Discrete Mathematics 16 (1976) 209–232

SOME RESULTS ABOUT THE CROSS-CORRELATION FUNCTION BETWEEN TWO MAXIMAL LINEAR SEQUENCES

Tor HELLESETH

Mathematical Institute, University of Bergen, Bergen, Norway

Received 11 March 1975
Revised 26 September 1975

Let $\{a_i\}$ and $\{a_{di}\}$ be two maximal linear sequences of period $p^n - 1$. The cross-correlation function is defined by $C_d(t) = \sum_{i=0}^{p^n-2} \zeta^{a_i - a_{di+t}}$ for $t = 0, 1, \ldots, p^n - 2$, where $\zeta = \exp(2\pi i/p)$. We find some new general results about $C_d(t)$. We also determine the values and the number of occurrences of each value of $C_d(t)$ for several new values of d.

1. Introduction

Maximal linear sequences have been the object of extensive studies. A well-known property of maximal linear sequences which has been extremely useful in applications is their two-level auto-correlation function.

To find the values of the cross-correlation function between two different maximal linear sequences of the same period is equivalent to finding the complete weight enumerator of the code with check polynomial which is the product of the recursion polynomials for the two maximal sequences. In general this seems to be a very difficult problem. The empirical results show great differences in the cross-correlation function depending on the decimation which relates the two maximal sequences. Most of the results so far consist of choosing a decimation and showing that it is three- or four-valued. Little has been done to study the general properties of the cross-correlation function. Here we will give some new general results about some of the basic properties of the cross-correlation function. We will also, however, find the values and the number of occurrences of each value of the cross-correlation function for some new decimations.

Let $c_1, \ldots, c_n$ be elements of GF(p), p prime, with $c_n \neq 0$. A linear recurrence relation over GF(p) is a difference equation of the form

$$a_i + c_1 a_{i-1} + \ldots + c_n a_{i-n} = 0. \tag{1}$$

We say that $f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$ is the characteristic polynomial associated with (1). An n-dimensional starting vector $(a_{-n}, \ldots, a_{-1})$ and (1) determine a sequence $\{a_i\}$ of period less than or equal to $p^n - 1$. It is known that $\{a_i\}$ has period exactly $p^n - 1$ if and only if $f(x)$ is a primitive polynomial over GF(p). Such

sequences are called maximal linear sequences. The following facts about maximal linear sequences are well-known.

(a) There exist $\varphi(p^n - 1)/n$ maximal linear sequences which are not equivalent under cyclic shifts.

(b) Let $\{a_i\}$ be a maximal linear sequence. Then $a_i = \mathrm{Tr}_1^n(\beta\alpha^i)$, where $\mathrm{Tr}_1^n(\xi) = \sum_{i=0}^{n-1} \xi^{p^i}$ and α is a primitive root of $f(x)$. Here $\beta \in \mathrm{GF}(p^n)^* = \mathrm{GF}(p^n) - \{0\}$, and each choice of β gives a cyclic shift of $\{a_i\}$.

(c) Let $\{a_i\}$ be a maximal linear sequence. Then $\{a_{di}\}$ is a maximal linear sequence if and only if g.c.d.$(d, p^n - 1) = 1$.

(d) Let $\{a_i\}$ and $\{b_i\}$ be two different maximal linear sequences of period $p^n - 1$. There exist a d prime to $p^n - 1$ and a k such that $\{b_{i+k}\} = \{a_{di}\}$.

Definition 1.1. Let $\{a_i\}$ and $\{b_i\}$ be sequences of elements from GF(p) with period ε. Let $\zeta \neq 1$ be a complex pth of unity. Let $\theta(x) = \zeta^x$ and $\bar{\theta}(x) = \zeta^{-x}$. *The cross-correlation function* between $\{a_i\}$ and $\{b_i\}$ is then defined as

$$C_{ab}(t) = \sum_{i=0}^{\varepsilon-1} \theta(a_{i+t})\bar{\theta}(b_i). \tag{2}$$

Let $\{a_i\}$ and $\{b_i\}$ be two maximal linear sequences. When we study the cross-correlation function between them we compare the two sequences term by term over one period. We do this for all $p^n - 1$ possible relative shifts between $\{a_i\}$ and $\{b_i\}$. We are only interested in the values of $C_{ab}(t)$ and of the number of occurrences of each value. According to (a)–(d) we can assume $a_i = \mathrm{Tr}_1^n(\alpha^i)$ and $\{b_i\} = \{a_{di}\}$ by suitable phase shifts. Therefore we can write

$$\begin{aligned} C_{ab}(t) &= \sum_{i=0}^{\varepsilon-1} \theta(a_{i+t})\bar{\theta}(b_i) \qquad (3)\\ &= \sum_{i=0}^{p^n-2} \theta(\mathrm{Tr}_1^n(\alpha^{i+t} - \alpha^{di})) \\ &= \sum_{x \in \mathrm{GF}(p^n)^*} \zeta^{\mathrm{Tr}_1^n(cx - x^d)}, \quad \text{where } c = \alpha^{-t}. \end{aligned}$$

We will from now on consider maximal linear sequences, and we write $C_d(t)$ instead of $C_{ab}(t)$.

2. Summary of known results

Let $p = 2$. The earlier results on enumeration of $C_d(t)$ can be summarized in the following theorems.

Theorem 2.1. *Let $d = 2^k + 1$ or $d = 2^{2k} - 2^k + 1$ with $e = n/$g.c.d.(n, k) odd. Then $C_d(t)$ takes on three values:*

(i) $-1+2^{(n+e)/2}$ *occurs* $2^{n-e-1}+2^{(n-e-2)/2}$ *times*,
(ii) -1 *occurs* $2^n-2^{n-e}-1$ *times*,
(iii) $-1-2^{(n+e)/2}$ *occurs* $2^{n-e-1}-2^{(n-e-2)/2}$ *times*.

For a proof see for instance Gold [3], Kasami [5] or Kasami et al. [6].

Theorem 2.2. *Let* $d=2^{m+1}-1$ *where* $n=2m$. *Then* $C_d(t)$ *takes on four values*:
(i) $-1+2^{m+1}$ *occurs* $\frac{1}{3}(2^{2m-1}-2^{m-1})$ *times*,
(ii) $-1+2^m$ *occurs* 2^m *times*,
(iii) -1 *occurs* $2^{2m-1}-2^{m-1}-1$ *times*,
(iv) $-1-2^m$ *occurs* $\frac{1}{3}(2^{2m}-2^m)$ *times*.

Theorem 2.3. *Let* $d=(2^m-1)(2^{2m}+1)+2$ *where* $n=4m$. *Then* $C_d(t)$ *takes on four values*:
(i) $-1+2^{3m}$ *occurs* 2^m *times*,
(ii) $-1+2^{2m}$ *occurs* $2^{4m-1}-2^{3m-1}$ *times*,
(iii) -1 *occurs* $2^{3m}-2^m-1$ *times*,
(iv) $-1-2^{2m}$ *occurs* $2^{4m-1}-2^{3m-1}$ *times*.

These two theorems are due to Niho [10].

For sequences over GF(p), p an odd prime, Trachtenberg [13] has proved the following:

Theorem 2.4. *When* n *is odd and* $d=\frac{1}{2}(p^{2k}+1)$ *or* $d=p^{2k}-p^k+1$ *where* $d\not\equiv p^i \pmod{p^n-1}$, *then* $C_d(t)$ *takes on three values*:
(i) $-1+p^{(n+e)/2}$ *occurs* $\frac{1}{2}(p^{n-e}+p^{(n-e)/2})$ *times*,
(ii) -1 *occurs* $p^n-p^{n-e}-1$ *times*,
(iii) $-1+p^{(n+e)/2}$ *occurs* $\frac{1}{2}(p^{n-e}-p^{(n-e)/2})$ *times, where* $e=$ g.c.d.(n,k).

For p a prime, Carlitz and Uchiyama [2] have proved the next theorem.

Theorem 2.5. *We have that*
(i) $|C_d(t)+1|\leq(d-1)p^{n/2}$, *and*
(ii) $|C_d(t)|\leq 2p^{n/2}$.

3. Preliminaries

Theorem 3.1. *We have*
(a) $C_d(t)$ *is a real number.*
(b) *The values and the number of occurrences of each value of* $C_d(t)$ *are independent of the choice of* ζ.
(c) $C_d(t)=C_{d^{-1}}(-dt)$ *where* $d^{-1}\cdot d\equiv 1 \pmod{p^n-1}$.

(d) $C_{cp^i}(t) = C_d(t)$.

(e) $C_d(p^i t) = C_c(t)$.

(f) $$\sum_{t=0}^{p^n-2} C_d(t) = 1.$$

(g) $$C_1(t) = \begin{cases} p^n - 1 & \text{when } t \equiv 0 \pmod{p^n - 1}, \\ -1 & \text{when } t \not\equiv 0 \pmod{p^n - 1}. \end{cases}$$

The proofs are simple consequences of properties of finite fields and of the trace function, cf. Trachtenberg [13].

Theorem 3.2. *We have*

$$\sum_{t=0}^{p^n-2} C_d(t)\, C_d(t+\tau_1) \ldots C_d(t+\tau_{m-1}) =$$

$$= -(p^n-1)^{m-1} + 2(-1)^{m-1} + a_m^{(\tau_1, \ldots, \tau_{m-1})} p^{2n},$$

where $a_m^{(\tau_1, \ldots, \tau_{m-1})}$ *is the number of solutions of the following two equations:*

$$\alpha^{-\tau_1} x_1 + \alpha^{-\tau_2} x_2 + \ldots + \alpha^{-\tau_{m-1}} x_{m-1} + 1 = 0, \tag{4}$$

$$x_1^d + x_2^d + \ldots + x_{m-1}^d + 1 = 0, \tag{5}$$

with $x_i \in \mathrm{GF}(p^n)^*$ *for* $i = 1, 2, \ldots, m-1$.

Proof. Define

$$K = \{(x_0, \ldots, x_{m-1}) : x_i \in \mathrm{GF}(p^n)^*\},$$

$$H_1 = \{(x_0, \ldots, x_{m-1}) \in K : x_0 + \alpha^{-\tau_1} x_1 + \ldots + \alpha^{-\tau_{m-1}} x_{m-1} = 0\},$$

$$H_2 = \{(x_0, \ldots, x_{m-1}) \in K : x_1^d + x_2^d + \ldots + x_{m-1}^d = 0\}.$$

Let $S(y) = \zeta^{\mathrm{Tr}_1^n(y)}$. Let $\varepsilon = p^n - 1$. Then

$$\sum_{t=0}^{p^n-2} C_d(t)\, C_d(t+\tau_1) \ldots C_d(t+\tau_{m-1}) =$$

$$= \sum_{t=0}^{p^n-2} \Big(\sum_{x_0 \in \mathrm{GF}(p^n)^*} S(\alpha^{-t} x_0 - x_0^d) \Big) \ldots \Big(\sum_{x_{m-1} \in \mathrm{GF}(p^n)^*} S(\alpha^{-t-\tau_{m-1}} x_{m-1} - x_{m-1}^d) \Big)$$

$$= \sum_{K} \sum_{t=0}^{p^n-2} S(\alpha^{-t}(x_0 + \ldots + \alpha^{-\tau_{m-1}} x_{m-1}) - (x_0^d + \ldots + x_{m-1}^d))$$

$$= \sum_{K} \sum_{y \in \mathrm{GF}(p^n)^*} S(y(x_0 + \ldots + \alpha^{-\tau_{m-1}} x_{m-1}) - (x_0^d + \ldots + x_{m-1}^d))$$

$$= \sum_{K \setminus (H_1 \cup H_2)} -S(-(x_0^d + \ldots + x_{m-1}^d)) + \varepsilon \sum_{H_1 \setminus H_2} S(-(x_0^d + \ldots + x_{m-1}^d))$$

$$+ \sum_{H_2 \setminus H_1} (-1) + \sum_{H_1 \cap H_2} \varepsilon.$$

We now use that if $(x_0, \ldots, x_{m-1}) \in K - (H_1 \cup H_2)$ and $z \in \mathrm{GF}(p^n)^*$, then $(zx_0, \ldots, zx_{m-1}) \in K - (H_1 \cup H_2)$ and therefore

$$\sum_{K-(H_1 \cup H_2)} S(-(x_0^d + \ldots + x_{m-1}^d)) = (-1)(|K| - |H_1 \cup H_2|)/\varepsilon.$$

By doing the same for the next term we get

$$\sum_{t=0}^{p^n-2} C_d(t) C_d(t+\tau_1) \ldots C_d(t+\tau_{m-1}) =$$

$$= \frac{(|K| - |H_1 \cup H_2|)}{\varepsilon} + \varepsilon \frac{|H_1 - H_2|(-1)}{\varepsilon} + |H_2 - H_1|(-1) + |H_1 \cap H_2|\varepsilon$$

$$= \frac{1}{\varepsilon}(|K| - |H_1 \cup H_2| - |H_1 - H_2|\varepsilon - |H_2 - H_1|\varepsilon + |H_1 \cap H_2|\varepsilon^2)$$

$$= \frac{1}{\varepsilon}(|K| - |H_1| - |H_2| + |H_1 \cap H_2| - |H_1|\varepsilon + |H_1 \cap H_2|\varepsilon - |H_2|\varepsilon$$
$$+ |H_1 \cap H_2|\varepsilon + |H_1 \cap H_2|\varepsilon^2)$$

$$= \frac{1}{\varepsilon}(|K| - (\varepsilon+1)(|H_1| + |H_2|) + (\varepsilon+1)^2|H_1 \cap H_2|).$$

We must now find an expression for $|H_1|$ and $|H_2|$. We note that $|H_1| = |H_2|$ because g.c.d.$(d, p^n - 1) = 1$ and $(y_0, \ldots, y_{m-1}) \in H_1$ if and only if $(y_0^{d^{-1}}, \ldots, \alpha^{\tau_{m-1} - d^{-1}} y_{m-1}^{d^{-1}}) \in H_2$.

Put $d = 1$ and $\tau_1 = \tau_2 = \ldots = \tau_{m-1} = 0$. Then $|H_1| = |H_2| = |H_1 \cap H_2|$ and we get

$$\sum_{t=0}^{p^n-2} C_1(t)^m = \frac{1}{\varepsilon}(|K| - 2(\varepsilon+1)|H_1| + (\varepsilon+1)^2|H_1|),$$

which means that

$$\varepsilon^m + (-1)^m(\varepsilon - 1) = \frac{1}{\varepsilon}(\varepsilon^m - 2(\varepsilon+1)|H_1| + (\varepsilon+1)^2|H_1|),$$

therefore

$$\frac{1}{\varepsilon}|H_1|((\varepsilon+1)^2 - 2(\varepsilon+1)) = \varepsilon^m - \varepsilon^{m-1} + (-1)^m(\varepsilon - 1),$$

and so

$$|H_1| = \varepsilon \frac{\varepsilon^{m-1} + (-1)^m}{\varepsilon + 1}.$$

Hence

$$\sum_{t=0}^{p^n-2} C_d(t) C_d(t+\tau_1) \ldots C_d(t+\tau_{m-1}) =$$

$$= \frac{1}{\varepsilon}(|K| - 2(\varepsilon+1)|H_1| + (\varepsilon+1)^2|H_1 \cap H_2|)$$

$$= \varepsilon^{m-1} - 2(\varepsilon^{m-1} + (-1)^m) + (\varepsilon + 1)^2 \frac{|H_1 \cap H_2|}{\varepsilon}$$

$$= -(p^n - 1)^{m-1} + 2(-1)^{m-1} + p^{2n} a_m^{(\tau_1, \ldots, \tau_{m-1})}.$$

In particular when $\tau_1 = \tau_2 = \ldots = \tau_{m-1} = 0$, then Theorem 3.2 can be considered as an analogue to the Pless dentities [11] for the rth power sum of the weights of the codewords in the $(p^n - 1, 2n)$ code with parity check polynomial $h(x) = f_1(x) f_d(x)$, where $f_d(x)$ denotes the minimal polynomial of α^d.

Theorem 3.3. *We have*

$$\sum_{t=0}^{p^n-2} C_d(t-\tau) C_d(t) = \begin{cases} p^{2n} - p^n - 1 & \text{when } \tau \equiv 0 \pmod{p^n - 1}, \\ -p^n - 1 & \text{when } \tau \not\equiv 0 \pmod{p^n - 1}. \end{cases}$$

Proof. By Theorem 3.2 we have

$$\sum_{t=0}^{p^n-2} C_d(t) C_d(t+\tau) = -(p^n - 1) - 2 + a_2^{(\tau)} p^{2n},$$

where $a_2^{(\tau)}$ is the number of solutions of

$$\alpha^{-\tau} x_1 + 1 = 0, \tag{6}$$

$$x_1^d + 1 = 0, \tag{7}$$

with $x_1 \in \mathrm{GF}(p^n)^*$. From (6) and (7) we get $\alpha^{\tau d} = 1$, and therefore $\tau d \equiv 0 \pmod{p^n - 1}$ which means that $\tau \equiv 0 \pmod{p^n - 1}$ since g.c.d.$(d, p^n - 1) = 1$. Hence

$$a_2^{(\tau)} = \begin{cases} 1 & \text{when } \tau \equiv 0 \pmod{p^n - 1}, \\ 0 & \text{when } \tau \not\equiv 0 \pmod{p^n - 1}. \end{cases}$$

This proves the theorem.

Theorem 3.4. *We have*

$$\sum_{t=0}^{p^n-2} (C_d(t) + 1)^3 = p^{2n} b_3,$$

where b_3 is the number of common solutions of

$$x + y + 1 = 0, \tag{8}$$

$$x^d + y^d + 1 = 0, \tag{9}$$

with $x, y \in \mathrm{GF}(p^n)$.

Proof. By Theorems 3.1–3.3 we have

$$\sum_{t=0}^{p^n-2}(C_d(t)+1)^3 = \sum_{t=0}^{p^n-2} C_d(t)^3 + 3\sum_{t=0}^{p^n-2} C_d(t)^2 + 3\sum_{t=0}^{p^n-2} C_d(t) + \sum_{t=0}^{p^n-2} 1$$

$$= -(p^n-1)^3 + 2 + p^{2n}a_1^{(0,0,0)} + 3(p^{2n}-p^n-1) + 3 + p^n - 1$$

$$= p^{2n}(a_1^{(0,0,0)}+2).$$

Here $a_1^{(0,0,0)}$ is the number of solutions of

$$x_1 + x_2 + 1 = 0, \qquad x_1^d + x_2^d + 1 = 0,$$

where $x_1, x_2 \in \mathrm{GF}(p^n)^*$. Hence $a_1^{(0,0,0)} + 2$ is the number of common solutions of (8) and (9).

For later applications we give some results on Gaussian sums. For a more comprehensive treatment see Baumert and McEliece [1].

Let ψ_n be a primitive element of $\mathrm{GF}(p^n)^* = \mathrm{GF}(p^n) - \{0\}$. When $\alpha \in \mathrm{GF}(p^n)^*$ we define $\mathrm{ind}(\alpha)$ as the unique integer i with the properties $\alpha = \psi_n^i$ and $0 \le i < p^n - 1$. Let $\mathrm{Tr}_1^n(\alpha) = \sum_{i=0}^{n-1} \alpha^{p^i}$. Put $\zeta = \exp(2\pi i/p)$ and let $S_1^n(\alpha) = \zeta^{\mathrm{Tr}_1^n(\alpha)}$.

Lemma 3.5. *Let $N \mid (p^n - 1)$ and suppose $N \mid (p^r + 1)$ for some integer r. Suppose l is the least integer such that $N \mid (p^l + 1)$.*

(i) *Let N be even, $(p^l + 1)/N$ odd and $N/2l$ odd.*

$$\sum_{y \in \mathrm{GF}(p^n)} S_1^n(ay^N) = \begin{cases} p^n & \text{when } a = 0, \\ (-1)^{n/2l+1}(N-1)p^{n/2} & \text{when } a \in C_{N/2}, \\ (-1)^{n/2l}p^{n/2} & \text{when } a \notin C_{N/2}, \end{cases}$$

(ii) *In all other cases, then*

$$\sum_{y \in \mathrm{GF}(p^n)} S_1^n(ay^N) = \begin{cases} p^n & \text{when } a = 0, \\ (-1)^{n/2l+1}(N-1)p^{n/2} & \text{when } a \in C_0, \\ (-1)^{n/2l}p^{n/2} & \text{when } a \notin C_0, \end{cases}$$

where $C_j = \{\alpha \in \mathrm{GF}(p^n)^*: \mathrm{ind}(\alpha) \equiv j \pmod N\}$.

As a corollary we get:

Lemma 3.6. *Let n be even, then*

$$\sum_{y \in \mathrm{GF}(p^n)} S_1^n(ay^{p^{n/2}+1}) = \begin{cases} p^n & \text{when } a + a^{p^{n/2}} = 0, \\ -p^{n/2} & \text{when } a + a^{p^{n/2}} \neq 0. \end{cases}$$

Lemma 3.7. *We have that*

$$\sum_{y \in \mathrm{GF}(p^n)} S_1^n(y^2 a) = \begin{cases} p^n & \text{when } a = 0, \\ A & \text{when } a \text{ is a square in } \mathrm{GF}(p^n)^*, \\ -A & \text{when } a \text{ is a non-square in } \mathrm{GF}(p^n)^*, \end{cases}$$

where $A = (-1)^{n+1}((-1)^{(p-1)/2}p)^{n/2}$.

For a proof of Lemmas 3.5–3.7 see Baumert and McEliece [1].

A useful theorem for calculating $C_d(t)$ when $d-p^i$ divides p^n-1 is the following:

Theorem 3.8. *Let* g.c.d.$(d, p^n-1)=1$ *and suppose there exists an integer i such that* $(d-p^i) \mid (p^n-1)$ *and* $0 \le i < n$. *Choose N such that* $(d-p^i)N \equiv 0 \pmod{p^n-1}$. *Then*

$$C_d(t) = -1 + \frac{1}{N} \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(y^N(c\psi^j - \psi^{d-p^i})).$$

Proof. By definition,

$$C_d(t) = \sum_{j=0}^{p^n-2} \zeta^{a_j + a_{dj}}.$$

Since $\{a_j\}$ is a maximal linear sequence, it is known that we can write after a cyclic shift $a_j = \mathrm{Tr}_1^n(\psi^j)$ where ψ is a primitive element of $GF(p^n)$. Hence

$$C_d(t) = \sum_{j=0}^{p^n-2} \zeta^{\mathrm{Tr}_1^n(\psi^j - \psi^{dj})}$$

$$= \sum_{x \in GF(p^n)^*} S_1^n(cx - x^d), \quad \text{where } c = \psi^{-1}.$$

Let $C_j = \{\alpha \in GF(p^n)^*: \mathrm{ind}(\alpha) \equiv j \pmod N\}$. Put $x = \psi^j y^N$. When y runs through $GF(p^n)$, then x runs through C_j N times and is 0 once. If we let $j = 0, 1, \ldots, N-1$ respectively and each time let y run through $GF(p^n)$, then x will have run through each C_j N times and the zero element N times. Therefore we can write

$$N(C_d(t)+1) = \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(c(\psi^j y^N) - (\psi^j y^N)^d)$$

$$= \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(y^N c\psi^j - \psi^{dj} y^{dN}).$$

We have $dN \equiv p^i N \pmod{p^n-1}$ and therefore $y^{dN} = y^{p^i N}$ for $y \in GF(p^n)$. We also have $S_1^n(x) = S_1^n(x^p)$ for $x \in GF(p^n)$. Hence

$$N(C_d(t)+1) = \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(y^N c\psi^j - \psi^{dj} y^{p^i N})$$

$$= \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(y^N c\psi^j - \psi^{dp^{-i}j} y^N)$$

$$= \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(y^N(c\psi^j - \psi^{dp^{-i}j})).$$

Corollary 3.9. *Let* g.c.d.$(d, p^n-1)=1$ *and suppose there exists an integer i such*

that $(d-p^i) \mid (p^n-1)$ *and* $0 \le i < n$ *and an integer* $l > 0$ *such that* $N = (p^n-1)/(d-p^i) \mid (p^l+1)$. *Then* $C_d(t)$ *takes on at most* $2N+1$ *distinct values.*

Proof. According to Lemma 3.5 we know that

$$\sum_{y \in GF(p^n)} S_1^n(ay^N)$$

has only two distinct values when $a \neq 0$. According to Theorem 3.8 we have

$$N(C_d(t)+1) = \sum_{j=0}^{N-1} \sum_{y \in GF(p^n)} S_1^n(y^N(c\psi^j - \psi^{dp^{-j}})), \quad \text{where } c = \psi^{-t}.$$

Suppose we choose t such that $c = \psi^{-t} \neq \psi^{(dp^{-j})}$ for $j = 0, 1, \ldots, N-1$. Then $C_d(t)$ is a sum of N terms each of which can take on at most two values. Therefore $C_d(t)$ has at most $N+1$ possibilities when t is chosen as above.

Suppose we choose t such that $c = \psi^{-t} = \psi^{(dp^{-j})}$ for $j = 0, 1, \ldots, N-1$. Each of these choices of c gives one value for $C_d(t)$. When $t = 0, 1, \ldots, p^n-2$, then $C_d(t)$ takes on at most $2N+1$ values.

4. New results

We now give some general results about $C_d(t)$.

The following result is stated without proof for binary sequences by Golomb [4]. We give here a proof for sequences over $GF(p)$ for all prime numbers p.

Theorem 4.1. *When* $t = 0, 1, \ldots, p^n-2$, *then* $C_d(t)$ *has at least three values if and only if* $d \notin \{1, p, \ldots, p^{n-1}\}$.

Proof. If $d \in \{1, p, \ldots, p^{n-1}\}$, then we have only two values according to Theorem 3.1(g).

Suppose now $d \notin \{1, p, \ldots, p^{n-1}\}$. Then we get from Theorem 3.1(f) and Theorem 3.3:

$$\sum_{t=0}^{d} C_d(t) = 1, \tag{10}$$

$$\sum_{t=0}^{d} C_d(t)^2 = p^{2n} - p^n - 1. \tag{11}$$

Suppose $C_d(t)$ has two values x and y which occur r and s times respectively. We then have:

$$r + s = p^n - 1, \tag{12}$$

$$rx + sy = 1, \tag{13}$$

$$rx^2 + sy^2 = p^{2n} - p^n - 1. \tag{14}$$

Multiplying (12) by x and subtracting (13) gives (15). Multiplying (13) by x and subtracting (14) gives (16).

$$s(x-y)=(p^n-1)x-1, \tag{15}$$

$$s(x-y)y=x-p^{2n}+p^n+1. \tag{16}$$

Combining (15) and (16) we get

$$(p^n-1)xy-y=x-p^{2n}+p^n+1,$$

$$(p^n-1)^2xy-(p^n-1)(x+y)=(p^n-1)(-p^{2n}+p^n+1),$$

$$((p^n-1)x-1)((p^n-1)y-1)=p^{2n}(2-p^n),$$

$$(p^nx-(x+1))(p^ny-(y+1))=p^{2n}(2-p^n). \tag{17}$$

Here x, y belongs to $Q(\zeta)$ and they can be written uniquely as

$$x=\sum_{i=0}^{p-2}u_i\zeta^i,\quad y=\sum_{i=0}^{p-2}v_i\zeta^i,\qquad \text{where } u_i, v_i\in \mathbf{Z}.$$

Because of the definitions of x and y we must have $|u_i|\le p^n-1$ and $|v_i|\le p^n-1$ for $i=0,1,\ldots,p-2$.

In the cyclotomic field $Q(\zeta)$, the ring of integers are $\mathbf{Z}[\zeta]$ or $\mathbf{Z}[\pi]$ where $\pi=1-\zeta$. We also have $(p)=(\pi)^{p-1}$. Let $\pi^a\mid(x+1)$ mean that $x+1\in(\pi)^a-(\pi)^{a+1}$. Suppose $\pi^a\mid(x+1)$ and $\pi^b\mid(y+1)$. We must consider three cases.

Case 1: $a\ge n_1=(p-1)n$ (or by symmetry $b\ge n_1$). Then $x+1\in(\pi)^a\subset(\pi)^{(p-1)n}=(p)^n$ and therefore $x+1=p^nx_1$ with $x_1=c_0+c_1\zeta+\ldots+c_{p-2}\zeta^{p-2}\in\mathbf{Z}[\zeta]$. This gives $x=p^nc_0-1+p^n(c_1\zeta+\ldots+c_{p-2}\zeta^{p-2})$. This means that $c_0=1, c_1=\ldots=c_{p-2}=0$ because $|c_i|\le p^n-1$ for $i=0,1,\ldots,p-2$. Therefore $x=p^n-1$, but this can only happen when $\{a_{i+d}\}=\{a_d\}$ for some i, which means that $d\in\{1,p,\ldots,p^{n-1}\}$, a contradiction.

Case 2: $a<n_1$ and $b<n_1$. Then $x+1=\pi^ax_1$ with $x_1\notin(\pi)$, and $y+1=\pi^by_1$ with $y_1\notin(\pi)$, and $p^n=\pi^{n_1}z_1$ with $z\notin(\pi)$. We can now write (17) as

$$\pi^{a+b}(\pi^{n_1-a}z_1x-x_1)(\pi^{n_1-b}z_1y-y_1)=\pi^{2n_1}z_1^2(2-p^n).$$

The right-hand side belongs to $(\pi)^{2n_1}$ but the left-hand side belongs to $(\pi)^{a+b}-(\pi)^{a+b+1}$. This gives a contradiction because $a+b+1<2n_1$.

Case 3: $x+1=0$ (or by symmetry $y+1=0$). Then $x=-1$ and (17) gives $y=p^n-1$ which gives the same contradiction as in Case 1.

Theorem 4.2. *We have $C_d(t)\in\mathbf{Z}$ for $t=0,1,\ldots,p^n-2$ if and only if $d\equiv 1 \pmod{p-1}$.*

Proof. Let $C(x)=\sum_{t=0}^{p^n-2}C_d(t)x^t$, and let $\beta\ne 1$ be a complex (p^n-1)th root of unity. By inversion we get

$$C_d(t) = \frac{1}{p^n - 1} \sum_{l=0}^{p^n-2} C(\beta^l)\beta^{-lt}. \tag{18}$$

First we show that $C(\beta^l)$, which is an element of $Q(\zeta\beta)$, belongs to $Q(\beta)$ if and only if $d \equiv 1 \pmod{p-1}$.

Let α be a primitive root of $f(x)$. Then $\alpha^{(p^n-1)/(p-1)}$ is a primitive element of $GF(p)$. The elements of $Q(\beta)$ are exactly those elements in $Q(\zeta\beta)$ which are invariant under the $p-1$ automorphisms given by $\sigma_i : \zeta \to \zeta^{\alpha^{i(p^n-1)/(p-1)}}$ and $\sigma_i \mid Q(\beta) = id$ for $i = 0, 1, \ldots, p-2$. We have

$$\begin{aligned}
\sigma_i(C(\beta^l)) &= \sigma_i\left(\sum_{t=0}^{p^n-2} C_d(t)\beta^{lt}\right) \\
&= \sum_{t=0}^{p^n-2} \beta^{lt} \sum_{j=0}^{p^n-2} \zeta^{\alpha^{i(p^n-1)/(p-1)}\alpha^{j}\alpha^{td}} \\
&= \sum_{t=0}^{p^n-2} \beta^{lt} \sum_{j=0}^{p^n-2} \zeta^{\mathrm{Tr}^n(\alpha^{i(p^n-1)/(p-1)}\alpha^{j}\alpha^{td})}
\end{aligned}$$

Put $d_j = dj + i(p^n-1)/(p-1) \pmod{p^n-1}$. Then

$$\begin{aligned}
\sigma_i(C(\beta^l)) &= \sum_{t=0}^{p^n-2} \beta^{lt} \sum_{j=0}^{p^n-2} \zeta^{\mathrm{Tr}^n(\alpha^{i(p^n-1)/(p-1)}\alpha^{j}\alpha^{td})} \\
&= \sum_{t=0}^{p^n-2} \beta^{lt} \sum_{j=0}^{p^n-2} \zeta^{\mathrm{Tr}^n(\alpha^{(td^{-1}+i(p^n-1)/(p-1))}\alpha^{d_j})} \\
&= \sum_{t=0}^{p^n-2} \beta^{lt} C_d(t + i(d^{-1}-1)(p^n-1)/(p-1)).
\end{aligned}$$

Put $t_i = t + i(d^{-1}-1)(p^n-1)/(p-1) \pmod{p^n-1}$. Then

$$\begin{aligned}
\sigma_i(C(\beta^l)) &= \sum_{t_i=0}^{p^n-2} C_d(t_i)\beta^{l(t_i - i(d^{-1}-1)(p^n-1)/(p-1))} \\
&= \beta^{-i(d^{-1}-1)l(p^n-1)/(p-1)} C(\beta^l).
\end{aligned}$$

Hence $C(\beta^l)$ belongs to $Q(\beta)$ if and only if $d^{-1} \equiv 1 \pmod{p-1}$ which is if and only if $d \equiv 1 \pmod{p-1}$. We are now able to prove the theorem.

Suppose $C_d(t)$ is an integer for $t = 0, 1, \ldots, p^n-2$. Then $C(\beta^l)$ belongs to $Q(\beta)$ for $l = 0, 1, \ldots, p^n-2$ and therefore $d \equiv 1 \pmod{p-1}$.

Suppose $d \equiv 1 \pmod{p-1}$. Then $C(\beta^l)$ belongs to $Q(\beta)$ for $l = 0, 1, \ldots, p^n-2$. From (18) we see that

$$C_d(t) = \frac{1}{p^n-1} \sum_{l=0}^{p^n-2} C(\beta^l)\beta^{-lt}$$

belongs to $Q(\zeta) \cap Q(\beta) = Q$. But then $C_d(t)$ is a rational number which also is an algebraic integer. Therefore $C_d(t)$ is an integer for $t = 0, 1, \ldots, p^n-2$.

Theorem 4.3. *Let $m \geq 2$, then*

$$\sum_{t=0}^{p^n-2} (C_d(t)+1)(C_d(t+\tau_1)+1)\dots(C_d(t+\tau_{m-1})+1) \equiv 0 \pmod{p^{2n}}.$$

Proof. By Theorem 3.1(f) and Theorem 3.2 we have

$$\sum_{t=0}^{p^n-2} (C_d(t)+1)(C_d(t+\tau_1)+1)\dots(C_d(t+\tau_{m-1})+1) =$$

$$= \sum_{t=0}^{p^n-2} 1 + \sum_{t=0}^{p^n-2} C_d(t) + \dots + \sum_{t=0}^{p^n-2} C_d(t+\tau_{m-1}) + \dots + \sum_{t=0}^{p^n-2} C_d(t)\dots C_d(t+\tau_{m-1})$$

$$\equiv \varepsilon + \binom{m}{1}(-\varepsilon^0 + 2(-1)^0) + \dots + \binom{m}{m}(-\varepsilon^{m-1} + 2(-1)^{m-1})$$

$$= \varepsilon - \sum_{k=1}^{m} \binom{m}{k} \varepsilon^{k-1} + 2\sum_{k=1}^{m} (-1)^{k-1}$$

$$= \varepsilon - \frac{(\varepsilon+1)^m - 1}{\varepsilon} + 2\frac{(1-1)^m - 1}{(-1)}$$

$$\equiv (\varepsilon+1)^2 \frac{1-(\varepsilon+1)^{m-2}}{\varepsilon}$$

$$\equiv 0 \pmod{p^{2n}}, \quad \text{when } m \geq 2.$$

Note that Theorem 4.3 fails when $m = 1$. But we have

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

because of Theorem 3.1(f).

Theorem 4.4. *The polynomial*

$$R(x) = \prod_{t=0}^{p^n-2} (x - (C_d(t)+1))$$

has integral coefficients which, apart from the leading coefficient, are divisible by p.

Proof. Put $y_t = C_d(t)+1$. Form the polynomial $R(x) = \prod_{t=0}^{p^n-2}(x - y_t)$. Then $R(x) = x^{p^n-1} + b_{p^n-2}x^{p^n-2} + \dots + b_1 x + b_0$.

Theorem 3.1(f) and Theorem 4.3 give

$$S_m = \sum_{t=0}^{p^n-2} y_t^m \equiv 0 \pmod{p^n}$$

for all $m \geq 1$. Newton's identities give

$$S_1 + b_{p^n-2} = 0,$$

$$S_2 + b_{p^n-2}S_1 + 2b_{p^n-3} = 0,$$

$$\vdots$$

$$S_{p^n-1} + \dots + b_2 S_2 + b_1 S_1 + (p^n-1)b_0 = 0.$$

From this we conclude that all coefficients in $R(x)$, apart from the leading coefficient, are integers divisible by p.

Theorem 4.5. *We have* $C_d(t) \equiv -1 \pmod{\pi}$

Proof. Put $y_t = C_d(t) + 1$. Then $R(y_t) = 0$. But this means

$$y_t^{p^n-1} + b_{p^n-2} y_t^{p^n-2} + \ldots + b_1 y_t + b_0 = 0,$$

and since $b_i \equiv 0 \pmod{p}$ for $i = 0, 1, \ldots, p^n - 2$, we have $y_t^{p^n-1} \equiv 0 \pmod{p}$. Therefore $C_d(t) = y_t - 1 \equiv -1 \pmod{\pi}$.

Corollary 4.6. *If* $C_d(t) \in \mathbf{Z}$, *then* $C_d(t) \equiv -1 \pmod{p}$.

Proof. This follows from the fact that a rational integer which is divisible by π is also divisible by p.

The congruence given by Theorem 4.5 is the best possible because there exist d and t such that $C_d(t) \not\equiv -1 \pmod{\pi^2}$. The same remark is true for Corollary 4.6.

Usually when d is given we can find better congruences by using a theorem due to McEliece [9, p. 180].

For binary sequences it is possible to improve Theorem 4.5.

Theorem 4.7. *For binary sequences we have*

$$C_d(t) \equiv -1 \pmod{4},$$

$$C_d(t) \equiv -1 \pmod{8} \quad \textit{when } d \notin \{-1, -2, \ldots, -2^{n-1}\}.$$

Proof. For binary sequences we have a connection between the cross-correlation function and the Hamming weight of the codewords in the $(p^n - 1, 2n)$-code with check polynomial $h(x) = f_1(x) f_d(x)$ where $f_i(x)$ is the minimal polynomial of α^i and α is a primitive element of GF(2^n). We have that $\{a_{t+1} + a_{d_t}\}$ is a codeword in this code and $C_d(t) = 2^n - 1 - 2w(\{a_{t+1} + a_{d_t}\})$ where $w(\{u_t\})$ is the Hamming weight of $\{u_t\}$. According to Van Lint [14, p. 122] we get $w(\{a_{t+1} + a_{d_t}\}) \equiv 0 \pmod{4}$ unless $h(x)$ has a pair of zeros with product 1. Since g.c.d.$(d, 2^n - 1) = 1$ this happens only when $d \in \{-1, -2, \ldots, -2^{n-1}\}$. In all cases $w(\{a_{t+1} + a_{d_t}\}) \equiv 0 \pmod{2}$ because $h(1) \neq 0$.

We now find the values and the number of occurrences of each value in $C_d(t)$ for some new values of d.

As an application of Theorem 3.4 we will prove a conjecture due to Niho [10].

Theorem 4.8. *Let* $d = 2^m + 3$ *where* $n = 2m$, $m > 2$. *Then* $C_d(t)$ *has five values*:

(i) $3 \cdot 2^m$ *occurs* $\frac{1}{4}(2^{m-3}(2^m + (-1)^{m+1} + 1) - 2^{m-1})$ *times*,

(ii) 2^{m+1} *occurs* 2^{m-1} *times,*
(iii) 2^m *occurs* $2^{2m-1} - 2^{m-2}(2^m + (-1)^{m+1} + 1)$ *times,*
(iv) 0 *occurs* $\frac{1}{2}(2^m(2^m + (-1)^{m+1} + 1) + 2^{m-1} - 3)$ *times,*
(v) -2^m *occurs* $2^{2m-1} - 2^{m-3}(2^m + (-1)^{m+1} + 1) - 2^{m-1}$ *times.*

Proof. Niho [10] has proved that the values which occur in $C_d(t) + 1$ are $2^m(N-1)$ with $N = 0, 1, 2, 3, 4$. Suppose -2^m occurs t_1 times, 0 occurs t_2 times, 2^m occurs t_3 times, 2^{m+1} occurs t_4 times and $3 \cdot 2^m$ occurs t_5 times. Theorems 3.1–3.4 give

$$t_1 + t_2 + t_3 + t_4 + t_5 = 2^{2m} - 1, \tag{19}$$

$$-2^m t_1 + 2^m t_3 + 2^{m+1} t_4 + 3 \cdot 2^m t_5 = 2^{2m},$$

$$2^{2m} t_1 + 2^{2m} t_3 + 2^{2m+2} t_4 + 9 \cdot 2^{2m} t_5 = 2^{4m},$$

$$-2^{3m} t_1 + 2^{3m} t_3 + 2^{3m+3} t_4 + 27 \cdot 2^{3m} t_5 = 2^{4m} b_3,$$

where b_3 is the number of solutions of

$$x + y = 1, \tag{20}$$

$$x^{2^{m+3}} + y^{2^{m+3}} = 1. \tag{21}$$

Here Niho has found $t_4 = 2^{m-1}$. We next show that $b_3 = 2^m + (-1)^{m+1} + 1$. Suppose this is done. We then have four equations with four unknowns and by solving (19) we prove Theorem 4.8.

It remains to prove that $b_3 = 2^m + (-1)^{m+1} + 1$. From (20) and (21) we get $(x+y)^{2^{m+3}} = 1$. Therefore

$$x^{2^{m+3}} + x^{2^{m+2}}y + x^{2^{m+1}}y^2 + x^{2^m}y^3 + x^3y^{2^m} + x^2y^{2^{m+1}} + xy^{2^{m+2}} + y^{2^{m+3}} = 1,$$

$$x^{2^m}(x^2y + xy^2 + y^3) + y^{2^m}(y^2x + yx^2 + x^3) = 0,$$

$$x^{2^m}(x^2(1+x) + x(1+x)^2 + (1+x)^3) + (1+x)^{2^m}((1+x)^2x + (1+x)x^2 + x^3) = 0,$$

$$x^{2^m}(1+x^3) + (1+x^{2^m})(x + x^2 + x^3) = 0,$$

$$(x^{2^m} + x)(1 + x + x^2) = 0,$$

which means that b_3 is the number of solutions of

$$(x^{2^m} + x)(1 + x + x^2) = 0.$$

We note that $x^{2^m} + x = 0$ if and only if $x \in \mathrm{GF}(2^m)$ and $1 + x + x^2 = 0$ if and only if $x \in \mathrm{GF}(2^2) - \mathrm{GF}(2)$. We also have $\mathrm{GF}(2^2) \subset \mathrm{GF}(2^m)$ if and only if m is even. Therefore $b_3 = 2^m$ when m is even and $b_3 = 2^m + 2$ when m is odd, which is what we wanted to show.

Theorem 4.9. *Let p be an odd prime. Let $e = \mathrm{g.c.d.}(n, k)$. Let n/e be odd. If $d = \frac{1}{2}(p^k + 1)$ or $d = p^{2k} - p^k + 1$ where $d \not\equiv p^i \pmod{p^n - 1}$, then $C_d(t)$ has three values:*

(i) $-1+p^{(n+\epsilon)/2}$ *occurs* $\frac{1}{2}(p^{n-\epsilon}+p^{(n-\epsilon)/2})$ *times.*
(ii) -1 *occurs* $p^n-p^{n-\epsilon}-1$ *times.*
(iii) $-1+p^{(n+\epsilon)/2}$ *occurs* $\frac{1}{2}(p^{n-\epsilon}-p^{(n-\epsilon)/2})$ *times.*

Theorem 4.9 is a generalization of Theorem 2.4, since the condition n odd is replaced by $n/\text{g.c.d.}(n,k)$ odd. The proof of Theorem 4.9 is omitted because it is lengthy and only needs a few modifications of Trachtenberg's proof [13].

Theorem 4.10. *Let p be an odd prime and $p^n \equiv 1 \pmod 4$. Let $d=\frac{1}{2}(p^n-1)+p^i$ with $0 \le i < n$. Then* g.c.d.$(d, p^n-1)=1$ *and $C_d(t)$ has the following values:*
(i) -1 *occurs* $\frac{1}{4}(p^n-5)$ *times.*
(ii) $-1+(-1)^{n+1}((-1)^{(p-1)/2}p)^{n/2}$ *occurs* $\frac{1}{4}(p^n-1)$ *times.*
(iii) $-1+(-1)^n((-1)^{(p-1)/2}p)^{n/2}$ *occurs* $\frac{1}{4}(p^n-1)$ *times.*
(iv) $-1+\frac{1}{2}(p^n+(-1)^{n+1}((-1)^{(p-1)/2}p)^{n/2})$ *occurs* 1 *time.*
(v) $-1+\frac{1}{2}(p^n+(-1)^n((-1)^{(p-1)/2}p)^{n/2})$ *occurs* 1 *time.*

Proof. Since $p^n \equiv 1 \pmod 4$ we get g.c.d.$(d, p^n-1)=1$. Since $d-p^i=\frac{1}{2}(p^n-1) \mid p^n-1$, we can choose $N=2$ and get $(d-p^i)N \equiv 0 \pmod{p^n-1}$. By Theorem 3.8 we have

$$C_d(t)=-1+\frac{1}{2}\sum_{c=0}^{1}\sum_{y\in GF(p^n)} S_1^n(y^N(c\psi^i-\psi^{dp^{-i}})),$$

where ψ is a primitive element of $GF(p^n)$. Hence we can write

$$2(C_d(t)+1)=\sum_{y\in GF(p^n)} S_1^n(y^2(c-1))+\sum_{y\in GF(p^n)} S_1^n(y^2(c-\psi^{(p^n-1)/2})\psi)$$

$$=\sum_{y\in GF(p^n)} S_1^n(y^2(c-1))+\sum_{y\in GF(p^n)} S_1^n(y^2(c+1)\psi),$$

since $\psi^{(p^n-1)/2}=-1$.

By Lemma 3.7 we see that to find $2(C_d(t)+1)$ we must study the pair $(c-1,(c+1)\psi)$ and find how often the components are squares, non-squares or zero element in $GF(p^n)$.

When $c-1$ and $(c+1)\psi$ are both squares we get the contribution $2A$. When one is a square and the other is a non-square we get the contribution $A-A=0$.

Suppose $c-1=0$. Then $(c+1)\psi=2\psi$ and we get the contribution $p^n-\chi(2)A$ where χ is the quadratic character of $GF(p^n)^*$.

Suppose $c+1=0$. Then $c-1=-2$ and we get the contribution $p^n+\chi(-2)A$.

This proves that $2(C_d(t)+1)$ takes on at most the five values $2A, -2A, 0, p^n-A, p^n+A$. This means that $C_d(t)$ takes on at most the following values:

$$-1,\quad -1\pm((-1)^{(p-1)/2}p)^{n/2},\quad -1+\tfrac{1}{2}(p^n\pm(-1)^{n+1}((-1)^{(p-1)/2}p)^{n/2}).$$

It remains to find how often $C_d(t)$ takes on each of these values. Theorem 3.1(f) and Theorem 3.3 give

$$\sum_{t=0}^{p^n-2} (C_d(t)+1) = p^n, \qquad \sum_{t=0}^{p^n-2} (C_d(t)+1)^2 = p^{2n}.$$

Suppose -1 occurs t_1 times, $-1+A$ occurs t_2 times, $-1-A$ occurs t_3 times. We know that $-1+\frac{1}{2}(p^n-\chi(2)A)$ and $-1+\frac{1}{2}(p^n+\chi(-2)A)$ occur one time each when $c=1$ and $c=-1$ respectively. Since $p^n \equiv 1 \pmod 4$, we have $\chi(-1) = (-1)^{(p^n-1)/2} = 1$ and therefore $-\chi(2) \neq \chi(-2)$. This discussion gives us three equations:

$$t_1 + t_2 + t_3 = p^n - 1 - 2 = p^n - 3,$$

$$At_2 - At_3 = p^n - \tfrac{1}{2}(p^n - A) - \tfrac{1}{2}(p^n + A) = 0,$$

$$A^2t_2 + A^2t_3 = p^{2n} - \tfrac{1}{4}(p^n - A)^2 - \tfrac{1}{4}(p^n - A)^2 = \tfrac{1}{2}p^{2n} - \tfrac{1}{2}A^2.$$

By inserting $A = (-1)^{n+1}((-1)^{(p-1)/2}p)^{n/2}$ we get $t_1 = \frac{1}{2}(p^n-1)$, $t_2 = t_3 = \frac{1}{4}(p^n-1)$ which proves Theorem 4.10.

We note that when n is odd and $p > 3$, then $d \not\equiv 1 \pmod{p-1}$ and therefore the values of $C_d(t)$, when $d = \frac{1}{2}(p^n-1)+p^i$ with $0 \le i < n$, are not always integers because of Theorem 4.2.

Theorem 4.11. *Suppose* $p \equiv 2 \pmod 3$ *and* $n \equiv 0 \pmod 2$. *Let* $d = \frac{1}{2}(p^n-1)+p^i$ *where* $0 \le i < n$ *and* $f = \frac{1}{2}p^{-i}(p^i-1) \not\equiv 2 \pmod 3$. *Then* g.c.d.$(d, p^n-1) = 1$ *and* $C_d(t)$ *takes on the following values. When* $f \equiv 0 \pmod 3$, *then*:

(i) -1 *occurs* $\frac{1}{6}(4p^n + 2(-1)^{n/2+1}p^{n/2} - 29)$ *times.*
(ii) $-1+(-1)^{n/2+1}p^{n/2}$ *occurs* $\frac{1}{6}(2p^n + 2(-1)^{n/2}p^{n/2} - 4)$ *times.*
(iii) $-1+(-1)^{n/2}p^{n/2}$ *occurs* $\frac{1}{27}(8p^n + 2(-1)^{n/2}p^{n/2} - 10)$ *times.*
(iv) $-1+2(-1)^{n/2+1}p^{n/2}$ *occurs* $\frac{1}{27}(p^n + 2(-1)^{n/2+1}p^{n/2} + 1)$ *times.*
(v) $-1+\frac{1}{3}(p^n + 2(-1)^{n/2}p^{n/2})$ *occurs* 1 *time.*
(vi) $-1+\frac{1}{3}(p^n + (-1)^{n/2+1}p^{n/2})$ *occurs* 2 *times.*

When $f \equiv 1 \pmod 3$, *then*:

(i) -1 *occurs* $\frac{1}{6}(4p^n + 2(-1)^{n/2+1}p^{n/2} - 20)$ *times.*
(ii) $-1+(-1)^{n/2+1}p^{n/2}$ *occurs* $\frac{1}{6}(2p^n + 2(-1)^{n/2}p^{n/2} - 4)$ *times.*
(iii) $-1+(-1)^{n/2}p^{n/2}$ *occurs* $\frac{1}{27}(8p^n + 2(-1)^{n/2}p^{n/2} - 28)$ *times.*
(iv) $-1+2(-1)^{n/2+1}p^{n/2}$ *occurs* $\frac{1}{27}(p^n + 2(-1)^{n/2+1}p^{n/2} - 8)$ *times.*
(v) $-1+\frac{1}{3}(p^n + 2(-1)^{n/2}p^{n/2})$ *occurs* 2 *times.*
(vi) $-1+\frac{1}{3}(p^n + 4(-1)^{n/2+1}p^{n/2})$ *occurs* 1 *time.*

Proof. We have

$$\text{g.c.d.}(\tfrac{1}{2}(p^n-1)+p^i, p^n-1) = \text{g.c.d.}(\tfrac{1}{2}p^{-i}(p^n-1)+1, p^n-1) = 1$$

since $\frac{1}{2}p^{-i}(p^n-1) \not\equiv 2 \pmod 3$. We have $d - p^i = \frac{1}{2}(p^n-1)$. Choose $N = 3$. Then $(d-p^i)N \equiv 0 \pmod{p^n-1}$ and we can apply Theorem 3.8 from which we get

$$3(C_d(t)+1) = \tag{22}$$

$$= \sum_{y\in GF(p^n)} S_1^n(y^3(c-1)) + \sum_{y\in GF(p^n)} S_1^n(y^3(c-\beta)\psi) + \sum_{y\in GF(p^n)} S_1^n(y^3(c-\beta^2)\psi^2),$$

where $\beta = \psi^{(p^n-1)/3}$.

Since $p \equiv 2 \pmod 3$ then $3 \mid (p+1)$ and we can apply Lemma 3.5(ii) which then says that

$$\sum_{y\in GF(p^n)} S_1^n(ay^3) = \begin{cases} p^n & \text{when } a = 0, \\ A & \text{when } a \in C_0, \\ -\frac{1}{2}A & \text{when } a \notin C_0, \end{cases} \tag{23}$$

where $A = (-1)^{n/2+1}2p^{n/2}$ and C_0 is the set of cubes in $GF(p^n)^*$.

Let $c \notin \{1, \beta, \beta^2\}$. According to (22) and (23), $3(C_d(t)+1)$ can take on at most the four values $3A, \frac{3}{2}A, 0, -\frac{3}{2}A$.

Let $c \in \{1, \beta, \beta^2\}$. We must study the triplet $(c-1, (c-\beta)\psi, (c-\beta^2)\psi^2)$ and find how often the components are zero, a cube or a non-cube in $GF(p^n)^*$.

$$\begin{aligned} c = 1 \quad &\text{gives} \quad (0, (1-\beta)\psi, (1-\beta^2)\psi^2), \\ c = \beta \quad &\text{gives} \quad (\beta-1, 0, (\beta-\beta^2)\psi^2), \\ c = \beta^2 \quad &\text{gives} \quad (\beta^2-1, (\beta^2-\beta)\psi, 0). \end{aligned} \tag{24}$$

We have $\beta^3 = 1$ since $\beta = \psi^{(p^n-1)/3}$. Therefore $1+\beta+\beta^2 = 0$ and $\beta^2 = -(1+\beta)$. Since $-1 = \psi^{(p^n-1)/2} \in C_0$ then $2f \equiv \text{ind}(1+\beta) \pmod 3$. Put $r = \text{ind}(1-\beta)$ and $\text{ind}(0) = -\infty$. The indices of the three triplets in (24) then become

$$\begin{aligned} &(-\infty, r+1, 2f+r+2), \\ &(r, -\infty, f+r+2), \\ &(r+2f, f+r+1, -\infty). \end{aligned} \tag{25}$$

According to (22), (23) and (25) we get, when $f \equiv 0 \pmod 3$,

$$3(C_d(t)+1) = \begin{cases} p^n - A, & 1 \text{ time}, \\ p^n + \frac{1}{2}A, & 2 \text{ times}. \end{cases}$$

When $f \equiv 1 \pmod 3$, then

$$3(C_d(t)+1) = \begin{cases} p^n - A, & 2 \text{ times}, \\ p^n + 2A, & 1 \text{ time}. \end{cases}$$

This proves that $C_d(t)$ takes on the following six values when $f \equiv 0 \pmod 3$:

$$-1, \quad -1+\tfrac{3}{2}A, \quad -1-\tfrac{3}{2}A, \quad -1+A, \quad -1+\tfrac{1}{3}(p^n-A), \quad -1+\tfrac{1}{3}(p^n+\tfrac{1}{2}A);$$

and the following six values when $f \equiv 1 \pmod 3$:

$$-1, \quad -1+\tfrac{3}{2}A, \quad -1-\tfrac{3}{2}A, \quad -1+A, \quad -1+\tfrac{1}{3}(p^n-A), \quad -1+\tfrac{1}{3}(p^n+2A).$$

By inserting $A = (-1)^{n/2+1}2p^{n/2}$ we find that these are the values in Theorem 4.11. It remains to find how often $C_d(t)$ takes on each of these values.

Suppose -1 occurs t_1 times, $-1+\frac{1}{2}A$ occurs t_2 times, $-1-\frac{1}{2}A$ occurs t_3 times, $-1+A$ occurs t_4 times, $-1+\frac{1}{3}(p^n-A)$ occurs t_5 times, $-1+\frac{1}{3}(p^n+\frac{1}{2}A)$ occurs t_6 times and $-1+\frac{1}{3}(p^n+2A)$ occurs t_7 times. We then get from Theorems 3.1–3.4,

$$t_1+t_2+t_3+t_4+t_5+t_6+t_7=p^n-1,$$

$$\tfrac{1}{2}At_2-\tfrac{1}{2}At_3+At_4+\tfrac{1}{3}(p^n-A)t_5+\tfrac{1}{3}(p^n+\tfrac{1}{2}A)t_6+\tfrac{1}{3}(p^n+2A)t_7=p^n,$$

$$\tfrac{1}{4}A^2t_2-\tfrac{1}{4}A^2t_3+A^2t_4+\tfrac{1}{9}(p^n-A)^2t_5+\tfrac{1}{9}(p^n+\tfrac{1}{2}A)^2t_6+\tfrac{1}{9}(p^n+2A)^2t_7=p^{2n},$$

$$\tfrac{1}{8}A^3t_2-\tfrac{1}{8}A^3t_3+A^3t_4+\tfrac{1}{27}(p^n-A)^3t_5+\tfrac{1}{27}(p^n+\tfrac{1}{2}A)^3t_6+\tfrac{1}{27}(p^n+2A)^3t_7=p^{2n}b_3,$$

where b_3 is the number of common solutions of

$$X+Y+1=0,$$

$$X^{(p^n-1)/3+p^i}+Y^{(p^n-1)/3+p^i}+1=0 \quad \text{with } X, Y\in \mathrm{GF}(p^n).$$

From previous discussions we know A, t_5, t_6, t_7. Lemma 4.12 below gives us b_3. We therefore have four equations with four unknowns. By straightforward calculations we get the result of Theorem 4.11.

Lemma 4.12. *Suppose* $p\equiv 2 \pmod 3$ *and* $n\equiv 0 \pmod 2$. *Let* $d=\frac{1}{3}(p^n-1)+p^i$ *where* $0\le i<n$ *and* $f=\frac{1}{3}p^{-i}(p^n-1)\not\equiv 2 \pmod 3$. *Let* b_3 *be the number of common solutions of*

$$X+Y+1=0, \tag{26}$$

$$X^d+Y^d+1=0 \quad \textit{with } X, Y\in \mathrm{GF}(p^n),$$

then

$$b_3=\begin{cases}\frac{1}{9}(p^n+2(-1)^{n/2+1}p^{n/2}+10) & \textit{when } f\equiv 0 \pmod 3,\\ \frac{1}{9}(p^n+2(-1)^{n/2+1}p^{n/2}+28) & \textit{when } f\equiv 1 \pmod 3.\end{cases}$$

Proof. Let ψ be a primitive element of $\mathrm{GF}(p^n)$ and let $\beta=\psi^{p^{-i}(p^n-1)/3}$. Note that $\beta^3=1$. Put $x=\psi^l$ and $y=\psi^m$ where $0\le l, m<p^n-1$. Then (26) can be written

$$\psi^l+\psi^m+1=0, \qquad \beta^l\psi^l+\beta^m\psi^m+1=0. \tag{27}$$

Let $l\equiv r \pmod 3$ and $m\equiv s \pmod 3$ when $0\le r, s<3$. We divide the solutions of (27) in 9 classes according to the pair (r,s). Since $\beta^l=\beta^r$ and $\beta^m=\beta^s$, it is straightforward to verify that the six classes $(0,1), (1,0), (0,2), (2,0), (1,1)$ and $(2,2)$ contain no solution to (27).

Suppose next that $(r,s)=(1,2)$. Then (27) becomes

$$\psi^l+\psi^m+1=0, \qquad \beta\psi^l+\beta^2\psi^m+1=0, \tag{28}$$

which gives $(\beta-1)\psi^l+(\beta^2-1)\psi^m=0$ and therefore $\psi^l=-(\beta+1)\psi^m=\beta^2\psi^m$. A necessary condition for (28) to have a solution is therefore $l\equiv 2f+m \pmod 3$. When $f\equiv 0 \pmod 3$ we have no solution to (28). When $f\equiv 1 \pmod 3$ we have the only solution $\psi^l=\beta$ and $\psi^m=\beta^2$. Because of the symmetry we get the same number of solutions in the class (2, 1).

Suppose at last that $(r,s)=(0,0)$. Then (27) reduces to the single equation $\psi^l+1=-\psi^m$. Since $-1\in C_0$ this is the cyclotomic number $(0,0)_3$ which according to Storer [12, p. 35] is given by $(0,0)_3=\frac{1}{6}(p^n-2(-1)^{n/2}p^{n/2}-8)$. From this discussion it follows that the number of solutions in these 9 classes is $(0,0)_3$ when $f\equiv 0 \pmod 3$ and $(0,0)_3+2$ when $f\equiv 1 \pmod 3$. In addition we must add the two solutions $X=0$, $Y=-1$ and $X=-1$, $Y=0$.

As another application of Theorem 3.8 we will prove a generalization of Theorem 2.2 when p is odd. The method of Niho [10] can not be applied for $p>2$ without modifications. By Theorem 3.8 we can prove:

Theorem 4.13. *Suppose $n\equiv 0 \pmod 2$ and $p^{n/2}\not\equiv 2 \pmod 3$. Let $d=2p^{n/2}-1$. Then* g.c.d.$(d,p^n-1)=1$ *and $C_d(t)$ takes on the following values:*

(i) $-1-p^{n/2}$ *occurs* $\frac{1}{3}(p^n-p^{n/2})$ *times,*

(ii) -1 *occurs* $\frac{1}{3}(p^n-p^{n/2}-2)$ *times,*

(iii) $-1+p^{n/2}$ *occurs* $p^{n/2}$ *times,*

(iv) $-1+2p^{n/2}$ *occurs* $\frac{1}{3}(p^n-p^{n/2})$ *times.*

Proof. For $p=2$ this is due to Niho [10]. Let p be odd and $n=2m$. Then

$$\begin{aligned}\text{g.c.d.}(2p^m-1,p^{2m}-1)&=\text{g.c.d.}(2(p^m-1)+1,p^m+1)\\&=\text{g.c.d.}(3,p^m+1)\\&=1,\end{aligned}$$

since $p^m\not\equiv 2 \pmod 3$.

We have $(d-1)=2(p^m-1)$. Choose $N=p^m+1$. Then $(d-1)N\equiv 0 \pmod{p^n-1}$. According to Theorem 3.8 we have

$$(p^m+1)(C_d(t)+1)=\sum_{j=0}^{p^m}\sum_{c\in GF(p^n)}S_1^n(y^{p^m+1}(c\psi^l-\psi^{dj})). \tag{29}$$

Let $K(c)$ denote the number of solutions of

$$(c\psi^l-\psi^{dj})^{p^m}+c\psi^l-\psi^{dj}=0 \quad \text{when } 0\le j\le p^m. \tag{30}$$

According to Lemma 3.6 we get from (29),

$$\begin{aligned}(p^m+1)(C_d(t)+1)&=p^{2m}K(c)+(-p^m)(p^m+1-K(c))\\&=-(p^{2m}+p^m)+(p^{2m}+p^m)K(c),\end{aligned}$$

and therefore

$$C_d(t) = -1 + p^m(K(c) - 1).$$

Next we want to show that $K(c) = 0, 1, 2$ or 3.

Suppose $p^m \equiv -1 \pmod 4$. Then g.c.d. $(\frac{1}{2}(p^m - 1), 2(p^m + 1)) = 1$ and therefore the primitive element ψ of $GF(p^{2m})$ can be written $\psi = \alpha\beta$ with $\alpha^{(p^m-1)/2} = 1$ and $\beta^{2(p^m+1)} = 1$.

We have

$$d = 2p^m - 1 \equiv \begin{cases} 1 \pmod{\frac{1}{2}(p^m - 1)}, \\ -3 \pmod{2(p^m + 1)}. \end{cases}$$

Put $\psi = \alpha\beta$ in (30) and note that $\alpha^{p^m} = \alpha$ and $\beta^{p^m} = -\beta^{-1}$. Then $K(c)$ is the number of solutions of

$$c^{p^m}\alpha^j(\beta^{p^m})^j - \alpha^j(\beta^{-3p^m})^j + c\alpha^j\beta^j - \alpha^j\beta^{-3j} = 0, \qquad 0 \le j \le p^m,$$

$$\alpha^j(c^{p^m}(-1)^j\beta^{-j} - (-1)^j\beta^{3j} + c\beta^j - \beta^{-3j}) = 0, \qquad 0 \le j \le p^m.$$

Multiplying by $-\beta^{3j}$ we get

$$((-1)^j\beta^{2j})^3 - c((-1)^j\beta^{2j})^2 - c^{p^m}((-1)^j\beta^{2j}) + 1 = 0, \qquad 0 \le j \le p^m.$$

As an equation of degree 3 this has at most three solutions for $(-1)^j\beta^{2j}$. Each of these solutions gives at most one value of j such that $0 \le j \le p^m$.

Suppose

$$(-1)^{j_1}\beta^{2j_1} = (-1)^{j_2}\beta^{2j_2},$$

then

$$\beta^{2j_1+(p^m+1)j_1} = \beta^{2j_2+(p^m+1)j_2},$$

$$2j_1 + (p^m + 1)j_1 \equiv 2j_2 + (p^m + 1)j_2 \pmod{2(p^m + 1)},$$

and so

$$(j_1 - j_2)(\tfrac{1}{2}(p^m + 3)) \equiv 0 \pmod{p^m + 1},$$

which means

$$j_1 \equiv j_2 \pmod{p^m + 1}.$$

Suppose $p^m \equiv 1 \pmod 4$. Then g.c.d. $(2(p^m - 1), \frac{1}{2}(p^m + 1)) = 1$ and therefore the primitive element of $GF(p^{2m})$ can be written $\psi = \alpha\beta$ with $\alpha^{2(p^m-1)} = 1$ and $\beta^{(p^m+1)/2} = 1$.

We have

$$d = 2p^m - 1 \equiv \begin{cases} 1 \pmod{2(p^m - 1)}, \\ -3 \pmod{\frac{1}{2}(p^m + 1)}. \end{cases}$$

Put $\psi = \alpha\beta$ in (30) and note that $\alpha^{p^m} = -\alpha$ and $\beta^{p^m} = \beta^{-1}$. Then $K(c)$ is the number of solutions of

$$c^{p^m}(-\alpha)^j\beta^{-j} - (-\alpha)^j\beta^{3j} + c\alpha^j\beta^j - \alpha^j\beta^{-3j} = 0, \qquad 0 \le j \le p^m,$$

$$\alpha^j(c^{p^m}(-1)^j\beta^{-j} - (-1)^j\beta^{3j} + c\beta^j - \beta^{-3j}) = 0, \qquad 0 \le j \le p^m.$$

Each of these solutions gives at most one value of j such that $0 \le j \le p^m$. Suppose namely that $(-1)^{j_1}\beta^{2j_1} = (-1)^{j_2}\beta^{2j_2}$. Then since -1 is not a power of β we get $j_1 \equiv j_2 \pmod 2$. Therefore we get $2j_1 \equiv 2j_2 \pmod{\frac{1}{2}(p^m+1)}$ which means $j_1 \equiv j_2 \pmod{\frac{1}{2}(p^m+1)}$ since $\frac{1}{2}(p^m+1)$ is odd. But then $j_1 \equiv j_2 \pmod{p^m+1}$, and it follows that (30) has at most three solutions.

It remains to find how often $C_d(t)$ takes on each of its four possible values. Suppose $-1-p^m$ occurs t_1 times, -1 occurs t_2 times, $-1+p^m$ occurs t_3 times and $-1+2p^m$ occurs t_4 times. Theorems 3.1–3.4 give us the four equations

$$t_1 + t_2 + t_3 + t_4 = p^{2m} - 1,$$

$$-p^m t_1 + p^m t_3 + 2p^m t_4 = p^{2m},$$

$$p^{2m} t_1 + p^{2m} t_3 + 4p^{2m} t_4 = p^{4m},$$

$$-p^{3m} t_1 + p^{3m} t_3 + 8p^{3m} t_4 = p^{4m} \cdot b_3,$$

where b_3 is the number of common solutions of

$$X + Y + 1 = 0,$$

$$X^{2p^m+1} + Y^{2p^m+1} + 1 = 0 \quad \text{with } X, Y \in \mathrm{GF}(p^{2m}).$$

The next lemma gives us $b_3 = p^m$. We therefore have four equations with four unknowns. By straightforward calculations we get Theorem 4.13.

Lemma 4.14. *The number of common solutions of*

$$X + Y + 1 = 0, \tag{31}$$

$$X^{2p^m+1} + Y^{2p^m+1} + 1 = 0 \quad \textit{with } X, Y \in \mathrm{GF}(p^{2m}) \tag{32}$$

is $b_3 = p^m$.

Proof. The number of common solutions of (31) and (32) is the number of solutions of

$$X^{2p^m+1} + (-X-1)^{2p^m+1} + 1 = 0,$$

$$X^{2p^m}(-X-1) + (-X-1)^{2p^m}X + (-X-1)X = 0,$$

$$-X^{2p^m+1} - X^{2p^m} + X^{2p^m+1} + 2X^{p^m+1} + X - X^2 - X = 0,$$

$$-X^2(X^{p^m+1}-1)^2 = 0,$$

which have p^m solutions.

Table 1. $p = 3$.

n	d	Number of occurrences (values)											
2	5	2	(−4)	2	(−1)	3	(2)	1	(5)				
3	5	3	(−10)	17	(−1)	6	(8)						
4	7	4	(−19)	18	(−10)	28	(−1)	26	(8)	3	(17)	1	(26)
	11	24	(−10)	35	(−1)	9	(8)	12	(17)				
	13	4	(−19)	17	(−10)	32	(−1)	20	(8)	7	(17)		
	41	20	(−10)	38	(−1)	20	(8)	1	(35)	1	(44)		
5	5	36	(−28)	161	(−1)	45	(26)						
	7	36	(−28)	161	(−1)	45	(26)						
	17	36	(−28)	161	(−1)	45	(26)						
	43	36	(−28)	161	(−1)	45	(26)						
6	11	54	(−55)	108	(−28)	395	(−1)	108	(26)	54	(53)	9	(80)
	19	54	(−55)	108	(−28)	395	(−1)	108	(26)	54	(53)	9	(80)
	29	234	(−28)	350	(−1)	27	(26)	117	(53)				
	41	36	(−82)	647	(−1)	45	(80)						
	79	254	(−28)	275	(−1)	127	(26)	67	(53)	5	(107)		
	107	246	(−28)	284	(−1)	144	(26)	42	(53)	3	(80)	9	(107)
	113	246	(−28)	284	(−1)	144	(26)	42	(53)	3	(80)	9	(107)
	365	182	(−28)	362	(−1)	182	(26)	1	(350)	1	(377)		
7	5	351	(−82)	1457	(−1)	378	(80)						
	7	351	(−82)	1457	(−1)	378	(80)						
	11	351	(−82)	1457	(−1)	378	(80)						
	41	351	(−82)	1457	(−1)	378	(80)						
	53	351	(−82)	1457	(−1)	378	(80)						
	61	351	(−82)	1457	(−1)	378	(80)						
	107	351	(−82)	1457	(−1)	378	(80)						
	365	351	(−82)	1457	(−1)	378	(80)						

Table 2. $p = 5$.

n	d	Number of occurrences (values)											
2	13	6	(−6)	10	(−1)	6	(4)	1	(9)	1	(14)		
3	13	10	(−26)	99	(−1)	15	(24)						
4	29	216	(−26)	238	(−1)	109	(24)	54	(49)	4	(74)	3	(99)
	49	200	(−26)	299	(−1)	25	(24)	100	(49)				
	53	216	(−26)	238	(−1)	109	(24)	54	(49)	4	(74)	3	(99)
	97	216	(−26)	236	(−1)	117	(24)	42	(49)	12	(74)	1	(99)
	121	216	(−26)	237	(−1)	113	(24)	48	(49)	8	(74)	2	(99)
	209	21	(−51)	144	(−26)	270	(−1)	186	(24)	1	(174)	2	(224)
	313	156	(−26)	310	(−1)	156	(24)	1	(299)	1	(324)		
5	13	300	(−126)	2499	(−1)	325	(124)						
	21	300	(−126)	2499	(−1)	325	(124)						
	313	300	(−126)	2499	(−1)	325	(124)						

5. Two conjectures

There exist many unsolved problems concerning the cross-correlation function. Most of the conjectures state that some specific choice of d gives few values. Here we will point out two conjectures of more global nature.

Conjecture 5.1. *When $d \equiv 1 \pmod{p-1}$ then -1 is one of the values $C_d(t)$ takes on.*

Conjecture 5.2. *When $n = 2^r$ and $d \notin \{1, p, \ldots, p^{n-1}\}$ then $C_d(t)$ takes on at least four values.*

Table 3. $p = 7$.

n	d	Number of occurrences (values)								
2	13	14	(−8)	20	(−1)	7	(6)	7 (13)		
	25	12	(−8)	22	(−1)	12	(6)	1 (20)	1 (27)	
3	25	21	(−50)	293	(−1)	28	(48)			
4	43	252	(−99)	294	(−50)	1048	(−1)	798 (48)	7 (293)	1 (342)
	97	784	(−50)	1175	(−1)	49	(48)	392 (97)		
	337	852	(−50)	910	(−1)	429	(48)	162 (97)	40 (146)	7 (195)
	433	852	(−50)	915	(−1)	409	(48)	192 (97)	20 (146)	12 (195)
	439	856	(−50)	898	(−1)	437	(48)	170 (97)	28 (146)	11 (195)
	1201	600	(−50)	1198	(−1)	600	(48)	1 (1175)	1 (1224)	

The Tables 1, 2 and 3 give the values and the number of occurrences of each value of $C_d(t)$ whenever $C_d(t)$ has less than seven values and when $d \equiv 1 \pmod{p-1}$ in the following cases.

p	n					
3	2	3	4	5	6	7
5	2	3	4	5		
7	2	3	4			

We let $10(-1)$ mean that -1 occurs 10 times.

For $p = 2$ the reader is referred to Niho [10].

References

[1] L.D. Baumert and R.J. McEliece, Weight of irreducible cyclic codes, Information and Control 20 (1972) 158–175.
[2] L. Carlitz and S. Uchiyama, Bounds for exponential sums, Duke Math. J. 24 (1957) 37–41.
[3] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE Trans. Information Theory 14 (1967) 154–156.
[4] S.W. Golomb, Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences, Information Sci. 1 (1968) 87–109.
[5] T. Kasami, Weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes, Information and Control 18 (1971) 369–394.
[6] T. Kasami, S. Lin and W.W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, Information and Control 11 (1968) 475–496.
[7] H.E. Mattson and G. Solomon, A new treatment of Bose–Chaudhuri codes, J. SIAM 9 (1961) 654–669.
[8] R.J. McEliece and H. Rumsey Jr., Euler products, cyclotomy, and coding, J. Number Theory 4 (1972) 302–311.
[9] R.J. McEliece, Weight congruences for p-ary cyclic codes, Discrete Math. 3 (1972) 177–192
[10] Y. Niho, Multi-valued cross-correlation function between two maximal linear recursive sequences, Ph.D. Dissertation, University of Southern California, Los Angeles, CA (1972).
[11] V. Pless, Power moment identities on weight distributions in error-correcting codes, Information and Control 6 (1963) 147–152.
[12] T. Storer, Cyclotomy and Difference Sets (Markham, Chicago, 1967).
[13] H.M. Trachtenberg, On the cross-correlation functions of maximal linear sequences, Ph.D. Dissertation, University of Southern California, Los Angeles, CA (1970).
[14] J.H. Van Lint, Coding Theory (Springer, Berlin, 1971).