Generalized Cross-Correlation Properties of Chu Sequences

Jae Won Kang, Younghoon Whang, Byung Hoon Ko, and Kwang Soon Kim, *Senior Member, IEEE*

***Abstract*—In this paper, detailed cross-correlation properties for Chu sequences are investigated. All possible values of the cross-correlation function of Chu sequences are derived for any given sequence length and lag, and the maximum magnitude distribution function $\rho_N(x)$, which is defined as the number of all Chu sequence pairs with length-N whose maximum magnitude of the cross-correlation function is $\sqrt{Nx}$, is obtained. Also, good lower and upper bounds on the maximum number of available Chu sequences and a construction algorithm for the corresponding partial Chu sequence set are proposed when the maximum magnitude of the cross-correlation among the sequences is constrained. Numerical examples show that the proposed bounds are quite tight and the proposed construction algorithm is near-optimal up to fairly large value of N.**

***Index Terms*—Chu sequences, cross-correlation function, distribution, maximum magnitude, maximum number of available Chu sequences.**

I. Introduction

In general, it is desired to design a set of sequences with an impulsive autocorrelation function and a zero cross-correlation function for many practical applications. However, according to the bounds in [1]–[5], it is known to be impossible to construct such an ideal set of sequences and searching large families of sequences with good auto-correlation function and cross-correlation function properties has been one of the most interesting topics in sequence design. For evaluating the correlation properties, one good choice is to use the maximum sidelobe magnitude of the autocorrelation function of a sequence $\boldsymbol{a}$ with length-N and the maximum magnitude of the cross-correlation function of two sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ with length-N, which are respectively denoted as $\hat{\theta}_N(\boldsymbol{a})$ and $\hat{\theta}_N(\boldsymbol{a},\boldsymbol{b})$. Among well known good sequences are Kasami [6], Gold [7], Chu [8], [9] and complex four-phase [10] sequences. For Kasami and Gold sequences, it was shown that there are $\sqrt{N+1}$ sequences satisfying $\hat{\theta}_N(\boldsymbol{a}) = 1$ and $\hat{\theta}_N(\boldsymbol{a},\boldsymbol{b}) = 1+\sqrt{2/N}$[6], [7]. For four-phase sequences, the number of sequences satisfying $\hat{\theta}_N(\boldsymbol{a}) = 1+\sqrt{N}$ and $\hat{\theta}_N(\boldsymbol{a},\boldsymbol{b}) = 1+\sqrt{N}$ is $N+2$[10]. In addition, the detailed cross-correlation properties of such sequences have been reported in [11], [12] and have been widely used in a variety of wireless communication applications, in which typical examples are the design and the performance analysis of spreading sequences [13] or preamble/pilot patterns [14], [15].

A set of Chu sequences with length-N is defined as $\mathbf{C}_N \triangleq \{\boldsymbol{a}_N^r \,|\, r \in \mathbf{R}_N\}$[9], where $\mathbf{R}_N \triangleq \{\, n \,|\, 0 < n < N,\ \gcd(N,n)^1 = 1\}$ and the k^{th} element of $\boldsymbol{a}_N^r$, $a_N^r(k)$, is defined as

$$a_N^r(k) \triangleq W_N\left(\frac{rk\,(k+(N)_2)}{2}\right) \tag{1}$$

where $W_N(i) = \exp(j2\pi i/N)$ and $(\cdot)_b$ denotes the modulo-b operation. It was shown that the periodic autocorrelation function of $\boldsymbol{a}_N^r$ with lag-τ, $\theta_N^r(\tau) \triangleq \sum_{k=0}^{N-1} a_N^r(k)\, a_N^r(k+\tau)^*$, satisfies the perfect auto-correlation function property as $\theta_N^r(\tau) = N\delta_K((\tau)_N)$, where $\delta_K(\cdot)$ is the Kronecker delta function. Also, the cross-correlation function $\theta_N^{r,s}(\tau)$ of $\boldsymbol{a}_N^r$ and $\boldsymbol{a}_N^s$ with lag-τ is defined as $\theta_N^{r,s}(\tau) \triangleq \sum_{k=0}^{N-1} a_N^r(k) a_N^s(k+\tau)^*$, and certain pairs of Chu sequences meet the lower bound, $\hat{\theta}_N(\boldsymbol{a}_N^r,\boldsymbol{a}_N^s) = \sqrt{N}$, when $\gcd(r-s,N) = 1$[17]. However, more detailed cross-correlation properties have not been reported yet.

In this paper, we derive general properties for the cross-correlation function of Chu sequences. For the Chu sequence set $\mathbf{C}_N$, we obtain the magnitude of the cross-correlation function between $\boldsymbol{a}_N^r, \boldsymbol{a}_N^s \in \mathbf{C}_N$ at lag-τ, $|\theta_N^{r,s}(\tau)|$, and the maximum magnitude distribution function $\rho_N(x)$. Here, the maximum magnitude distribution function $\rho_N(x)$ is defined as the number of all sequence pairs from $\mathbf{C}_N$ whose maximum magnitude of the cross-correlation function is $\sqrt{Nx}$. Let $\mathbf{C}_N(\mathbf{\Lambda}) \triangleq \{\boldsymbol{a}_N^r \,|\, r \in \mathbf{\Lambda}\}$ denote the partial Chu sequence set for a given $\mathbf{\Lambda} \subset \mathbf{R}_N$ and $\mathbf{\Xi}_N(\theta)$ be the collection of all subsets of $\mathbf{R}_N$ satisfying $\hat{\theta}_N(\boldsymbol{a}_N^r,\boldsymbol{a}_N^s) \triangleq \max_\tau |\theta_N^{r,s}(\tau)| < \theta$ for any $\mathbf{\Lambda} \in \mathbf{\Xi}_N(\theta)$ and any two elements $r, s \in \mathbf{\Lambda}$. Then, the maximum number of available Chu sequences for a given θ, $\lambda_N(\theta)$, is defined as $\lambda_N(\theta) \triangleq \max_{\mathbf{\Lambda}\in\mathbf{\Xi}_N(\theta)} |\mathbf{C}_N(\mathbf{\Lambda})|$, where $|\mathbf{A}|$ denotes the cardinality of a set $\mathbf{A}$, and we obtain lower and upper bounds on $\lambda_N(\theta)$ and provide a partial sequence set construction algorithm corresponding to the lower bound.

The remaining of this paper is organized as follows. Section II describes the magnitude of the cross-correlation function of Chu sequences and Section III investigates the maximum magnitude distribution and the number of available Chu sequences for given maximum cross-correlation value and the sequence length. Finally, Section IV concludes this paper.

[1]Here, $\gcd(a,b)$ denotes the greatest common divisor (gcd) of two integers a and b. Note that, for an integer c, $\gcd(c,N) = \gcd(|c|,N)$ and $\gcd(0,c) = |c|$[16].

Manuscript received January 13, 2011; revised August 03, 2011; accepted August 15, 2011. Date of publication August 30, 2011; date of current version January 06, 2012. This work was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2011-C1090-1121-0007).

J. W. Kang, B. H. Ko, and K. S. Kim are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Korea (e-mail: ks.kim@yonsei.ac.kr).

Y. Whang is with the School of Electrical Engineering and Computer Science, Oregon State University, Corvallis, OR 97331 USA.

Communicated by N. Y. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2166244

II. Characteristic of the Cross-Correlation Function of Chu Sequences

The following theorem provides what are the possible values that the cross-correlation function of Chu sequences can take.

Definition 1: For $r, s \in \mathbf{R}_N$, define $g \triangleq \gcd(N, r-s)$, $u \triangleq N/g$ and $v \triangleq (r-s)/g$. Then, u is relatively prime with v. Also, for a given lag-τ, define $i \triangleq \lfloor \tau/g \rfloor$ and $d \triangleq \tau - ig$, so that $\tau = ig + d$.

Theorem 1: The magnitude of the cross-correlation function $\theta_N^{r,s}(\tau)$, $|\theta_N^{r,s}(\tau)|$, is given as

$$|\theta_N^{r,s}(\tau)| = \begin{cases} \sqrt{Ng}\delta_K(d), & N \text{ and } uv \text{ even, or } N \text{ odd} \\ \sqrt{Ng}\delta_K\left(d - \frac{g}{2}\right), & N \text{ even and } uv \text{ odd} \end{cases} \tag{2}$$

and the maximum magnitude of the cross-correlation function $\theta_N^{r,s}(\tau)$, $\hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s)$, is given as

$$\begin{aligned} \hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s) &= \max_{\tau} |\theta_N^{r,s}(\tau)| \\ &= \sqrt{Ng}. \end{aligned} \tag{3}$$

To prove Theorem 1, the following lemma may be useful.

Lemma 1: The squared magnitude of the cross-correlation function is given as

$$|\theta_N^{r,s}(\tau)|^2 = \begin{cases} N\sum_{m=0}^{g-1}(-1)^{m^2uv} W_g(-smd), & N \text{ even} \\ N\sum_{m=0}^{g-1}(-1)^{m(mu+1)v} W_g(-smd), & N \text{ odd.} \end{cases} \tag{4}$$

The proof of Lemma 1 is given in Appendix A and the proof of Theorem 1 is given as follows.

Proof of Theorem 1: First, consider the case where N and uv are even or N is odd. When N and uv are even, $(-1)^{m^2uv} = 1$ and when N is odd, u should be odd and $m(mu+1)v$ is even. Then, from Lemma 1, we obtain

$$|\theta_N^{r,s}(\tau)|^2 = N\sum_{m=0}^{g-1} W_g(-smd) \tag{5}$$

in both cases. Since $s \in \mathbf{R}_N$, s is relatively prime with g, which implies $\sum_{m=0}^{g-1} W_g(-smd) = g\delta_K(d)$. Thus, $|\theta_N^{r,s}(\tau)|^2 = Ng\delta_K(d)$.

Now, consider the case where N is even and uv is odd. Since $s \in \mathbf{R}_N$ and N is even, s should be odd. If m is odd, uvm is odd and $uvm+s$ is even, which implies $m(uvm+s)$ is always even. Thus, we can rewrite $|\theta_N^{r,s}(\tau)|^2$ from Lemma 1 as

$$\begin{aligned} \left|\theta_N^{r,s}\left(ig + \frac{g}{2} + d'\right)\right|^2 &= N\sum_{m=0}^{g-1}(-1)^{m(uvm+s)} W_g(-smd') \\ &= N\sum_{m=0}^{g-1} W_g(-smd') \\ &= Ng\delta_K\left(d - \frac{g}{2}\right) \end{aligned} \tag{6}$$

where $d' = d - g/2$, which concludes the proof. ■

III. Maximum Magnitude Distribution Function

Theorem 1 tells us that the maximum value of the cross-correlation function between $\boldsymbol{a}_N^r$ and $\boldsymbol{a}_N^s$ depends only on g. As shown in [17], when $r-s$ and N is relatively prime, i.e, $g=1$, $\hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s)$ meets the lower bound of $\sqrt{N}$. On the other hand, when $g = N$, $\hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s)$ becomes the largest value of N. However, it has not yet been investigated the entire distribution function $\rho_N(x)$ of $\mathbf{C}_N$ denoting the number of all pairs (r,s), $r, s \in \mathbf{R}_N$, satisfying $\hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s) = \sqrt{Nx}$.

A. Uniform Property

Definition 2: Any integer N can be represented as $N = \prod_{i=0}^{k-1} p_i^{c_i}$, where p_i denotes the $(i+1)^{\text{th}}$ smallest prime factor of N. Let's define $\mathbf{Z}_N \triangleq \{0, 1, \ldots N-1\}$, $\mathbf{I}(N) \triangleq \{i \,|p_i$ is the $(i+1)^{\text{th}}$ smallest prime factor of $N\}$ and $\mathbf{Z}_{N,x} \triangleq \{nx | n \in \mathbf{Z}_{N/x}\}$ for $x \in \mathbf{X}_N \triangleq \{\text{all divisors of } N\}$. Also, for any set of integers $\mathbf{A}$, define $\mathbf{D}_x(\mathbf{A}) \triangleq \{n - x | n \in \mathbf{A}\}$ and $\mathbf{G}_N^x(\mathbf{A}) \triangleq \{n | n \in \mathbf{A} \text{ and } \gcd(n, N) = x\}$.

From Theorem 1, $\hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s) = \sqrt{Ng}$. Also, for given N, $s \in \mathbf{R}_N$ and x, it is easily seen that $\mathbf{R}_N^s(x) \triangleq \mathbf{G}_N^x(\mathbf{D}_s(\mathbf{R}_N)) = \{r - s \,|\, \gcd(r-s, N) = x \text{ and } r \in \mathbf{R}_N\}$ is the set of differences between s and the indices of all Chu sequences satisfying $\hat{\theta}_N(\boldsymbol{a}_N^r, \boldsymbol{a}_N^s) = \sqrt{Nx}$. Then, $|\mathbf{R}_N^s(x)|$ denotes the number of the sequences in $\mathbf{C}_N$ whose maximum magnitude of the cross-correlation function with $\boldsymbol{a}_N^s$ is $\sqrt{Nx}$. The main result of this subsection is given in the following theorem.

Theorem 2: For any $r, s \in \mathbf{R}_N$, $|\mathbf{R}_N^r(x)| = |\mathbf{R}_N^s(x)|$. Thus, $\rho_N(x) = \phi(N)|\mathbf{R}_N^s(x)|$ for any $s \in \mathbf{R}_N$, where $\phi(N) \triangleq \prod_{i=0}^{k-1} p_i^{c_i-1}(p_i - 1)$ denotes the Euler's totient function [16] for a given $N = \prod_{i=0}^{k-1} p_i^{c_i}$.

Proof: See Appendix B. ■

B. Distribution

The maximum magnitude distribution function $\rho_N(x)$ is given in the following theorem.

Theorem 3: For $N = \prod_{i=0}^{k-1} p_i^{c_i}$, $\rho_N(x)$ is given as

$$\rho_N(x) = \begin{cases} \phi(N)\varphi_N(x)\xi_N(x), & x \in \mathbf{X}_N \\ 0, & x \notin \mathbf{X}_N \end{cases} \tag{7}$$

where $n_i(x)$ is the exponent of the $(i+1)^{\text{th}}$ prime factor p_i of x, i.e., $x = \prod_{i \in \mathbf{I}(x)} p_i^{n_i(x)}$ for $x \in \mathbf{X}_N$

$$\begin{aligned} &\varphi_N(x) \triangleq \\ &\begin{cases} \prod_{i \in \mathbf{I}(x)} \left(p_i^{c_i - n_i(x) - 1}(p_i - 1 + \delta_K(c_i - n_i(x)))\right), & \mathbf{I}(x) \neq \emptyset \\ 1, & \mathbf{I}(x) = \emptyset \end{cases} \\ &\zeta_N(x) \triangleq \begin{cases} \prod_{i \in \mathbf{Z}_k - \mathbf{I}(x)} \left(p_i^{c_i} - 2p_i^{c_i - 1}\right), & \mathbf{Z}_k - \mathbf{I}(x) \neq \emptyset \\ 1, & \mathbf{Z}_k - \mathbf{I}(x) = \emptyset. \end{cases} \end{aligned} \tag{8}$$

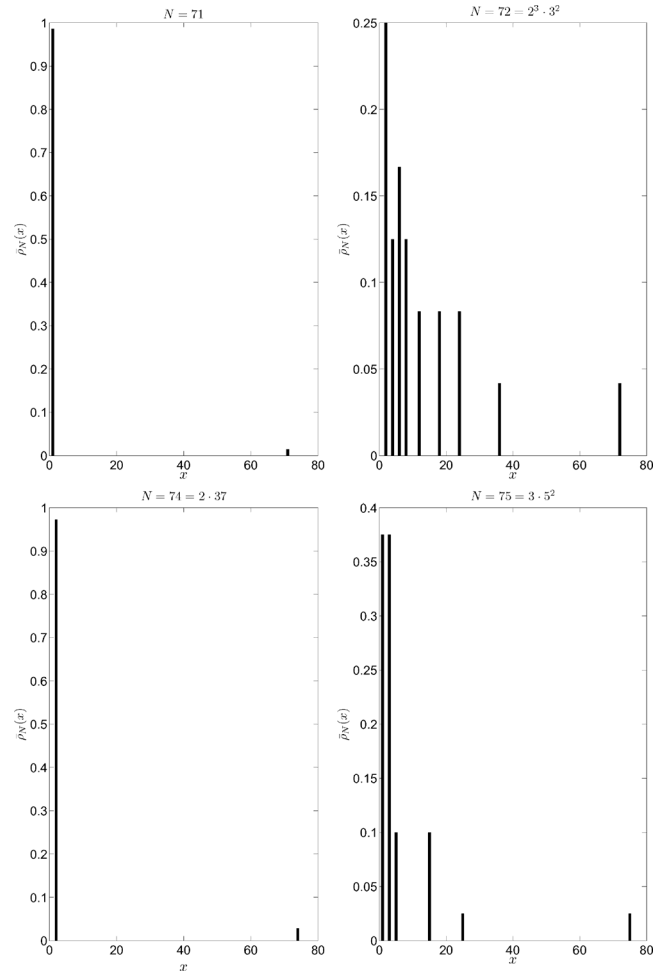

Fig. 1. Normalized distribution function, $\bar{\rho}_N(x) = \rho_N(x)/\phi^2(N)$, for $N = 71$, 72, 74, and 75.

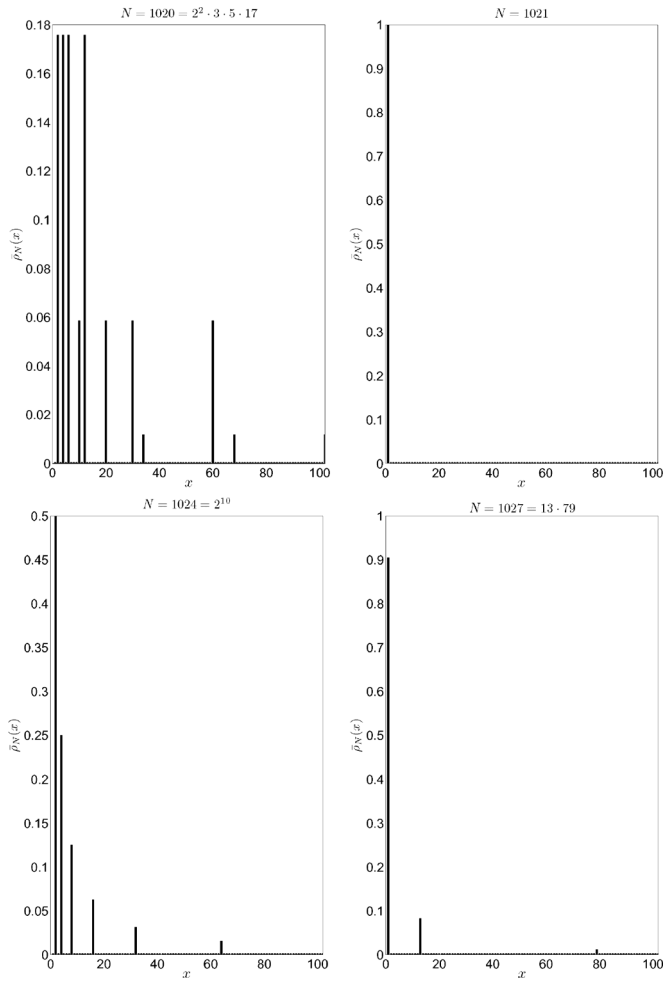

Fig. 2. Normalized distribution function, $\bar{\rho}_N(x) = \rho_N(x)/\phi^2(N)$, for $N = 1020$, 1021, 1024, and 1027.

Let $\bar{\mathbf{X}}_N \triangleq \{x | \rho_N(x) > 0\}$. Then, $\bar{\mathbf{X}}_N = \mathbf{X}_N$ and $\left|\bar{\mathbf{X}}_N\right| = \prod_{i \in \mathbf{Z}_k} (c_i + 1)$ when N is odd and $\bar{\mathbf{X}}_N = \{x | x \in \mathbf{X}_N,\ x \text{ is even}\}$ and $\left|\bar{\mathbf{X}}_N\right| = c_0 \prod_{i \in \mathbf{Z}_k - \{0\}} (c_i + 1)$.

Proof: See Appendix C. ■

Note that $\rho_N(N) = \prod_{i=0}^{k-1} p_i^{c_i - 1}(p_i - 1) = \phi(N)$ denotes the number of all possible auto-correlation functions (i.e., the number of sequences) and $\rho_N(x)$, $0 < x < N$, denotes the number of all cross-correlation functions (i.e., the number of sequence pairs) with the maximum magnitude of $\sqrt{Nx}$. Figs. 1 and 2 respectively compare the normalized distribution function $\bar{\rho}_N(x) = \rho_N(x)/\phi^2(N)$ for $N = 71, 72, 74, 75$ and $N = 1020, 1021, 1024, 1027$. As expected from Theorem 3, for $N = 71, 1021$, $\bar{\rho}_N(x)$ is concentrated at $x = 1$ except $x = N$ and for $N = 74 = 2 \cdot 37$, $\bar{\rho}_N(x)$ is concentrated at $x = 2$ except $x = N$. On the other hand, for $N = 72 = 2^3 \cdot 3^2$, $N = 75 = 3 \cdot 5^2$, $N = 1020 = 2^2 \cdot 3 \cdot 5 \cdot 17$, $N = 1024 = 2^{10}$ and $N = 1027 = 13 \cdot 79$, $\bar{\rho}_N(x)$ is spread over 9, 6, 16, 10, and 4 divisors, respectively.

IV. Maximum Number of Available Chu Sequences

In this section, the maximum number of available Chu sequences satisfying a given maximum magnitude of the cross-correlation is investigated. The main result is given in Theorem 4.

Definition 3: For $\sqrt{N} \le \theta \le N$, define $\mathbf{C}_N(\theta) \triangleq \{\mathbf{C}_N(\mathbf{\Lambda}) | \mathbf{\Lambda} \in \mathbf{\Xi}_N(\theta)\}$ as the collection of all partial Chu sequence sets when the maximum magnitude of the cross-correlation function is constrained to be less than θ and $\lambda_N(\theta) \triangleq \max_{\mathbf{C} \in \mathbf{C}_N(\theta)} |\mathbf{C}|$ as the maximum number of available Chu sequences at given θ.

Definition 4: For $N = \prod_{i=0}^{k-1} p_i^{c_i}$ and $\sqrt{N} \le \theta \le N$, define $\mathbf{X}_N(\theta) \triangleq \left\{x \middle| \frac{\theta^2}{N} \le x < \frac{p_0 \theta^2}{N}, x \in \mathbf{X}_N\right\}$, $x_N(\theta) \triangleq \max\left\{\arg\min_{x \in \mathbf{X}_N(\theta)} \phi(x)\right\}$, $\mathbf{Q}_N^c(\theta) \triangleq \{n \mid c \le n < c + x_N(\theta), n \in \mathbf{R}_N\}$ and $\mathbf{Y}_N^c(\theta) \triangleq \left\{n \middle| \gcd(m-n, N) < \frac{\theta^2}{N}\right.$ for any $m \in \mathbf{Q}_N^c(\theta), n \in \mathbf{R}_N - \mathbf{Q}_N^c(\theta)\left.\right\}$.

Definition 5: Define $\mathbf{\Psi}_N^r(\theta) \triangleq \left\{\mathbf{Y} \middle| \gcd(m-n, N) < \frac{\theta^2}{N}\right.$ for any $m, n \in \mathbf{Y}, \mathbf{Y} \subset \mathbf{Y}_N^r(\theta)\left.\right\}$, $\hat{\mathbf{\Xi}}_N(\theta) \triangleq \{\mathbf{Q}_N^r(\theta) \cup \mathbf{Y} | r \in$

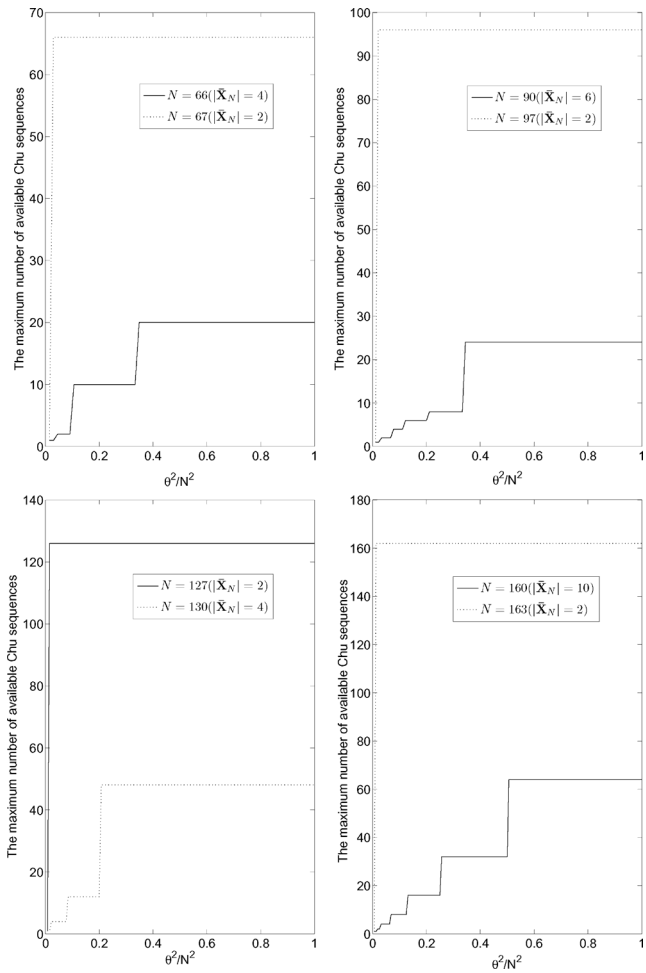

Fig. 3. Maximum number of available Chu sequences, $\hat{\boldsymbol{\lambda}}_N(\theta)$, $N \approx 64$, 96, 128, and 160.

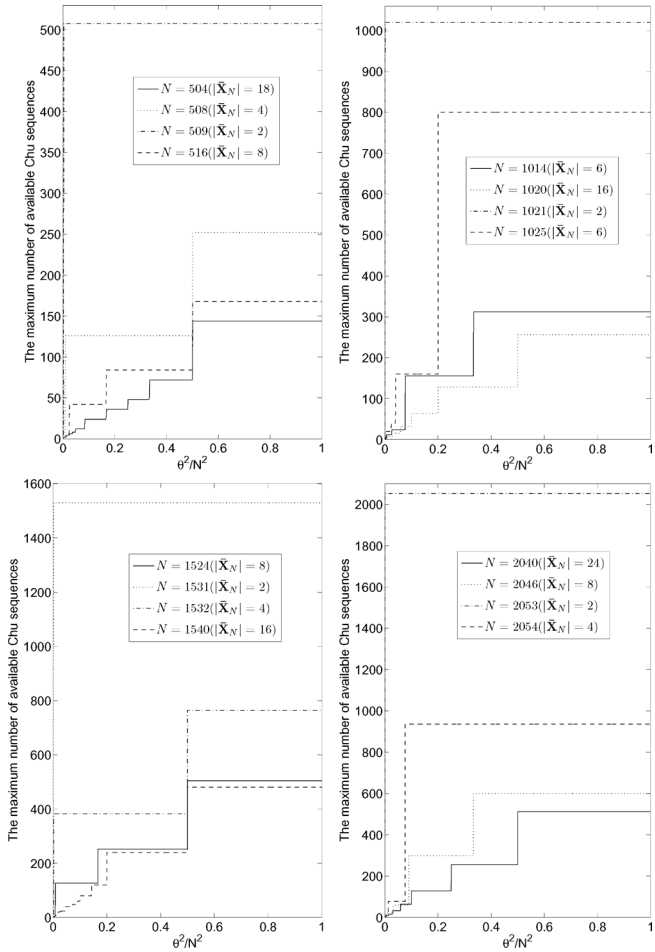

Fig. 4. Maximum number of available Chu sequences, $\hat{\boldsymbol{\lambda}}_N(\theta)$, $N \approx 512$, 1024, 1536, and 2048.

$\mathbf{R}_N, \mathbf{Y} \in \boldsymbol{\Psi}_N^r(\theta)\}$, $\hat{\boldsymbol{\Lambda}}_N(\theta) \triangleq \underset{\boldsymbol{\Lambda}\in\hat{\boldsymbol{\Xi}}_N(\theta)}{\arg\max} |\boldsymbol{\Lambda}|$ and $\hat{\lambda}_N(\theta) \triangleq \left|\hat{\boldsymbol{\Lambda}}_N(\theta)\right|$.

Note that although finding $\lambda_N(\theta)$ requires an exponential complexity of N, we can construct $\hat{\boldsymbol{\Lambda}}_N(\theta)$ and calculate $\hat{\lambda}_N(\theta)$ in a polynomial complexity of N so that $\hat{\boldsymbol{\Lambda}}_N(\theta)$ and $\hat{\lambda}_N(\theta)$ can be easily found via computer search.

Theorem 4: For a given $\sqrt{N} \le \theta \le N$, $\hat{\lambda}_N(\theta) \le \lambda_N(\theta) \le \phi(x_N(\theta))$.

Proof: Consider the upper bound part. For $x \in \mathbf{X}_N(\theta)$, $\boldsymbol{\Lambda} \cap \mathbf{D}_{-c}(\mathbf{Z}_{N,x}) \le 1$ for any $\boldsymbol{\Lambda} \in \boldsymbol{\Xi}_N(\theta)$ and any integer c because the difference of any two distinct elements in $\mathbf{D}_{-c}(\mathbf{Z}_{N,x})$ is an integer multiple of x and then the GCD between its difference and N is at least x. Suppose that $n \in \mathbf{Z}_x - \mathbf{R}_x$. Since $\gcd(n, N) \neq 1$, $\mathbf{D}_{-n}(\mathbf{Z}_{N,x})$ and $\mathbf{R}_N$ are mutually exclusive so that $\boldsymbol{\Lambda} \cap \mathbf{D}_{-n}(\mathbf{Z}_{N,x}) = \emptyset$. Also, when $n \in \mathbf{R}_x$, we can pick at most one element in $\mathbf{D}_{-n}(\mathbf{Z}_{N,x})$, which proves $\lambda_N(\theta) \le \phi(x_N(\theta))$. The lower bound part is straightforward since $\hat{\boldsymbol{\Xi}}_N(\theta) \subset \boldsymbol{\Xi}_N(\theta)$, which concludes the proof. ■

In order to show that the bounds in Theorem 4 are very tight, we constructed $\hat{\boldsymbol{\Lambda}}_N(\theta)$ and obtained $\hat{\lambda}_N(\theta)$ using computer search for $\theta^2/N \in \{0.05k | 1 \le k \le 10\}$ and the length of N from 21 up to 3000, compared the lower bound $\hat{\lambda}_N(\theta)$ to the upper bound $\phi(x_N(\theta))$ and found that both bounds are equal in 99.98% among all 29800 cases with only three exceptional cases of $\left(N = 1575,\ \theta^2/N^2 = 0.1, \hat{\lambda}_N(\theta) = 118, \phi(x_N(\theta)) = 120\right)$, $\left(N = 2079, \theta^2/N^2 = 0.05, \hat{\lambda}_N(\theta) = 107, \phi(x_N(\theta)) = 108\right)$ and $\left(N = 2520, \theta^2/N^2 = 0.05, \hat{\lambda}_N(\theta) = 34, \phi(x_N(\theta)) = 36\right)$. In Figs. 3 and 4, $\hat{\lambda}_N(\theta)$ is plotted for $N \approx 64, 96, 128, 160, 512, 1024, 1536$ and 2048, which shows that $\hat{\lambda}_N(\theta)\,(\approx \lambda_N(\theta))$ increases step-wisely. For similar size of N, the number of the steps increases while the height of each steps decreases as the number of divisors increases.

V. Conclusions

In this paper, we investigated detailed cross-correlation properties for Chu sequences and obtained that i) the possible values of the magnitude of the cross-correlation function $\theta_N^{r,s}(\tau)$ depends only on the GCD between N and $r - s$, ii) the maximum magnitude distribution function among a given Chu sequence set in a closed form as in Theorem 3, which shows that the maximum magnitude distribution tends to spread out as the number of divisors increases, and iii) the upper and lower bounds on

the maximum number of available Chu sequences satisfying a given cross-correlation constraint and the corresponding partial Chu sequence set construction algorithm. Numerical examples show that the proposed bounds are quite tight and the proposed construction algorithm is near-optimal up to fairly large value of N.

APPENDIX

A) Proof of Lemma 1: When N is an even number, we can rewrite $\theta_N^{r,s}(\tau)$ as

$$\theta_N^{r,s}(\tau) = \sum_{k=0}^{N-1} W_N\left(\frac{rk^2}{2}\right) W_N\left(-\frac{s(k+\tau)^2}{2}\right) = W_N\left(-\frac{s\tau^2}{2}\right) \sum_{k=0}^{N-1} W_u\left(\frac{vk^2}{2} - \frac{sk(ig+d)}{g}\right). \quad (9)$$

Then, the squared magnitude, $|\theta_{r,s}(\tau)|^2$, is given as

$$|\theta_N^{r,s}(\tau)|^2 = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} W_u\left(\frac{vk^2}{2} - \frac{sk(ig+d)}{g}\right) W_u\left(\frac{sl(ig+d)}{g} - \frac{vl^2}{2}\right). \quad (10)$$

Here, $r-s$ is even when N is even because both r and s should be odd and each summand in (10) is periodic with N because the last term in (10) is periodic with period N as follows.

$$W_u\left(\frac{s(l+N)(ig+d)}{g} - \frac{v(l+N)^2}{2}\right) = W_u\left(\frac{sl(ig+d)}{g} - \frac{vl^2}{2}\right) W_2(-vgN) = W_u\left(\frac{sl(ig+d)}{g} - \frac{vl^2}{2}\right). \quad (11)$$

Then, (10) can be rewritten as

$$\begin{aligned}|\theta_N^{r,s}(\tau)|^2 &= \sum_{k=0}^{N-1} W_u\left(\frac{v(k+l)^2}{2} - \frac{s(k+l)(ig+d)}{g}\right) \sum_{l=0}^{N-1} W_u\left(\frac{sl(ig+d)^2}{g} - \frac{vl^2}{2}\right) \\ &= \sum_{k=0}^{N-1} W_u\left(\frac{vk^2}{2} - \frac{sk(ig+d)}{g}\right) \sum_{l=0}^{N-1} W_u(vkl) \\ &= \sum_{p=0}^{u-1}\sum_{m=0}^{g-1} W_u\left(\frac{v(mu+p)^2}{2} - \frac{s(mu+p)(ig+d)}{g}\right) \sum_{l=0}^{N-1} W_u(vl(mu+p)) \\ &= N\sum_{m=0}^{g-1} W_1\left(\frac{m^2uv}{2} - \frac{sm(ig+d)}{g}\right) \\ &= N\sum_{m=0}^{g-1} (-1)^{m^2uv} W_g(-smd) \end{aligned} \quad (12)$$

where the fourth equality comes from the fact that $\sum_{l=0}^{N-1} W_u(vl(mu+p)) = \sum_{l=0}^{N-1} W_u(plv) = N\delta_K(p)$ because u is relatively prime with v.

When N is an odd number, we can rewrite $|\theta_{r,s}(\tau)|^2$ similarly as

$$|\theta_N^{r,s}(\tau)|^2 = \sum_{k=0}^{N-1}\sum_{l=0}^{N-1} W_u\left(\frac{v\left(k^2+k\right)}{2} - \frac{sk(ig+d)}{g}\right) W_u\left(\frac{sl(ig+d)}{g} - \frac{v\left(l^2+l\right)}{2}\right). \quad (13)$$

Here, the last term is again periodic with period N and (13) can be similarly rewritten as

$$\begin{aligned}|\theta_N^{r,s}(\tau)|^2 &= \sum_{k=0}^{N-1} W_u\left(\frac{v\left(k^2+k\right)}{2} - \frac{sk(ig+d)}{g}\right) \sum_{l=0}^{N-1} W_u(vkl) \\ &= N\sum_{m=0}^{g-1} W_1\left(\frac{m(mu+1)v}{2} - \frac{sm(ig+d)}{g}\right) \\ &= N\sum_{m=0}^{g-1} (-1)^{m(mu+1)v} W_g(-smd) \end{aligned} \quad (14)$$

which concludes the proof.

B) Proof of Theorem 2: The following lemmas are useful for the proof of Theorem 2.

Lemma B-1: Let $\mathbf{Z}_N^c(x) \triangleq \mathbf{G}_N^x(\mathbf{D}_c(\mathbf{Z}_N))$. Then, for any two different integers c and c', $\mathbf{Z}_N^c(x) = \mathbf{Z}_N^{c'}(x)$ because $\{\gcd(-c+1,N), \ldots, \gcd(-c+N,N)\} = \{\gcd(1,N), \ldots, \gcd(N,N)\}$.

Lemma B-2: Let a and b be positive integers satisfying $\gcd(a,b)=1$. Then, for a positive integer m, $\mathbf{B} = \{na-c \,|\, k \le n < k+mb\}$, where k is an arbitrary integer, contains m integer multiples of b.

Proof: The i^{th} element of $\mathbf{B}$, $e_i = (k+i-1)a - c$, can be represented as $e_i = q_i b + r_i$, where $q_i = \lfloor e_i/b \rfloor$ and $r_i = e_i \bmod b$ are uniquely determined from e_i[21]. Let $\{\mathbf{B}^r \,|\, r \in \mathbf{Z}_m\}$ be the partition of $\mathbf{B}$, where $\mathbf{B}^r = \{e_i \,|\, rb \le i < (r+1)b\}$. Then, each $\mathbf{B}^r$ contains exactly one integer multiple of b since $\{r_i | rb \le i < (r+1)b\} = \mathbf{Z}_b$, which concludes the proof. ■

Then, the proof of Theorem 2 is now given as follows.

Proof of Theorem 2: Let $\mathbf{L}_N^s(x) \triangleq \mathbf{G}_N^x(\mathbf{D}_s(\mathbf{Z}_N)) - \mathbf{G}_N^x(\mathbf{D}_s(\mathbf{R}_N)) = \mathbf{Z}_N^s(x) - \mathbf{R}_N^s(x)$. Then, $|\mathbf{R}_N^s(x)| = |\mathbf{Z}_N^s(x)| - |\mathbf{L}_N^s(x)|$. When $x \notin \mathbf{X}_N$, $\mathbf{R}_N^s(x) = 0$ regardless of s because $x \ne \gcd(N,r)$ for any integer $r \in \mathbf{R}_N^s$. Thus, $|\mathbf{R}_N^r(x)| = |\mathbf{R}_N^s(x)| = 0$. When $x \in \mathbf{X}_N$, $|\mathbf{L}_N^s(x)|$ can be rewritten for a given $N = \prod_{i=0}^{k-1} p_i^{c_i}$ as

$$|\mathbf{L}_N^s(x)| = \sum_{i=0}^{k-1} |\mathbf{G}_N^x(\mathbf{D}_s(\mathbf{Z}_{N,p_i}))| - \sum_{i_0=0}^{k-2}\sum_{i_1=i_0+1}^{k-1} \left|\mathbf{G}_N^x\left(\mathbf{D}_s\left(\mathbf{Z}_{N,p_{i_0}} \cap \mathbf{Z}_{N,p_{i_1}}\right)\right)\right| + \cdots$$

$$+(-1)^{k-2}\sum_{i_0=0}^{1}\sum_{i_1=i_0+1}^{2}\cdots\sum_{i_{k-1}=i_{k-2}+1}^{k-1}\left|\mathbf{G}_N^x\left(\mathbf{D}_s\left(\bigcap_{m=0}^{k-2}\mathbf{Z}_{N,p_{i_m}}\right)\right)\right|$$
$$+(-1)^{k-1}\left|\mathbf{G}_N^x\left(\mathbf{D}_s\left(\bigcap_{i=0}^{k-1}\mathbf{Z}_{N,p_i}\right)\right)\right|. \quad (15)$$

If $\gcd(x,p_i)=1$, there always exist $N/(p_i x)$ integer multiples of x among the elements in $\mathbf{D}_s(\mathbf{Z}_{N,p_i})$ from Lemma B-2. If $\gcd(x,p_i)\neq 1$, p_i should be a divisor of x since p_i is a prime number. Thus, there is no integer multiple of x among the elements in $\mathbf{D}_s(\mathbf{Z}_{N,p_i})$ since s is relatively prime with p_i. Thus, $\mathbf{G}_N^x(\mathbf{D}_s(\mathbf{Z}_{N,p_i}))$ does not depend on s as long as $s\in\mathbf{R}_N$. Let $\mathbf{M}$ be an arbitrary subset of $\mathbf{Z}_k$ and m_i denote the $(i+1)^{\text{th}}$ smallest element of $\mathbf{M}$. Then, for a given index set $\mathbf{M}$, $\mathbf{D}_s\left(\bigcap_{i=0}^{|\mathbf{M}|-1}\mathbf{Z}_{N,p_{m_i}}\right)=\{nl-s\,|\,0\le n<N/l\}$, where $l=\prod_{i=0}^{|\mathbf{M}|-1}p_{m_i}$. Similarly, if $\gcd(x,l)=1$, there exist $N/(lx)$ integer multiples of x among the elements in $\mathbf{D}_s\left(\bigcap_{i=0}^{|\mathbf{M}|-1}\mathbf{Z}_{N,p_{m_i}}\right)$ from Lemma B-2 and if $\gcd(x,l)\neq 1$, x should be an integer multiple of p_{m_i} for some $m_i\in\mathbf{M}$. Since s is relatively prime with all p_{m_i}, $m_i\in\mathbf{M}$, there is no integer multiple of x in $\mathbf{D}_s\left(\bigcap_{i=0}^{|\mathbf{M}|-1}\mathbf{Z}_{N,p_{m_i}}\right)$. Thus, $\mathbf{G}_N^x\left(\mathbf{D}_s\left(\bigcap_{i=0}^{|\mathbf{M}|-1}\mathbf{Z}_{N,p_{m_i}}\right)\right)$ does not depend on s as long as $s\in\mathbf{R}_N$. Thus, from (15), $|\mathbf{L}_N^r(x)|=|\mathbf{L}_N^s(x)|$ for any $r,s\in\mathbf{R}_N$. Also, since $|\mathbf{Z}_N^r(x)|=|\mathbf{Z}_N^s(x)|$ from Lemma B-1, $|\mathbf{R}_N^s(x)|$ does not depend on s as long as $s\in\mathbf{R}_N$. Since $|\mathbf{R}_N|=\phi(N)$, $\rho_N(x)=\phi(N)\,|\mathbf{R}_N^s(x)|$. ■

C) Proof of Theorem 3:

Lemma C-1: When $N=p^c$, $\rho_N(x)$ is given as

$$\rho_N(x)=\begin{cases}\phi(N)p^{c-n(x)-1}(p-1+\delta_K(c-n(x))), & \text{if } x=p^{n(x)},\ 0<n(x)\le c\\ \phi(N)\left(p^c-2p^{c-1}\right), & \text{if } x=1\\ 0, & \text{otherwise.}\end{cases} \quad (16)$$

Proof: When $x=N$, $\mathbf{R}_N^s(N)=\{r-s|\gcd(r-s,N)=N, r\in\mathbf{R}_N\}=\{0\}$, which implies $|\mathbf{R}_N^s(x)|=1$. When $x=p^{n(x)}$, $0<n(x)<c$, $\mathbf{R}_N^s\left(p^{n(x)}\right)=\{r-s|\gcd(r-s,N)=p^{n(x)}, r\in\mathbf{R}_N\}=\{r-s|r=mp^{n(x)}+s, m\in\mathbf{Z}_{p^{c-n(x)}}, \gcd(m,p)=1\}$. Since there are $p^{c-n(x)-1}$ integer multiples of p in $\mathbf{Z}_{p^{c-n(x)}}$, $\left|\mathbf{R}_N^s\left(p^{n(x)}\right)\right|=p^{c-n(x)}-p^{c-n(x)-1}$. When $x=1$, $|\mathbf{R}_N^s(1)|=\{\,r-s\,|\,\gcd(r-s,N)=1, r\in\mathbf{R}_N\}$. Note that $|\mathbf{R}_N^s(1)|=|\mathbf{R}_N|-\sum_{x=2}^{N}|\mathbf{R}_N^s(x)|=|\mathbf{R}_N|-\sum_{i=1}^{c}\left|\mathbf{R}_N^s\left(p^i\right)\right|$. Since $|\mathbf{R}_N|=\phi(p^c)=p^c-p^{c-1}$, $|\mathbf{R}_N^s(1)|=p^c-p^{c-1}-\sum_{i=1}^{c-1}(p^{c-i}-p^{c-i-1})-1=p^c-2p^{c-1}$.

Then, the sketch of the proof of Theorem 3 is as follows. When $k=1$, (7) holds from Lemma C-1. Suppose that (7) holds for $x\in\mathbf{X}_N$ when $k=K$ and let $N'=Np_K^{c_K}$. Then, the set of all divisors of N' can be written as $\{y=xp_K^l|x\in\mathbf{X}_N,\,0\le l\le c_K\}$. Note that $\mathbf{R}_{N'}=\{n|n\in\mathbf{Z}_{N'},\gcd(n,N')=1\}=\mathbf{G}_{p_K}^1\left(\bigcup_{n\in\mathbf{R}_N}\mathbf{D}_{-n}\left(\mathbf{Z}_{N',N}\right)\right)$ and $\mathbf{G}_N^x\left(\mathbf{D}_s\left(\bigcup_{n\in\mathbf{R}_N}\mathbf{D}_{-n}(\mathbf{Z}_{N',N})\right)\right)=\bigcup_{n\in\mathbf{R}_N^s(x)}\mathbf{D}_{-n}\left(\mathbf{Z}_{N',N}\right)$ because $\gcd(mN+x,N)=\gcd(x,N)=x$ for any integer m. Let $y=xp_K^l$, $0\le l\le c_K$, and $\mathbf{V}_n(a,b)\triangleq\mathbf{G}_a^b(\mathbf{D}_{-n}(\mathbf{Z}_{N',N}))$. Then, $\mathbf{R}_{N'}^s(y)$ can be rewritten as

$$\begin{aligned}\mathbf{R}_{N'}^s(y)&=\mathbf{G}_{N'}^y\left(\mathbf{D}_s\left(\mathbf{R}_{N'}\right)\right)\\&=\mathbf{G}_{N'}^y\left(\mathbf{D}_s\left(\mathbf{G}_{p_K}^1\left(\bigcup_{n\in\mathbf{R}_N}\mathbf{D}_{-n}\left(\mathbf{Z}_{N',N}\right)\right)\right)\right)\\&=\mathbf{D}_s\left(\left(\mathbf{G}_{p_K}^1\left(\mathbf{D}_{-s}\left(\mathbf{G}_{N'}^y\left(\mathbf{D}_s\left(\bigcup_{n\in\mathbf{R}_N}\mathbf{D}_{-n}\left(\mathbf{Z}_{N',N}\right)\right)\right)\right)\right)\right)\right)\\&=\mathbf{D}_s\left(\mathbf{G}_{p_K}^1\left(\mathbf{D}_{-s}\left(\mathbf{G}_{N'/N}^{p_K^l}\left(\mathbf{G}_N^x\left(\mathbf{D}_s\left(\bigcup_{n\in\mathbf{R}_N}\mathbf{D}_{-n}(\mathbf{Z}_{N',N})\right)\right)\right)\right)\right)\right)\\&=\mathbf{D}_s\left(\mathbf{G}_{p_K}^1\left(\mathbf{D}_{-s}\left(\mathbf{G}_{N'/N}^{p_K^l}\left(\bigcup_{n\in\mathbf{R}_N^s(x)}\mathbf{D}_{-n}\left(\mathbf{Z}_{N',N}\right)\right)\right)\right)\right)\\&=\mathbf{D}_s\left(\mathbf{G}_{p_K}^1\left(\mathbf{D}_{-s}\left(\bigcup_{n\in\mathbf{R}_N^s(x)}\mathbf{V}_n\left(p_K^{c_K},p_K^l\right)\right)\right)\right)\\&=\bigcup_{n\in\mathbf{R}_N^s(x)}\mathbf{V}_n\left(p_K^{c_K},p_K^l\right)\\&\quad-\mathbf{D}_s\left(\mathbf{G}_{p_K}^{p_K}\left(\mathbf{D}_{-s}\left(\bigcup_{n\in\mathbf{R}_N^s(x)}\mathbf{V}_n\left(p_K^{c_K},p_K^l\right)\right)\right)\right). \quad (17)\end{aligned}$$

When $y=x$, (i.e., $l=0$), $\mathbf{G}_{p_K}^{p_K}(\mathbf{D}_{-s}(\mathbf{V}_n(p_K^{c_K},1)))$ can be written as

$$\begin{aligned}&\mathbf{G}_{p_K}^{p_K}\left(\mathbf{D}_{-s}\left(\mathbf{V}_n\left(p_K^{c_K},1\right)\right)\right)\\&=\mathbf{G}_{p_K}^{p_K}\left(\mathbf{D}_{-s}\left(\mathbf{G}_{p_K^{c_K}}^1\left(\mathbf{D}_{-n}\left(\mathbf{Z}_{N',N}\right)\right)\right)\right)\\&=\mathbf{D}_{-s}\left(\mathbf{G}_{p_K^{c_K}}^1\left(\mathbf{D}_s\left(\mathbf{G}_{p_K}^{p_K}\left(\mathbf{D}_{-n-s}\left(\mathbf{Z}_{N',N}\right)\right)\right)\right)\right)\\&=\mathbf{D}_{-s}\left(\mathbf{D}_s\left(\mathbf{G}_{p_K}^{p_K}\left(\mathbf{D}_{-n-s}\left(\mathbf{Z}_{N',N}\right)\right)\right)\right)\\&=\mathbf{V}_{n+s}\left(p_K,p_K\right)\end{aligned} \quad (18)$$

where the third equality comes from the fact that $\gcd\left(mp_K-s,p_K^{c_K}\right)=1$ for $s\in\mathbf{R}_{N'}$. From Lemma B-2, it is easily seen that $|\mathbf{V}_n(p_K^{c_K},1)|=p_K^{c_K}-p_K^{c_K-1}$ and $|\mathbf{V}_{n+s}(p_K,p_K)|=p_K^{c_K-1}$ when $y=x$ since there exist $p_K^{c_K-1}$ integer multiples of p_K in $\mathbf{D}_c(\mathbf{Z}_{N',N})$. Note that $\varphi_{N'}(y)=\varphi_{N'/N}(y/x)\,\varphi_N(x)$ and $\zeta_{N'}(y)=\zeta_{N'/N}(y/x)\,\zeta_N(x)$. Thus, when $y=x$, $|\mathbf{R}_{N'}^s(y)|$ is given as

$$\begin{aligned}|\mathbf{R}_{N'}^s(y)|&=\left(p_K^{c_K}-p_K^{c_K-1}\right)\varphi_N(x)\xi_N(x)-p_K^{c_K-1}\varphi_N(x)\xi_N(x)\\&=\varphi_{N'}(y)\,\xi_{N'}(y)\end{aligned} \quad (19)$$

because $\varphi_{N'/N}(y/x) = \varphi_{p_K^{c_K}}(1) = 1$, $\zeta_{N'/N}(y/x) = \zeta_{p_K^{c_K}}(1) = p_K^{c_K} - 2p_K^{c_K-1}$ so that $\varphi_{N'}(y) = \varphi_N(x)$ and $\xi_{N'}(y) = \left(p_K^{c_K} - 2p_K^{c_K-1}\right)\xi_N(x)$. When $y = xp_k^l$, $0 < l \leq c_k$, $|\mathbf{V}_n(p_K^{c_K}, p_K^{c_l})| = p_K^{c_K-l} - p_K^{c_K-l-1}$ similarly from Lemma B-2 and $\mathbf{G}_{p_K}^{p_K}\left(\mathbf{D}_{-s}\left(\mathbf{V}_n\left(p_K^{c_K}, p_K^{l}\right)\right)\right) = \emptyset$ since $\gcd\left(mp_K^l + s, p_K\right) = 1$ for $s \in \mathbf{R}_{N'}$. Thus, $|\mathbf{R}_{N'}^s(y)|$ is given as

$$\begin{aligned}|\mathbf{R}_{N'}^s(y)| &= \left(p_K^{c_K-l} - p_K^{c_K-l-1}\right)\varphi_N(x)\,\xi_N(x) \\ &= \varphi_{N'}(y)\,\xi_{N'}(y) \end{aligned} \tag{20}$$

because $\varphi_{N'/N}(y/x) = \varphi_{p_K^{c_K}}\left(p_K^l\right) = p_K^{c_K-l} - p_K^{c_K-l-1}$, $\zeta_{N'/N}(y/x) = \zeta_{p_K^{c_K}}\left(p_K^l\right) = 1$ so that $\varphi_{N'}(y) = \left(p_K^{c_K-l} - p_K^{c_K-l-1}\right)\varphi_N(x)$ and $\xi_{N'}(y) = \xi_N(x)$.

Finally from (8), $\rho_N(x) > 0$ as long as $x \in \mathbf{X}_N$ and $c_0 \neq 2$ (i.e., N is odd). When $c_0 = 2$ (i.e., N is even), $\rho_N(x) = 0$ for $x \in \{\text{odd divisors of } N\}$, which concludes the proof. ■

REFERENCES

[1] D. V. Sarwate, "Bounds on correlation and autocorrelation of sequences," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 6, pp. 720–724, Nov. 1979.

[2] 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.

[3] V. M. Sidelnikov, "On mutual correlation of sequences," *Soviet Math. Doklady*, vol. 12, no. 3, pp. 197–201, 1971.

[4] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code division multiple-access systems," in *Sequences II, Methods in Communications, Security and Computer Science*. New York: Springer-Verlag, 1993.

[5] S. Waldron, "Generalized Welch bound equality sequences are tight frames," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2307–2309, Sep. 2003.

[6] T. Kasami, *Weight Distribution Formula for Some Class of Cyclic Codes,* Coordinated Science Lab., Univ. Illinois Urbana-Champaign, 1966, Tech. Rep. R285.

[7] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154–156, Jan. 1968.

[8] R. L. Frank and S. A. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inf. Theory*, vol. 8, no. 6, pp. 381–382, Oct. 1962.

[9] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 4, pp. 531–532, Jul. 1972.

[10] S. Bozta, R. Hammons, and P. V. Kummer, "4-phase sequences with near optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 1101–1113, May 1992.

[11] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, no. 5, pp. 593–619, May 1980.

[12] P. Fan, M. Darnell, and F. Fan, *Sequence Design for Communications Applications*, 1st ed. New York: Taylor & Francis, 1996.

[13] A. M. D. Turkmani and U. S. Goni, "Performance evaluation of maximal-length, Gold and Kasami codes as spreading sequences in CDMA systems," in *Proc. Int. Conf. Universal Personal Commun.*, Ottawa, ON, Canada, Oct. 1993, vol. 2, pp. 970–974.

[14] J. Choi, J. Lee, J. P. Choi, and H. Lou, "Low-complexity mean-delay estimation for OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3790–3795, Sep. 2009.

[15] J. W. Kang, Y. Whang, H. Y. Lee, and K. S. Kim, "Optimal pilot sequence design for multi-cell MIMO-OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3354–3367, Oct. 2011.

[16] D. M. Burton, *Elementary Number Theory*, 2nd ed. Boston, MA: Allyn and Bacon, 1980.

[17] B. M. Popovic, "Generalized chirp-like polyphase sequences with optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1406–1409, Jul. 1992.

[18] Y. Liu and P. Fan, "Modified Chu sequences with smaller alphabet size," *Electron. Lett.*, vol. 40, no. 10, pp. 598–599, May 2004.

[19] L. Liru and V. K. Dubey, "Extended orthogonal polyphase codes for multicarrier CDMA System," *IEEE Commun. Lett.*, vol. 8, no. 12, pp. 700–702, Dec. 2004.

[20] D. Y. Peng and P. Z. Fan, "Generalized Sarwate bounds on the periodic autocorrelation and crosscorrelations of binary sequences," *Electron. Lett.*, vol. 38, no. 24, pp. 1521–1523, Nov. 2002.

[21] R. Kwiatek and G. Zwara, "The divisibility of integers and integer relatively primes," *Formalized Math.*, vol. 1, no. 5, pp. 855–866, Nov. 1990.

Jae Won Kang was born in Daegu, Korea, on August 7, 1979. He received the B.S., and M.S.E. in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in February 2003 and February 2005, respectively.

He is currently working towards his Ph.D. degree the Department of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea. His research interests include sequence design, channel estimation, and compressive sensing.

Younghoon Whang was born in Seoul, Korea, on March 12, 1980. He received the B.S. and M.S.E. in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in February 2004 and February 2009, respectively.

He is currently working towards his Ph.D. degree with the School of Electrical Engineering and Computer Science at the Oregon State University, Corvallis, USA. His research interests include OFDM techniques, MIMO systems, and the security in cooperative relay and cognitive radio network.

Byung Hoon Ko was born in Goheung, Korea, on June 20, 1979. He received the B.S. in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in February 2007.

He is currently working towards his Ph.D. degree the Department of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea. His research interests include cooperative communication, wireless ad hoc network and cross layer optimization.

Kwang Soon Kim (M'95–SM'04) was born in Seoul, Korea, on September 20, 1972. He received the B.S. (summa cum laude), M.S.E., and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea, in February 1994, February 1996, and February 1999, respectively.

From March 1999 to March 2000, he was with the Department of Electrical and Computer Engineering, University of California at San Diego, La Jolla, CA, U.S.A., as a Postdoctoral Researcher. From April 2000 to February 2004, he was with the Mobile Telecommunication Research Laboratory, Electronics and Telecommunication Research Institute, Daejeon, Korea as a Senior Member of Research Staff. Since March 2004, he has been with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul, Korea, now is an Associate Professor.

Prof. Kim has served as an Editor of the Journal of Communications and Networks (JCN) since 2008, and as an Editor of the IEEE Transactions on Wireless Communications since 2009. Prof. Kim was a recipient of the Postdoctoral Fellowship from Korea Science and Engineering Foundation (KOSEF) in 1999. He received the Outstanding Researcher Award from Electronics and Telecommunication Research Institute (ETRI) in 2002 and Jack Neubauer Memorial Award (Best system paper award, IEEE Transactions on Vehicular Technology) from IEEE Vehicular Technology Society in 2008. His research interests include communication theory, channel coding, multiuser/multicell MIMO, capacity and cross-layer optimization of wireless ad-hoc networks and heterogeneous cellular networks.