New Sets of Optimal p-ary Low-Correlation Zone Sequences

Ji-Woong Jang, Jong-Seon No, *Member, IEEE*,
Habong Chung, *Member, IEEE*, and Xiaohu Tang, *Member, IEEE*

***Abstract*—In this correspondence, three methods of constructing low-correlation zone (LCZ) sequences are proposed. In the first method, we constructed binary LCZ sequence sets of period 2^n-1 using the Legendre sequences of period 2^m-1 as a column sequence when $m|n$. In the second method, we devise a column sequence set of length $2^{m+1}-1$ from a binary sequence of period 2^m-1 having ideal autocorrelation property and this column sequence set is used to construct binary LCZ sequence sets of period 2^n-1 when $(m+1)|n$. In the third method, p-ary LCZ sequence sets are constructed by adopting p-ary sequence of period p^m-1 with ideal autocorrelation for integers n and m such that $m|n$ as a column sequence. The second and third methods give us the optimal sets with respect to the bound by Tang, Fan, and Matsufuji. Finally, a construction method of $p^n \times p^n$ p-ary Hadamard matrices from optimal LCZ sequence sets is proposed.**

***Index Terms*—p-ary sequences, binary sequences, Legendre sequences, low-correlation zone (LCZ) sequences, sequences, unified sequences.**

I. Introduction

Unlike the conventional code-division multiple-access (CDMA) systems, in the quasi-synchronous CDMA system [1] where maintaining synchronization within a few chips is feasible even in the reverse link due to the relatively small transmission delay, the most important property of the sequences used for reducing multiple-access interference (MAI) is low-correlation property around the origin [2]. Long, Zhang, and Hu [2] proposed the sequence set that has low-correlation value around the origin, which can be used as a spreading sequence in the quasi-synchronous CDMA system. The sequence set with this property is called low-correlation zone (LCZ) sequence. They also have shown that an LCZ sequence set has better performance than other well-known sequence sets with optimal correlation property [2]. For a prime p, Tang and Fan [3] proposed p-ary LCZ sequence sets by extending the alphabet size of each sequence in Long's work [2]. And they also proposed a construction method of p-ary LCZ sequence sets by using interleaved sequences [4]. Kim, Jang, No, and Chung proposed a new construction method of quaternary LCZ sequence sets by using binary sequence of the same period with ideal autocorrelation and they also calculated the correlation distributions of their sequence sets constructed from m-sequence and GMW sequence [5]. Their quaternary LCZ sequence set is optimal with respect to the bound by Tang, Fan, and Matsufuji [6]. But for a prime p, no optimal set of p-ary LCZ sequence set has been reported yet.

Manuscript received March 28, 2005; revised September 19, 2006. This work was supported in part by the Korean Ministry of Information and Communications. This material was presented in part at the International Workshop on Sequence Design and Its Applications in Communications, Shimonoseki, Yamaguchi, Japan, October 2005 and at the IEEE International Symposium on Information Theory, Seattle, WA, July 2006.

J.-W. Jang and J.-S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: stasera@ccl.snu.ac.kr; jsno@snu.ac.kr).

H. Chung is with School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@hongik.ac.kr).

X. Tang is with Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, China (e-mail: xhutang@ieee.org).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2006.889715

In this correspondence, three methods of constructing LCZ sequences are proposed. In the first method, we constructed binary LCZ sequence sets of period 2^n-1 using the Legendre sequences of period 2^m-1 as a column sequence when $m|n$. In the second method, we devise a column sequence set of length $2^{m+1}-1$ from a binary sequence of period 2^m-1 having ideal autocorrelation property and this column sequence set is used to construct binary LCZ sequence sets of period 2^n-1 when $(m+1)|n$. In the third method, p-ary LCZ sequence sets are constructed by adopting p-ary sequence of period p^m-1 with ideal autocorrelation for integers n and m such that $m|n$ as a column sequence. The second and third methods give us the optimal sets with respect to the bound by Tang, Fan, and Matsufuji [6]. Finally, a construction method of $p^n \times p^n$ p-ary Hadamard matrices from optimal LCZ sequence sets is proposed.

II. Preliminaries

In this section, we introduce some definitions and notations.

Let $\mathcal{S}$ be a set of D sequences of period N. If the magnitude of correlation function between any two sequences in $\mathcal{S}$ takes the values less than or equal to ϵ for the offset τ in the range $-Z < \tau < Z$, then $\mathcal{S}$ is called an (N, D, Z, ϵ) LCZ sequence set.

Let p be a prime and F_{p^n} be the finite field with p^n elements. Let $v_i(x)$ and $v_j(x)$ be two p-ary sequences of period p^n-1, defined in $F_{p^n}^* = F_{p^n} \setminus \{0\}$. Then for $\delta \in F_{p^n}^*$, the correlation function between two p-ary sequences $v_i(x)$ and $v_j(x)$ is defined as

$$R_{v_i,v_j}(\delta) = \sum_{x \in F_{p^n}^*} \omega_p^{v_i(x\delta)-v_j(x)}$$

where ω_p is a complex primitive p-th root of unity. We will abuse the notation of the correlation function as $R_{i,j}(\tau) = R_{v_i,v_j}(\alpha^\tau)$ for $\delta = \alpha^\tau$, where α is a primitive element in F_{p^n}.

Let $v(t)$ be a p-ary sequence of period p^n-1. Then $v(t)$ is said to have balance property if number of zero element is one less than that of each nonzero element in one period of the sequence. And if the sequence $v(t)-v(t+\tau)$ is balanced for all $\tau \not\equiv 0 \bmod p^n-1$, then $v(t)$ is said to have difference-balance property.

The trace function $\mathrm{tr}_m^n(\cdot)$ from F_{p^n} to F_{p^m} is defined by

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{p^{mi}}$$

where $x \in F_{p^n}$ and $m|n$. The trace function has the following properties:

1) $\mathrm{tr}_m^n(ax+by) = a\,\mathrm{tr}_m^n(x) + b\,\mathrm{tr}_m^n(y)$, for all $a, b \in F_{p^m}$, $x, y \in F_{p^n}$;
2) $\mathrm{tr}_m^n(x^{p^m}) = \mathrm{tr}_m^n(x)$, for all $x \in F_{p^n}$.

It is well known that $\mathrm{tr}_m^n(\alpha^t)$ is a p^m-ary m-sequence of period p^n-1, where α is a primitive element in F_{p^n}.

Klapper [7] introduced the d-form function. A d-form function $H(x)$ on F_{p^n} over F_{p^m} is defined as a function satisfying for any $y \in F_{p^m}$ and $x \in F_{p^n}$

$$H(yx) = y^d H(x). \tag{1}$$

Kim, Jang, No, and Chung [5] derived the following lemma, which can be used in the proof of the subsequent theorem.

Lemma 1 ([5]): Let m and n be positive integers such that $m|n$. Let $A = \{1, \alpha, \ldots, \alpha^{T-1}\}$, where α is a primitive element in F_{p^n} and $T = (p^n-1)/(p^m-1)$. Let $h(x)$ be a 1-form function from F_{p^n}

onto F_{p^m} with balance and difference-balance property. For a given $\delta \in F_{p^n} \setminus F_{p^m}$, let $M_\delta(a,b)$ be the number of $x_2 \in A$ satisfying

$$h(\delta x_2) = a \text{ and } h(x_2) = b, \text{ for } a, b \in F_{p^m}. \tag{2}$$

Then, we have

$$M_\delta(0,0) = \frac{p^{n-2m}-1}{p^m-1}$$
$$\sum_{c \in F^*_{p^m}} M_\delta(c,0) = \sum_{c \in F^*_{p^m}} M_\delta(0,c) = p^{n-2m}$$
$$\sum_{d \in F^*_{p^m}} M_\delta(cd,d) = p^{n-2m}, \text{ for any } c \in F^*_{p^m}.$$

□

Tang and Fan [4] stated the following theorem using the interleaved sequence [8], which can be used for the construction of an LCZ sequence set.

Theorem 2 ([4]): Let m and n be integers such that $m|n$. Let $f(y)$ and $g(y)$ be cyclically distinct sequences of period p^m-1 from F_{p^m} to F_p and the function $h(x)$ from F_{p^n} to F_{p^m} be a 1-form function over F_{p^m} with balance and difference-balance property. If we set $f(0) = g(0) = 0$, then the correlation function $R_{f,g}(\delta)$ between $f(h(x))$ and $g(h(x))$ is given as

$$R_{f,g}(\delta) = \sum_{x \in F^*_{p^n}} \omega_p^{f(h(\delta x))-g(h(x))}$$
$$= \begin{cases} p^{n-m}\Big(C_{f,g}(\delta)+1\Big)-1, & \text{if } \delta \in F_{p^m} \\ p^{n-2m}(I(f)+1)(\bar{I}(g)+1)-1, & \text{if } \delta \notin F_{p^m} \end{cases}$$

where $I(f) = \sum_{y \in F^*_{p^m}} \omega_p^{f(y)}$, $C_{f,g}(\delta) = \sum_{y \in F^*_{p^m}} \omega_p^{f(\delta y)-g(y)}$, and $\bar{I}(\cdot)$ denotes complex conjugate of $I(\cdot)$.

□

In the above theorem, $f(\cdot)$ and $g(\cdot)$ are called the *column sequences* of period p^m-1 in the two dimensional representation of the sequences $f(h(\cdot))$ and $g(h(\cdot))$ of period p^n-1, respectively.

It is clear that $I(f) = -1$ corresponds to the balance property of the column sequence $f(y)$ defined on $F^*_{p^m}$ if p is a prime. If the column sequences are balanced, we have

$$R_{f,g}(\delta) = -1, \text{ for } \delta \notin F_{p^m}.$$

In order to have $R_{f,g}(1) = -1$, we have to have $C_{f,g}(1) = -1$, which means that the in-phase cross-correlation function of each pair of sequences in the column sequence set has the value -1.

Property 3: Let $\mathcal{A}$ be the set of sequences of period p^m-1 satisfying the following properties:

1) all the sequences in the set $\mathcal{A}$ are cyclically distinct;
2) each sequence in the set $\mathcal{A}$ has the balance property;
3) in-phase cross-correlation value of each pair of the sequences in the set $\mathcal{A}$ is always -1.

□

Theorem 2 tells us that if we have the sequence set $\mathcal{A}$ satisfying Property 3, then the $(p^n-1, |\mathcal{A}|, (p^n-1)/(p^m-1), 1)$ p-ary LCZ sequence set can be constructed.

In the subsequent sections, we propose methods of constructing the column sequence sets satisfying Property 3, some of which are of the maximum size.

III. Binary LCZ Sequence Sets From Legendre Sequences

In this section, we propose a new binary LCZ sequence set using the Legendre sequence as a column sequence.

Let $s(t)$ be a binary sequence from $F^*_{2^m}$ to F_2 and β be a primitive element in F_{2^m}. Then Fourier transform $S(\lambda)$ of the sequence $s(t)$ and its inverse transform are given as

$$S(\lambda) = \sum_{t=0}^{2^m-2} s(t)\beta^{-\lambda t}$$
$$s(t) = \sum_{\lambda=0}^{2^m-2} S(\lambda)\beta^{\lambda t}.$$

Legendre sequences of period p for any prime p are defined as

$$s(t) = \begin{cases} 1, & \text{if } t = 0 \bmod p \\ 0, & \text{if } t \text{ is a quadratic residue } \bmod p \\ 1, & \text{if } t \text{ is a quadratic nonresidue } \bmod p. \end{cases} \tag{3}$$

And it is well known that $s(t), t = 0, 1, 2, \ldots, p-1$, has the ideal autocorrelation property if and only if $p \equiv 3 \pmod 4$.

Lemma 4 ([10]): Let m be an integer such that 2^m-1 is a prime. Let $s(t)$ be the Legendre sequence defined in (3). Then $s(t)$ can be represented as follows:

$$s(t) = \sum_{j \in QR} \beta^{jt}$$

where β is a primitive element in F_{2^m} and QR is the set of quadratic residues mod 2^m-1. □

Then the Legendre sequences have the properties in the following lemmas.

Lemma 5: Let $m > 3$ be an integer such that $2^m-1 = p \equiv 3 \pmod 4$ is a prime. Let $s(t)$ be the Legendre sequence of period 2^m-1 defined in (3). Then there is no integer pair (a,b) that satisfies the relation

$$s(t)+s(t+a)+s(t+b) = 0, \ 0 \le a, b \le 2^{m-1}-1. \tag{4}$$

Proof: It is clear that (4) cannot hold when $a = b$. Therefore without loss of generality, we assume $a < b$. Taking Fourier transform of (4), we get the following equation.

$$(1+\beta^{\lambda a}+\beta^{\lambda b})S(\lambda) = 0 \tag{5}$$

where β is a primitive element in F_{2^m}. The above equation implies that for every λ such that $S(\lambda) \neq 0$, β^λ is the solution of $1+z^a+z^b = 0$.

From Lemma 4, and the definition of inverse Fourier transform, we have

$$S(\lambda) = \begin{cases} 1, & \text{for } \lambda \in QR \\ 0, & \text{otherwise.} \end{cases}$$

If $S(\lambda) \neq 0$, i.e., $\lambda \in QR$, β^λ is always the solution of equation $z^b+z^a+1 = 0$. It is clear that $\beta^{-\lambda}$ is the solution of $z^b+z^{b-a}+1 = 0$, the reciprocal polynomial of $z^b+z^a+1 = 0$. This means that for each of the quadratic nonresidues λ, β^λ is the solution of $z^b+z^{b-a}+1 = 0$, since -1 is a quadratic nonresidue. Therefore, we have

$$(z^b+z^a+1)(z^b+z^{b-a}+1)(z+1) \equiv 0 \pmod{z^p-1}$$

which is equivalent to

$$(z^b+z^a+1)(z^b+z^{b-a}+1) = 1+z+z^2+\cdots+z^{p-1}.$$

But the equation

$$\begin{aligned}(z^b+z^a+1)(z^b+z^{b-a}+1) &= z^{2b}+z^{b+a}+z^{2b-a}\\ &\quad +z^{b-a}+z^b+z^a+1\\ &= 1+z+z^2+\cdots+z^{p-1}\end{aligned}$$

only holds when $p=7$ with $(a,b)=(1,3),(2,3),(2,6)$, and $(4,6)$. That means that if $m>3$, there is no integer pair (a,b) such that $s(t)+s(t+a)+s(t+b)=0$. □

Lemma 6: Let $m>3$ be an integer such that $2^m-1=p\equiv 3 \pmod 4$ is a prime. Let $s(t)$ be the Legendre sequence of period 2^m-1 defined in (3). Then for nonzero a and $b\neq c$, there is no integer triplet (a,b,c) that satisfies the relation

$$s(t)+s(t+a)+s(t+b)+s(t+c)=0, 0\le a,b,c\le 2^{m-1}-1 \quad (6)$$

except for $(a,0,a)$ and $(a,a,0)$.

Proof: It is manifest that (6) holds when $(a,b,c)=(a,0,a)$ and $(a,b,c)=(a,a,0)$. Let $a<b<c$ be integers and $S(\lambda)$ be the Fourier transform of $s(t)$. Then by the similar argument in the proof of Lemma 5, we can say that $1+\beta^{\lambda a}+\beta^{\lambda b}+\beta^{\lambda c}=0$ for all quadratic residues λ, and $1+\beta^{\lambda(c-a)}+\beta^{\lambda(c-b)}+\beta^{\lambda c}=0$ for all quadratic nonresidues λ.

Therefore, the equation

$$(z^c+z^b+z^a+1)(z^c+z^{c-b}+z^{c-a}+1)\equiv 0 \pmod{z^p-1}$$

holds, since $z=1$ is the common solution of $z^c+z^b+z^a+1=0$ and $z^c+z^{c-b}+z^{c-a}+1=0$. After careful scrutiny, we can deduce that for the integers $a<b<c$, the above equation cannot hold. □

Using Lemmas 5 and 6, we construct a set of cyclically distinct binary sequences of period 2^m-1 satisfying Property 3 from a binary Legendre sequence.

Theorem 7: Let m be an integer such that $m>3$ and 2^m-1 is a prime. Let $s(t)=l(\beta^t)$ be a Legendre sequence of period 2^m-1, where β is a primitive element in F_{2^m}. Define the new sequences $s_i(t)$, $0\le i\le 2^{m-1}-1$ of period 2^m-1 such that

$$s_i(t)=\begin{cases} s(t), & \text{if } i=0\\ s(t)+s(t+i), & \text{if } 1\le i\le 2^{m-1}-1.\end{cases}$$

Then the set of sequences $s_i(t)$ satisfies Property 3.

Proof: From the balance and difference-balance properties of the Legendre sequence, it is easy to see that $s_i(t)$ is balanced. And from the definition of $s_i(t)$, it is also clear that the in-phase cross-correlation $C_{s_i,s_j}(1)$ between $s_i(t)$ and $s_j(t)$ always takes the value -1. Finally, Lemmas 5 and 6 tell us that all $s_i(t)$ are cyclically distinct. Thus the set of sequences $s_i(t)$ satisfies Property 3. □

Using Theorems 2 and 7, we can construct a binary LCZ sequence set with parameters $(2^n-1,2^{m-1},(2^n-1)/(2^m-1),1)$ as in the following theorem.

Theorem 8: Let n and m be integers such that $m>3$, $m|n$, and 2^m-1 is a prime and $T=(2^n-1)/(2^m-1)$. Let α be a primitive element in F_{2^n} and $\beta=\alpha^T$ be a primitive element in F_{2^m}. Let $l(\beta^t)=s(t)$ be the Legendre sequence defined in (3) of period 2^m-1. Let $h(x)$ from F_{2^n} to F_{2^m} be a 1-form function over F_{2^m} with balance and difference-balance property, i.e., either a 2^m-ary m-sequence, a 2^m-ary GMW sequence, or a 2^m-ary generalized GMW sequence. Then the sequence set $\mathcal{S}$ defined by

$$\mathcal{S}=\{v_i(t)\mid 0\le t\le 2^n-1,\ 0\le i\le 2^{m-1}-1\}$$

where $v_i(t)$ is given as

$$v_i(t)=\begin{cases} l(h(\alpha^t)), & \text{if } i=0\\ l(h(\alpha^t))+l(h(\alpha^{t+Ti})), & \text{if } 1\le i\le 2^{m-1}-1\end{cases}$$

is a $(2^n-1,2^{m-1},(2^n-1)/(2^m-1),1)$ LCZ sequence set. □

No, Lee, Chung, Song, and Yang found the trace representation of Legendre sequence as in the following theorem.

Theorem 9 ([10]): Let $p=2^m-1$ be a prime for some integer $m\ge 3$ and u be a primitive element in Z_p, the set of integers mod p. Let β be a primitive element in F_{2^m} such that

$$\sum_{i=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m(\beta^{u^{2i}})=0.$$

Then the Legendre sequence $s(t)$ in (3) can be rewritten as

$$s(t)=\sum_{i=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m(\beta^{u^{2i}t}).$$

□

Using the above theorem, we can represent the new binary LCZ sequence set in the closed form as in the following corollary.

Corollary 10: Let m and n be integers such that $m>3$, $m|n$, and $p=2^m-1$ be a prime. Let α be a primitive element in F_{2^n} and $h(x)=\mathrm{tr}_m^n(x)$. Then the sequence $v_i(t)$ defined in Theorem 8 can be represented as

$$v_i(t)=\begin{cases} \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t)]^{u^{2j}}), & \text{for } i=0\\ \sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^t)]^{u^{2j}}) & \\ \quad +\sum_{j=0}^{\frac{p-1}{2m}-1} \mathrm{tr}_1^m([\mathrm{tr}_m^n(\alpha^{t+Ti})]^{u^{2j}}), & \text{for } 1\le i\le 2^{m-1}-1\end{cases}$$

where u is defined in Theorem 9. □

IV. New Optimal Binary LCZ Sequence Sets

In this section, for integers n and m such that $(m+1)|n$, we construct the optimal binary LCZ sequence set of period 2^n-1 by using binary sequences of period 2^m-1 with ideal autocorrelation.

The following lemma can be easily stated without proof.

Lemma 11: Let $m_1(t)$ and $m_2(t)$ be two cyclically distinct p-ary sequences with linear span L_1 and L_2, respectively. The maximum run lengths of the symbol 0 and the symbol a, $1\le a\le p-1$, for the difference sequence $m_1(t)-m_2(t)$ are less than or equal to L_1+L_2-1 and L_1+L_2, respectively. □

Using two binary sequences with ideal autocorrelation, we can construct a set of column sequences satisfying Property 3 as in the following theorem.

Theorem 12: : Let $m_1(t)$ and $m_2(t)$ be two binary sequences, not necessarily distinct, of period 2^m-1 with ideal autocorrelation. Let L_1 and L_2 be the linear spans of the sequences $m_1(t)$ and $m_2(t)$, respectively. Assume that $L_1+L_2+\max(L_1,L_2) < 2^m-1$, if $m_1(t)$ and $m_2(t)$ are cyclically inequivalent and $L_1=L_2<2^{m-1}$, if $m_1(t)$ and $m_2(t)$ are cyclically equivalent. Define the new sequences $s_i(t),\ 0\le i\le 2^{m+1}-2$ of period $2^{m+1}-1$ such that

i) for $0\le i\le 2^m-2$

$$s_i(t)=\begin{cases} m_1(t+i), & 0\le t\le 2^m-2\\ 0, & t=2^m-1\\ m_2(t-1-i), & 2^m\le t\le 2^{m+1}-2.\end{cases} \tag{7}$$

ii) for $2^m-1\le i\le 2^{m+1}-3$

$$s_i(t)=\begin{cases} m_1(t+i), & 0\le t\le 2^m-2\\ 1, & t=2^m-1\\ m_2(t-1-i)+1, & 2^m\le t\le 2^{m+1}-2\end{cases} \tag{8}$$

and

$$s_{2^{m+1}-2}(t)=\begin{cases}0, & 0\le t\le 2^m-2\\ 1, & 2^m-1\le t\le 2^{m+1}-2.\end{cases}$$

Then the set of sequences $s_i(t)$ satisfies Property 3.

Proof: From the definition of $s_i(t)$, it is clear that $s_i(t)$ is balanced and it is also easy to see that the in-phase cross-correlation $C_{s_i,s_j}(1)$ between $s_i(t)$ and $s_j(t)$ takes the value -1.

Certainly the last sequence $s_{2^{m+1}-2}(t)$ is cyclically distinct to every other sequence. What we are going to show is that for any $i,\ j,\ 0\le i,j\le 2^{m+1}-3$, and τ, $s_j(t)=s_i(t+\tau)$ implies that $i=j$ and $\tau=0$.

Case 1) $0\le i,j\le 2^m-3$ and $0\le\tau\le 2^m-2$.

It is not difficult to see that $s_i(t+\tau)$ can be expressed as (9) shown at the bottom of the page.

Assume $s_j(t)=s_i(t+\tau)$ for all t. From (7) and (9), we have

$$m_1(t+j)+m_1(t+i+\tau)=0,\quad 0\le t\le 2^m-2-\tau \tag{10}$$

$$m_1(t+j)+m_2(t-1-i+\tau)=0,\quad 2^m-\tau\le t\le 2^m-2 \tag{11}$$

$$m_2(t-1-j)+m_2(t-1-i+\tau)=0,\quad 2^m\le t\le 2^{m+1}-2-\tau \tag{12}$$

$$m_2(t-1-j)+m_1(t+i+\tau-1)=0,\quad 2^{m+1}-1-\tau\le t\le 2^{m+1}-2. \tag{13}$$

Left-hand side of (10) and (12) has $2^m-1-\tau$ consecutive zeros. Thus if $\tau<2^m-max(L_1,L_2)$, i.e., $2^m-1-\tau\ge\max(L_1,L_2)$, then we have $j=i-\tau=i+\tau$, which further tells us that $i=j$ and $\tau=0$. Note that in this case (11) and (13) become meaningless. If $\tau\ge 2^m-max(L_1,L_2)$, then left (11) and (13) does not hold unless $m_1(t)=m_2(t)$ since $\tau-1\ge L_1+L_2$. Thus, satisfying (11) and (13) at the same time means that $m_1(t)$ and $m_2(t)$ are cyclically equivalent and $i+j=\tau-1=-\tau$, which further implies $\tau=2^{m-1}$. But $\tau=2^{m-1}$ is not in the range $\tau\ge 2^m-\max(L_1,L_2)$, since $\max(L_1,L_2)<2^{m-1}$.

Case 2) $0\le i,j\le 2^m-3$ and $2^m\le\tau\le 2^{m+1}-2$.

Case 3) $2^m-1\le i,j\le 2^{m+1}-3$ and $0\le\tau\le 2^m-2$.

Case 4) $2^m-1\le i,j\le 2^{m+1}-3$ and $2^m\le\tau\le 2^{m+1}-2$.

Case 5) $2^m-1\le i\le 2^{m+1}-3$, $0\le j\le 2^m-2$, and $0\le\tau\le 2^m-2$.

Case 6) $2^m-1\le i\le 2^{m+1}-3$, $0\le j\le 2^m-2$, and $2^m\le\tau\le 2^{m+1}-2$.

Using the similar argument in Case 1), in each case, $s_i(t)$ and $s_j(t)$ is cyclically distinct when $L_1+L_2+max(L_1+L_2)<2^m-1$.

Case 7) $\tau=2^m-1$.

In this case, it is straightforward that $s_i(t+\tau)\ne s_j(t), 0\le i,j\le 2^{m+1}-3$.

From the above seven cases, we proved that $s_i(t)$ and $s_j(t)$ are cyclically distinct for all i and j. Thus, we proved that the set of sequences $s_i(t)$ satisfies Property 3.

□

Example 13: $m_1(t)=m_2(t)$ be binary m-sequences with period $2^3-1=7$ given as

$$m_1(t)=m_2(t)=1001011.$$

Then the sequences $s_i(t)$ are given as

$$\begin{aligned}
s_0(t)&=100101101001011\\
s_1(t)&=001011101100101\\
s_2(t)&=010111001110010\\
s_3(t)&=101110000111001\\
s_4(t)&=011100101011100\\
s_5(t)&=111001000101110\\
s_6(t)&=110010100010111\\
s_7(t)&=100101110110100\\
s_8(t)&=001011110011010\\
s_9(t)&=010111010001101\\
s_{10}(t)&=101110011000110\\
s_{11}(t)&=011100110100011\\
s_{12}(t)&=111001011010001\\
s_{13}(t)&=110010111101000\\
s_{14}(t)&=111111110000000
\end{aligned}$$

which satisfy Property 3.

□

Using Theorem 2 and the column sequence sets in Theorem 12, we can construct the binary LCZ sequence sets as in the following theorem.

Theorem 14: Let n and m be integers such that $(m+1)|n$ and $T=(2^n-1)/(2^{m+1}-1)$. Let α be a primitive element in F_{2^n} and $\beta=\alpha^T$ be a primitive element in $F_{2^{m+1}}$. Let $h(x)$ from F_{2^n} to $F_{2^{m+1}}$ be a

$$s_i(t+\tau)=\begin{cases} m_1(t+i+\tau), & 0\le t\le 2^m-2-\tau\\ 0, & t=2^m-1-\tau\\ m_2(t-1-i+\tau), & 2^m-\tau\le t\le 2^{m+1}-2-\tau\\ m_1(t+i+\tau-1), & 2^{m+1}-1-\tau\le t\le 2^{m+1}-2.\end{cases} \tag{9}$$

1-form function over $F_{2^{m+1}}$ with balance and difference-balance property, i.e., either a 2^{m+1}-ary m-sequence, a 2^{m+1}-ary GMW sequence, or a 2^{m+1}-ary generalized GMW sequence. Let $f_i(\beta^t) = s_i(t)$, where $s_i(t)$ is the binary sequence defined in Theorem 12. Then the sequence set $\mathcal{B}$ defined by

$$\mathcal{B} = \{v_i(t) = f_i(h(\alpha^t)) \mid 0 \le i \le 2^{m+1} - 2,\ 0 \le t \le 2^n - 2\}$$

is a binary LCZ sequence set with parameters $(2^n - 1, 2^{m+1} - 1, T, 1)$. □

Tang, Fan, and Matsufuji [6] derived the lower bound on LCZ sequences using the Welch bound [12].

Theorem 15 (Tang, Fan, and Matsufuji [6]): Let $\mathcal{S}$ be a set of LCZ sequences with parameters (N, D, Z, ϵ). Then,

$$DZ - 1 \ge \frac{N-1}{1 - \epsilon^2/N}. \tag{14}$$

□

Now we can check the optimality of our binary LCZ sequence set $\mathcal{B}$.

Corollary 16: The binary LCZ sequence set $\mathcal{B}$ in Theorem 14 is optimal with respect to the Tang-Fan-Matsufuji bound given in Theorem 15.

Proof: The proof is straightforward. By substituting $N = 2^n - 1$, $D = 2^{m+1} - 1$, and $\epsilon = 1$ in (14), we have

$$(2^{m+1} - 1)Z - 1 \le \frac{2^n - 2}{1 - 1/(2^n - 1)}$$

and thus

$$Z \le \frac{2^n}{2^{m+1} - 1}.$$

Since Z is an integer, we have

$$Z \le \left\lfloor \frac{2^n}{2^{m+1} - 1} \right\rfloor = \frac{2^n - 1}{2^{m+1} - 1} = T.$$

Clearly, $\mathcal{B}$ is optimal with respect to the Tang-Fan-Matsufuji bound. □

V. New Optimal p-ary LCZ Sequence Sets

In this section, for a prime p and integers n and m such that $m|n$, we propose a new construction method of the optimal p-ary LCZ sequence set of period $p^n - 1$ by using a p-ary sequence of period $p^m - 1$ with ideal autocorrelation.

In the next theorem, we construct a set of p-ary cyclically distinct sequences of period $p^m - 1$ satisfying Property 3 from a p-ary sequence with ideal autocorrelation.

Theorem 17: Let p be a prime and $m(t)$ be a p-ary sequence with ideal autocorrelation of period $M = p^m - 1$. Let L_m be the linear span of $m(t)$ and assume that $3L_m - 1 < M/2$. Let $\{m_i(t) \mid 0 \le i \le M - 1\}$ be a set of cyclic shifts of $m(t)$, such that $m_i(t) = m(t + i)$, $t = 0, 1, 2, \ldots, M - 1$. Define new sequences $s_i(t)$, $0 \le i \le M - 1$, such that

$$s_i(t) = \begin{cases} m_i(M - 1 - t), & 0 \le t \le M - K - 1 \\ m_i(t + K), & M - K \le t \le M - 1 \end{cases} \tag{15}$$

for some integer K in the range $3L_m - 1 \le K \le M/2$. Then the set of p-ary sequences $s_i(t)$, $0 \le i \le M - 1$ satisfies Property 3.

Proof: From the definition of $s_i(t)$, it is clear that all $s_i(t)$ are balanced and it is also easy to see that the in-phase cross-correlation $C_{s_i,s_j}(1)$ between $s_i(t)$ and $s_j(t)$ takes the value -1.

Now, what we have to show is that for any i, j, and τ, $s_j(t) = s_i(t + \tau)$ implies that $i = j$ and $\tau = 0$. The sequence $s_i(t)$ in (15) can be rewritten as

$$s_i(t) = \begin{cases} m(M - 1 - t + i), & 0 \le t \le M - K - 1 \\ m(t + i + K), & M - K \le t \le M - 1. \end{cases} \tag{16}$$

It is not difficult to see that $s_i(t + \tau)$ can be expressed as:

Case 1) $0 \le \tau \le M - K - 1$.

See (17) shown at the bottom of the page.

Assume $s_j(t) = s_i(t + \tau)$ for all t. Then from (16) and (17), we have

$$m(M - 1 - t + j) = m(M - 1 - t - \tau + i) \quad 0 \le t \le M - K - 1 - \tau \tag{18}$$

$$m(M - 1 - t + j) = m(t + \tau + i + K) \quad M - K - \tau \le t \le M - K - 1 \tag{19}$$

$$m(t + j + K) = m(t + \tau + i + K) \quad M - K \le t \le M - \tau - 1 \tag{20}$$

$$m(t + j + K) = m(M - 1 - t - \tau + i) \quad M - \tau \le t \le M - 1. \tag{21}$$

Here, we consider the following two cases depending on τ.

When $\tau \le 2L_m - 1$, both $M - K - \tau$ and $K - \tau$ are greater than or equal to L_m since $3L_m - 1 \le K \le M/2$. From (18), we have

$$m(M - 1 - t + j) - m(M - 1 - t - \tau + i) = 0 \tag{22}$$

for consecutive $M - K - \tau$ values of t. And similarly from (20), we have

$$m(t + j + K) - m(t + \tau + i + K) = 0 \tag{23}$$

for consecutive $K - \tau$ values of t. It is clear that the linear span of $m(t) - m(t + k)$ for all k, $1 \le k \le p^m - 2$, is L_m. Since both $M - K - \tau$ and $K - \tau$ are greater than or equal to L_m, (22) and (23) imply that

$$j = i - \tau = i + \tau$$

which further tells us that $i = j$ and $\tau = 0$. And again in this case, (19) and (21) vanish.

When $\tau \ge 2L_m$, (19) or (21) implies that some consecutive τ bits of two sequences $m(t)$ and $m(-t)$ are identical, which is a contradiction from Lemma 11 since the linear span of $m(t) - m(-t + k)$ for all k, $0 \le k \le p^m - 2$, is at most $2L_m$.

Case 2) $\tau \ge M - T$.

Similarly to Case 1), since both $\tau - K$ and $\tau - (M - K)$ are greater than or equal to L_m, we can deduce $i = j$ and $\tau = 0$.

□

Note that even if we limit the range of K as $3L_m - 1 \le K \le M/2$ in Theorem 17 for the sake of the simplicity of the proof, in fact the

$$s_i(t + \tau) = \begin{cases} m(M - 1 - t - \tau + i), & 0 \le t \le M - K - 1 - \tau \\ m(t + \tau + i + K), & M - K - \tau \le t \le M - \tau - 1 \\ m(M - 1 - t - \tau + i), & M - \tau \le t \le M - 1. \end{cases} \tag{17}$$

theorem holds for all K such that $3L_m - 1 \le K \le M - (3L_m - 1)$. If $3L_m - 1 > M/2$, the above theorem cannot be directly applied. But we can observe that the sequences $s_i(t)$ in (15) constructed from the binary m-sequence with $L_m = 4$ are all cyclically distinct for $K = 7$, even though the condition $3L_m - 1 < M/2$ is not met.

Using Theorem 2 and the column sequence set in Theorem 17, we can construct the p-ary LCZ sequence sets as in the following theorem.

Theorem 18: Let p be a prime and n and m be integers such that $m|n$. Let $T = (p^n-1)/(p^m-1)$ and $M = p^m-1$. Let α be a primitive element in F_{p^n} and $\beta = \alpha^T$ be a primitive element in F_{p^m}. Let $h(x)$ from F_{p^n} to F_{p^m} be a 1-form function over F_{p^m} with balance and difference-balance property, i.e., a p^m-ary unified sequence [9] which includes an m-sequence, a GMW sequence, and a generalized GMW sequence. Let $f_i(\beta^t) = s_i(t)$, where $s_i(t)$ is the sequence defined in Theorem 17. Then the following sequence set $\mathcal{P}$ defined by

$$\mathcal{P} = \{v_i(t) = f_i(h(\alpha^t)) \mid 0 \le i \le p^m - 2,\ 0 \le t \le p^n - 2\}$$

is a LCZ sequence set with parameters $(p^n - 1, p^m - 1, T, 1)$. □

Corollary 19: The p-ary LCZ sequence set $\mathcal{P}$ in Theorem 18 is optimal with respect to the Tang-Fan-Matsufuji bound given in Theorem 15.

Proof: The proof is straightforward. By substituting $N = p^n - 1$, $D = p^m - 1$, and $\epsilon = 1$ in (14), we have

$$(p^m - 1)Z - 1 \le \frac{p^n - 2}{1 - 1/(p^n - 1)}$$

and thus

$$Z \le \frac{p^n}{p^m - 1}.$$

Since Z is an integer, we have

$$Z \le \left\lfloor \frac{p^n}{p^m - 1} \right\rfloor = \frac{p^n - 1}{p^m - 1} = T.$$

Clearly, $\mathcal{P}$ is optimal with respect to the Tang-Fan-Matsufuji bound. □

VI. Some Theorems of LCZ Sequences Related to Hadamard Matrices

In this section, we propose a construction method of a $p^n \times p^n$ Hadamard matrix from an optimal LCZ sequence set with parameters $(p^n - 1, p^m - 1, (p^n - 1)/(p^m - 1), 1)$.

Theorem 20: Let p be a prime and n and m be integers such that $m|n$. Let $T = (p^n - 1)/(p^m - 1)$. Let $\mathcal{S}$ be the LCZ sequence set with parameters $(p^n - 1, p^m - 1, T, 1)$ given by

$$\mathcal{S} = \{v_i(t) \mid 0 \le i \le p^m - 2,\ 0 \le t \le p^n - 2\}.$$

Then we can construct the p-ary $p^n \times p^n$ Hadamard matrix $\mathcal{H}_L$ as follows:

$$\mathcal{H}_L = (h_{ij})$$

where h_{ij} is given as

$$h_{ij} = \begin{cases} 0, & \text{if } i = 0 \text{ or } j = 0 \\ v_{\lfloor i/T \rfloor}(j - 1 + i_T), & \text{otherwise} \end{cases}$$

and $i_T = (i - 1) \bmod T$.

Proof: It is clear that the inner product between any two distinct rows in $\mathcal{H}_L$ can be represented as

$$1 + \sum_{t=0}^{p^n-2} \omega_p^{v_i(t) - v_j(t+\tau)}$$

where τ is given as

$$\begin{aligned} &0 \le \tau \le T - 1, \quad \text{if } i \ne j \\ &1 \le \tau \le T - 1, \quad \text{if } i = j. \end{aligned} \tag{24}$$

From the definition of LCZ sequence set with parameters $(p^n - 1, p^m - 1, T, 1)$, it is easy to see that the following equation holds for τ in (24)

$$\sum_{t=0}^{p^n-2} \omega_p^{v_i(t) - v_j(t+\tau)} = -1.$$

Therefore, $\mathcal{H}_L$ is a $p^n \times p^n$ Hadamard matrix. □

Using the above theorem and the optimal LCZ sequence sets in Theorems 14 and 18, we can construct Hadamard matrices as follows.

Corollary 21: Let n and m be integers such that $(m + 1)|n$ and $T = (2^n - 1)/(2^{m+1} - 1)$. Let $v_i(t)$ be the sequences defined in Theorem 14 and $i_T = (i-1) \bmod T$. Then we can construct a $2^n \times 2^n$ Hadamard matrix $\mathcal{H}_B$ as follows:

$$\mathcal{H}_B = (h_{ij})$$

where h_{ij} is given as

$$h_{ij} = \begin{cases} 0, & \text{if } i = 0 \text{ or } j = 0 \\ v_{\lfloor i/T \rfloor}(j - 1 + i_T), & \text{otherwise.} \end{cases}$$

□

Corollary 22: Let n and m be integers such that $m|n$ and $T = (p^n - 1)/(p^m - 1)$. Let $v_i(t)$ be the sequence defined in Theorem 18 and $i_T = (i-1) \bmod T$. Then we can construct a $p^n \times p^n$ generalized Hadamard matrix $\mathcal{H}_P$ as follows:

$$\mathcal{H}_P = (h_{ij})$$

where h_{ij} is given as

$$h_{ij} = \begin{cases} 0, & \text{if } i = 0 \text{ or } j = 0 \\ v_{\lfloor i/T \rfloor}(j - 1 + i_T), & \text{otherwise.} \end{cases}$$

□

Acknowledgment

The authors wish to thank the anonymous reviewers for their valuable comments and suggestions that much improved the presentation of this correspondence.

References

[1] R. De Gaudenzi, C. Elia, and R. Viola, "Bandlimited quasisynchronous CDMA: A novel satellite access technique for mobile and personal communication system," *IEEE J. Sel. Areas Commun.*, vol. 10, pp. 328–343, Feb. 1992.

[2] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vol. 47, pp. 1268–1275, Nov. 1998.

[3] X. H. Tang and P. Z. Fan, "A class of pseudonoise sequences over $\mathrm{GF}(p)$ with low correlation zone," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1644–1649, May 2001.
[4] X. H. Tang and P. Z. Fan, Large families of generalized d–form sequences with low correlations and large linear span based on the interleaved technique 2004, to be published.
[5] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1469–1477, Apr. 2005.
[6] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlatoin zone," *Electron. Lett.*, vol. 36, no. 6, pp. 551–552, Mar. 2000.
[7] A. Klapper, "d-form sequence: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 423–431, Mar. 1995.
[8] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, pp. 400–411, Mar. 1995.
[9] J.-S. No, "p-ary unified sequences p-ary extended d-form sequences with ideal autocorrelation property," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2540–2546, Sep. 2002.
[10] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 2254–2255, Nov. 1996.
[11] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. IEEE Int. Symp. Inform. Theory and Its Appl. (ISITA'96)*, Victoria, BC, Canada, Sep. 1996, pp. 837–840.
[12] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.

A Note on Numerical Semigroups

Maria Bras-Amorós

***Abstract*—This correspondence is a short extension to the previous article Bras-Amorós, 2004. In that work, some results were given on one-point codes related to numerical semigroups. One of the crucial concepts in the discussion was the so-called ν-*sequence* of a semigroup. This sequence has been used in the literature to derive bounds on the minimum distance as well as for defining improvements on the dimension of existing codes. It was proven in that work that the ν-sequence of a semigroup uniquely determines it. Here this result is extended to another object related to a semigroup, the $\oplus$ operation. This operation has also been important in the literature for defining other classes of improved codes. It is also proven here that, although the infinite set of values in the ν-sequence (resp. the $\oplus$ values) uniquely determines the associated semigroup, no finite part of it can determine it, because it is shared by infinitely many semigroups. In that reference the proof of the fact that the ν-sequence of a numerical semigroup uniquely determines it is constructive. The result here presented shows that, however, that construction can not be performed as an algorithm with finite input.**

***Index Terms*—ν-sequence, $\oplus$-operation, improved one-point codes, numerical semigroup, one-point codes.**

I. Introduction

Let $\mathbb{N}_0$ denote the set of all nonnegative integers. A *numerical semigroup* is a subset Λ of $\mathbb{N}_0$ containing 0, closed under summation and with $\mathbb{N}_0 \setminus \Lambda$ being finite. The elements in Λ are called the *nongaps* of Λ while the elements in $\mathbb{N}_0 \setminus \Lambda$ are called the *gaps* of Λ. The *enumeration* of Λ is the unique increasing bijective map $\lambda : \mathbb{N}_0 \longrightarrow \Lambda$. We use λ_i for $\lambda(i)$.

A first object describing the addition behavior of a numerical semigroup with enumeration λ is the binary operation $\oplus$ on $\mathbb{N}_0$ defined by $i \oplus j = \lambda^{-1}(\lambda_i + \lambda_j)$. A second object describing the addition behavior of a numerical semigroup Λ with enumeration λ is the sequence $\nu = (\nu_i)_{i \in \mathbb{N}_0}$, defined by $\nu_i = \#\{j \in \mathbb{N}_0 \mid \lambda_i - \lambda_j \in \Lambda\}$.

Both the ν-sequence and the $\oplus$ operation have important applications related to *one-point codes*. Let $F/\mathbb{F}$ be a function field on the finite field $\mathbb{F}$ and let P be a rational point of $F/\mathbb{F}$. For a divisor D of $F/\mathbb{F}$, let $\mathcal{L}(D) = \{0\} \cup \{f \in F^* \mid (f) + D \geqslant 0\}$. Define $A = \bigcup_{m \geqslant 0} \mathcal{L}(mP)$ and let $\Lambda = \{-v_P(f) \mid f \in A \setminus \{0\}\} = \{-v_i \mid i \in \mathbb{N}_0\}$ with $-v_i < -v_{i+1}$. It holds that $v_P(1) = 0$ and $v_P(fg) = v_P(f) + v_P(g)$ for all $f, g \in A$. Hence, Λ is a numerical semigroup. It is called the *Weierstrass semigroup* at P. Suppose moreover that $P_1, \ldots, P_n$ are pairwise distinct rational points of $F/\mathbb{F}$ which are different from P and let φ be the map $A \to \mathbb{F}^n$ such that $f \mapsto (f(P_1), \ldots, f(P_n))$. For $m \geqslant 0$ the *one-point code* of order m associated to P and $P_1, \ldots, P_n$ is defined as $C_m = \varphi(\mathcal{L}(\lambda_m P))^{\perp}$.

A first application of the sequence ν is on the *order bound* on the minimum distance of the code C_m, defined as $d_{ORD}(C_m) = \min\{\nu_i \mid i > m\}$. It satisfies $d_{C_m} \geqslant d_{ORD}(C_m)$, where d_{C_m} is the minimum distance of the code C_m [1]–[3]. A second application is on the definition of improved codes. Let $\{f_i \in A \mid i \in \mathbb{N}_0\}$ be such that $v_P(f_i) = v_i$. Given a design minimum distance $\delta \in \mathbb{N}_0$, define $\widetilde{C}(\delta) = [\varphi(f_i) \mid \nu_i < \delta]^{\perp}$, where $[u_1, \ldots, u_n]$ is the $\mathbb{F}$-vector space spanned by $u_1, \ldots, u_n$. This is a code improving the dimension of one-point codes while keeping the same design minimum distance [4]. By just guaranteeing correction of the so-called *generic errors* [5] we can define new codes which have still less parity-checks. Those codes are defined by means of the $\oplus$ operation as $\widetilde{C}(\delta) = [\varphi(f_i) \mid i \notin \{a \oplus b \mid a, b \geqslant \lfloor \frac{\delta-1}{2} \rfloor\}]^{\perp}$ [6].

Notice that in both applications of the sequence ν its increasingness is very important. In [7] we prove that the unique numerical semigroup for which ν is strictly increasing is $\mathbb{N}_0$ while the only numerical semigroups for which it is nondecreasing are ordinary numerical semigroups, that is, numerical semigroups whose set of gaps is $\{1, 2, \ldots, g\}$ for some positive integer g. This gives a characterization of a class of semigroups by means of a property on the sequence ν. In the same reference we further showed that a numerical semigroup can be uniquely determined by its associated sequence ν.

Here we show that, similarly, the $\oplus$ operation determines completely the numerical semigroup. However, we also prove that any finite set of $\oplus$-values is shared by an infinite number of semigroups. The same thing will happen for the ν-sequence. Thus, the construction given in [7] to determine a numerical semigroup from its ν-sequence can only be performed if we know the behavior of the infinitely many values in the ν-sequence.

II. The ν-Sequence

Recall that for a numerical semigroup Λ with enumeration λ the sequence $\nu = (\nu_i)_{i \in \mathbb{N}_0}$ is defined by $\nu_i = \#\{j \in \mathbb{N}_0 \mid \lambda_i - \lambda_j \in \Lambda\}$.

Example 2.1: For the numerical semigroup

$$\{0, 4, 5, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 \ldots\}$$

the first values of ν are

$$1, 2, 2, 3, 4, 3, 4, 6, 6, 4, 5, 8, 9, 8, 9, 10, 12, 12, 13, 14, \ldots.$$

Manuscript received February 28, 2006; revised October 16, 2006. The material in this correspondence was presented in part at Arithmetic, Geometry, and Coding Theory, CIRM, Luminy, Marseille, France, May 2003.

The author is with the Departament d'Enginyeria de la Informació i de les Comunicacions, Escola Tècnica Superior d'Enginyeria, Universitat Autònoma de Barcelona, Bellaterra 08193, Spain (e-mail: maria.bras@uab.cat).

Communicated by M. Sudan, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.889739