x+1)^{(q-1)s} = 1$. Since $\{(x+1)^{q-1}\}^{q+1} = 1$, $\{(x+1)^{q-1}\}^{gcd(s,q+1)} = 1$. And thus $\{(x+1)^{q-1}\}^2 = 1$. This means that $ord((x+1)^{q-1}) \leq 2$. But by Lemma 3.5 $ord((x+1)^{q-1}) > 2$. This is a contradiction.
(ii) $x^d = \overline{x}$: In this case $x^{d-q} = x^{(q-1)(s-1)} = 1$. Thus $(x^{q-1})^{gcd(s-1,q+1)} = x^{gcd((q-1)(s-1), q^2-1)} = 1$. Since $gcd(s-1, q+1)|2$, $x^{2(q-1)} = 1$. Thus $\overline{x}^2 = x^{2q} = x^{2(q-1)} \cdot x^2 = x^2$. Therefore from (3.6.4) we obtain $(x - \overline{x})(x^2 + 1) = 0$. Since $x \notin GF(q)$, $x^2 = -1$. Thus $x^4 = 1$.
(a) If $q \equiv 1 (mod\ 4)$, then $x^{q-1} = 1$. This is a contradiction.
(b) If $q \equiv -1 (mod\ 4)$, then $x^{q+1} = 1$. Since $(x+1)^d = (x+1)^{(q-1)(s-1)}(x+1)^q = x^q + 1$, $(x+1)^{(q-1)(s-1)} = 1$. Since $\{(x+1)^{q-1}\}^{q+1} = 1$, $\{(x+1)^{q-1}\}^{gcd(s-1,q+1)} =$

1. And thus $\{(x+1)^{q-1}\}^2 = 1$. This means that $ord((x+1)^{q-1}) \leq 2$. But by Lemma 3.5 $ord((x+1)^{q-1}) > 2$. This is a contradiction. Hence by (I) and (II) $x \in GF(q)$. This completes the proof. □

Theorem 3.7. *Assume that $d \equiv 1(mod\ 2^k - 1)$. If $gcd(d \pm 1, 2^k + 1) = 1$, then*

$$(x+1)^d = x^d + 1 \tag{3.7.1}$$

has exactly 2^k solutions in $GF(2^n)$.

Proof. Since $d \equiv 1(mod\ 2^k - 1)$, every $x \in GF(2^k)$ is a solution to (3.7.1). So we may assume that $x \neq 0, 1$ satisfies (3.7.1). Since x is a solution to (3.7.1), $x^d = x$ or $x^d = \overline{x}$ by Lemma 3.1. Let $x^d = x$. Then by Corollary 3.2 $(\frac{x+1}{\overline{x}+1})^{d-1} = 1$. And let $x^d = \overline{x}$. Then by Corollary 3.2 $(\frac{x+1}{\overline{x}+1})^{d+1} = 1$. Since $gcd(d \pm 1, 2^k + 1) = 1$,

$$\frac{x+1}{\overline{x}+1} = 1. \tag{3.7.2}$$

Thus $\overline{x} = x$. This means that $x \in GF(2^k)$. □

Theorem 3.8. *Assume that $gcd(s, q+1) > 2$ or $gcd(s-1, q+1) > 2$. Then*

$$\{x \in GF(q^2) | (x+1)^d = x^d + 1\} \neq GF(q) \tag{3.8.1}$$

Proof. Let $gcd(s, q+1) = w > 2$. Then $s = wa$ and $q + 1 = wb$, where $gcd(a, b) = 1$. Let $x_0 = \alpha^b$ and $x_1 = \alpha^{2b}$. Then $x_0 \neq 1,\ x_1 \neq 1,\ x_0 \neq x_1,\ x_0^{q-1} \neq x_1^{q-1}$ and $x_0^{d-1} = x_1^{d-1} = 1$ because $w > 2$. Since $(x_0^{q-1})^{q+1} = (x_1^{q-1})^{q+1} = 1$, $\{x_0^{q-1}, x_1^{q-1}\} \in S$. Also $x_0^{q-1} \neq 1$ and $x_1^{q-1} \neq 1$. Let $u_0 = \frac{x_0 x_1^q - x_0 x_1}{x_0^q x_1 - x_0 x_1^q}$ and $u_1 = \frac{x_0^q x_1 - x_0 x_1}{x_0^q x_1 - x_0 x_1^q}$. Since $x_0^{q-1} \neq x_1^{q-1}$, u_0 and u_1 are well-defined. Since

$$\begin{aligned} u_0^q &= (\tfrac{x_0 x_1^q - x_0 x_1}{x_0^q x_1 - x_0 x_1^q})^q \\ &= \tfrac{x_0^q x_1 - x_0^q x_1^q}{x_0 x_1^q - x_0^q x_1} \\ &= x_0^{q-1} \tfrac{x_0 x_1 - x_0 x_1^q}{x_0 x_1^q - x_0^q x_1} \\ &= x_0^{q-1} u_0 \end{aligned}$$

and $x_0^{q-1} \neq 1,\ u_0^q \neq u_0$. Therefore $u_0 \notin GF(q)$. Similarly we can show that $u_1^q = x_1^{q-1} u_1$. Since $x_1^{q-1} \neq 1,\ u_1 \notin GF(q)$. Also $u_1 = u_0 + 1$. Moreover,

$$u_0^{d-1} = u_0^{(q-1)s} = (x_0^{q-1})^s = x_0^{d-1} = 1 \tag{3.8.2}$$

and

$$u_1^{d-1} = u_1^{(q-1)s} = (x_1^{q-1})^s = x_1^{d-1} = 1. \tag{3.8.3}$$

By (3.8.2) and (3.8.3) we have

$$(u_0 + 1)^d = u_1^d = u_1 = u_0 + 1 = u_0^d + 1. \tag{3.8.4}$$

Hence u_0 is a solution to (3.8.1) which is not in $GF(q)$. For the case $gcd(s-1, q+1) > 2$ we can prove (3.8.1) using the similar method of the case $gcd(s, q+1) > 2$. □

Lemma 3.9. *Let $q = p^k$ for a prime p and $d = (q-1)s+1$.*
(a) If $gcd(s-1, q+1) = 1$ and $gcd(s, q+1) = p^i + 1$ for some integer $i \geq 1$, then $gcd(d-1, q+1) = gcd(s, q+1)$.
(b) If $gcd(s-1, q+1) = p^i + 1$ and $gcd(s, q+1) = 1$ for some integer $i \geq 1$, then $gcd(d+1, q+1) = gcd(s-1, q+1)$.

Proof. (I) Let $p = 2$.
a) $gcd(s-1, q+1) = 1$ and $gcd(s, q+1) = p^i + 1$: Since $q+1$ is odd,

$$\begin{aligned} gcd(d-1, q+1) &= gcd((q-1)s, q+1) \\ &= gcd((q+1)s + 2s, q+1) \\ &= gcd(2s, q+1) \\ &= gcd(s, q+1). \end{aligned}$$

b) $gcd(s-1, q+1) = p^i + 1$ and $gcd(s, q+1) = 1$: Since $q+1$ is odd,

$$\begin{aligned} gcd(d+1, q+1) &= gcd((q-1)s + 2, q+1) \\ &= gcd((q+1)s - 2s + 2, q+1) \\ &= gcd(2(s-1), q+1) \\ &= gcd(s-1, q+1). \end{aligned}$$

In fact, the conditions in (a) and (b) are not necessary.
(II) Let p be an odd prime.
By conditions (a) and (b), $p^i + 1$ divides $p^k + 1$. Thus $i|k$ and $\frac{k}{i}$ is odd.
Let $p^k + 1 = (p^i + 1) \cdot a$. Then

$$p^k + 1 = (p^i + 1)\{[(p^i)^{k/i-1} - (p^i)^{k/i-2}] + \cdots + [(p^i)^2 - p^i] + 1\}. \qquad (3.9.1)$$

Thus by equation (3.9.1) a is odd.
a) $gcd(s-1, q+1) = 1$ and $gcd(s, q+1) = p^i + 1$:
Since $gcd(s, q+1) = p^i + 1$, let $s = (p^i + 1)b$ where $gcd(a, b) = 1$. Then

$$\begin{aligned} gcd(d-1, q+1) &= gcd((q-1)s, q+1) \\ &= gcd((q+1)s + 2s, q+1) \\ &= gcd(2s, q+1) \\ &= gcd(2b(p^i + 1), (p^i + 1)a) \\ &= (p^i + 1)gcd(2b, a) \\ &= p^i + 1 \\ &= gcd(s, q+1). \end{aligned}$$

b) $gcd(s-1, q+1) = p^i + 1$ and $gcd(s, q+1) = 1$:
Since $gcd(s-1, q+1) = p^i + 1$, let $s - 1 = (p^i + 1)c$ where $gcd(a, c) = 1$. Then

$$\begin{aligned} gcd(d+1, q+1) &= gcd(2(s-1), q+1) \\ &= gcd(2c(p^i + 1), (p^i + 1)a) \\ &= (p^i + 1)gcd(2c, a) \\ &= p^i + 1 \\ &= gcd(s-1, q+1). \end{aligned}$$

□

Theorem 3.10. *Let $q = p^k$ for a prime p and $d = (q-1)s+1$. Assume that for some i ($i|k$ and $\frac{k}{i}$:odd) (i) $gcd(s-1, q+1) = 1$ and $gcd(s, q+1) = p^i + 1$ or (ii) $gcd(s-1, q+1) = p^i + 1$ and $gcd(s, q+1) = 1$. Then the set of solutions in $GF(q^2)$ to the following equation is $GF(q) \cup GF(p^{2i})$.*

$$(x+1)^d = x^d + 1 \tag{3.10.1}$$

Proof. Clearly every $x \in GF(q)$ is a solution to (3.10.1). So we may assume that $x \notin GF(q)$. Then $x^q = \overline{x} \neq x$. Since x is a solution to (3.10.1), $x^d = x$ or $x^d = \overline{x}$ by Lemma 3.1. By Corollary 3.2

$$\left(\frac{x+1}{\overline{x}+1}\right)^{d-1} = 1 \ \ or \ \ \left(\frac{x+1}{\overline{x}+1}\right)^{d+1} = 1 \tag{3.10.2}$$

Since $\frac{x+1}{\overline{x}+1} \in S$, $(\frac{x+1}{\overline{x}+1})^{q+1} = 1$. By Lemma 3.9, $gcd(d-1, q+1) = p^i + 1$ or $gcd(d+1, q+1) = p^i + 1$. Thus $(\frac{x+1}{\overline{x}+1})^{p^i+1} = 1$. Therefore

$$x^{p^i+1} + x^{p^i} + x + 1 = \overline{x}^{p^i+1} + \overline{x}^{p^i} + \overline{x} + 1. \tag{3.10.3}$$

Since $(x^{q-1})^{q+1} = 1$ and $(x^{q-1})^s = x^{d-1} = 1, (x^{q-1})^{gcd(s,q+1)} = 1$. Thus by hypothesis $(x^{q-1})^{p^i+1} = 1$. Therefore

$$\overline{x}^{p^i+1} = (x^q)^{p^i+1} = (x^{q-1})^{p^i+1} x^{p^i+1} = x^{p^i+1}. \tag{3.10.4}$$

Thus we obtain

$$x^{p^i} + x = \overline{x}^{p^i} + \overline{x}, \tag{3.10.5}$$

i.e.,

$$x^{p^i} - \overline{x}^{p^i} = \overline{x} - x. \tag{3.10.6}$$

Since $\overline{x} \neq x$,

$$x^{p^i-1} + x^{p^i-2}\overline{x} + x^{p^i-3}\overline{x}^2 + \cdots + x\overline{x}^{p^i-2} + \overline{x}^{p^i-1} + 1 = 0. \tag{3.10.7}$$

From (3.10.7) we obtain

$$x^{p^i}(1 + x^{q-1} + x^{2(q-1)} + \cdots + x^{(p^i-2)(q-1)} + x^{(p^i-1)(q-1)}) = -x. \tag{3.10.8}$$

Since $(x^{q-1})^{p^i+1} = 1$ by (3.10.4),

$$1 + x^{q-1} + x^{2(q-1)} + \cdots + x^{(p^i-1)(q-1)} + x^{p^i(q-1)} = \frac{1 - (x^{q-1})^{p^i+1}}{1 - x^{q-1}} = 0. \tag{3.10.9}$$

Thus

$$x^{p^i} \cdot x^{p^i(q-1)} = x. \tag{3.10.10}$$

Therefore $\overline{x}^{p^i} = x$. And thus from (3.10.5) we have $x^{p^i} = \overline{x} = x^{p^k}$. So

$$x^{p^{2i}} = (x^{p^i})^{p^i} = (x^{p^i})^{p^k} = \overline{x}^{p^i} = x. \tag{3.10.11}$$

Hence $x \in GF(p^{2i})$.
Now we show that every $x \in GF(p^{2i})$ is a solution to (3.10.1).

(a) $p^i + 1|s$: Since $i|k$, $p^i - 1$ divides $q - 1$. Thus $q - 1 = (p^i - 1)u_1$ for some integer u_1. Since $s = (p^i + 1)u_2$ for some u_2,

$$d - 1 = (q - 1)s = (p^i - 1)u_1(p^i + 1)u_2 = (p^{2i} - 1)u_1u_2.$$

Thus $d \equiv 1(mod\ p^{2i} - 1)$. Hence x is a solution to (3.10.1).
(b) $(p^i + 1)|(s - 1)$: Since $i|k$, $(p^i - 1)$ divides $(q - 1)$. Thus $q - 1 = (p^i - 1)u_3$ for some integer u_3. Since $s - 1 = (p^i + 1)u_4$ for some u_4,

$$d - q = (q - 1)(s - 1) = (p^{2i} - 1)u_3u_4.$$

Thus $d \equiv q = p^k(mod\ p^{2i} - 1)$. Hence x is a solution to (3.10.1). This completes the proof. □

Remark 3.11. Since $i|k$, $GF(q) \cap GF(p^{2i}) = GF(p^i)$. Thus the number of solutions to (3.10.1) is $p^k + p^{2i} - p^i$.

4. Conclusion

The equation $(x+1)^d = x^d+1$ gives the value of the third power sum equation in case of Niho type exponents and is helpful in finding the distribution of the values $C_d(\tau)$. In this paper we solved the equation $(x+1)^d = x^d+1$ and provided the number of the solutions by using the new method different to method of Niho.

References

1. H. Dobbertin, *Almost perfect nonlinear power functions on $GF(2^n)$:the Welch case*, IEEE Transactions on Information Theory, 45(4):1271-1275, 1999.
2. S.W. Golomb, *Shift register sequences*, Discrete Mathematics, Holden Day, 1967.
3. Han-Doo Kim and Sung-Jin Cho, *A new proof about the decimations with Niho type five-valued cross-correlation functions*, J. Appl. Math. and Informatics, 30(5-6):903-911, 2012.
4. T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Mathematics, 16(3):209-232, 1976.
5. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.
6. R. McEliece, *Finite fields for computer scientists and engineers*, Kluwer Academic Publishers, Boston, 1987.
7. G. McGuire, *On certain 3-weight cyclic codes having symmetric weights and a conjecture of Helleseth*, In Sequences and their applications(Bergen, 2001), Discrete Math. Theor. Comput. Sci. (Lond.), pages 281-295. Springer, London, 2002.
8. Y. Niho, *Multi-valued cross-correlation functions between two maximal linear recursive sequences*, Ph.D thesis, University of Southern California, 1972.
9. P. Rosendahl, *Niho type cross-correlation functions and related equations*, Ph.D thesis, Turku center for computer science, 2004.

Ji-Mi Yim received M.Sc. at Pukyong National University. She is currently a Ph.D. candidate at Pukyong National University since 2008. Her research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 608-737, Korea.
e-mail: jimiya15@hanmail.net

Sung-Jin Cho received M.Sc. and Ph.D. at Korea University. He is currently a professor at Pukyong University since 1988. His research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 608-737, Korea.
e-mail: sjcho@pknu.ac.kr

Han-Doo Kim received M.Sc. and Ph.D. at Korea University. He is currently a professor at Inje University since 1989. His research interests include finite field theory, discrete mathematics and cellular automata.

Institute of Basic Science and Department of Computer Aided Science, Inje University, Gimhae 621-749, Korea.
e-mail: mathkhd@inje.ac.kr

Un-Sook Choi received M.Sc. and Ph.D. at Pukyong National University. She is currently a professor at Tongmyong University. Her research interests include finite field theory, discrete mathematics and cellular automata.

School of Free Major, Tongmyoung University, Busan, 608-711, Korea.
e-mail: choies@tu.ac.kr

Ji-Youn Choi received B.S. at Pukyong National University. She is currently a M.Sc. candidate at Pukyong National University since 2010. Her research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 608-737, Korea.
e-mail: piggyya@hanmail.net