On Designing Sequences With Impulse-Like Periodic Correlation

Petre Stoica, *Fellow, IEEE*, Hao He, *Student Member, IEEE*, and Jian Li, *Fellow, IEEE*

***Abstract*—Sequences with impulse-like correlations are at the core of several radar and communication applications. Two criteria that can be used to design such sequences, and which lead to rather different results in the aperiodic correlation case, are shown to be identical in the periodic case. Furthermore, two simplified versions of these two criteria, which similarly yield completely different sequences in the aperiodic case, are also shown to be equivalent. A corollary of these unexpected equivalences is that the periodic correlations of an arbitrary sequence must satisfy an intriguing identity, which is also presented in this letter.**

***Index Terms*—Cyclic algorithm, periodic correlation, sequence design.**

I. Introduction and Preliminary Results

LET $\{x_n\}_{n=1}^{N}$ be the sequence in question, and let $\{r_k\}_{k=-N+1}^{N-1}$ denote its periodic correlation coefficients (or correlations, for short):

$$r_k = \sum_{n=1}^{N} x_n x^*_{n+k(\bmod N)} = r^*_{-k},\ k=0,\ldots,N-1. \quad (1)$$

In (1), the superscript * denotes the complex conjugate for scalars (as well as the conjugate transpose for matrices), and

$$n(\bmod N) = n - \left\lfloor \frac{n}{N} \right\rfloor N \quad (2)$$

where $\lfloor n/N \rfloor$ is the largest integer smaller than or equal to n/N. In most applications the elements of the sequence are constrained in some way; for instance, they may be required to be binary or polyphase, or at least to be unimodular (i.e., to have constant modulus). However we do not make such an assumption in the theoretical analysis here, for the sake of generality: therefore we simply let $x_n \in \mathbb{C}$ $(n=1,\ldots,N)$ to avoid restraining the validity of the results that follow.

Manuscript received February 11, 2009; revised April 02, 2009. First published April 21, 2009; current version published June 11, 2009. This work was supported in part by the Swedish Research Council (VR), the European Research Council (ERC), the Army Research Office (ARO) under Grant W911NF-07-1-0450, the Office of Naval Research (ONR) under Grants N00014-09-1-0211 and N00014-07-1-0193, and the National Science Foundation (NSF) under Grant CCF-0634786. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Eduard A. Jorswieck.

P. Stoica is with the Department of Information Technology, Uppsala University, SE-75105 Uppsala, Sweden (e-mail: ps@it.uu.se).

H. He and J. Li are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611-6130 USA (e-mail: haohe@ufl.edu; li@dsp.ufl.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LSP.2009.2021378

Sequences with impulse-like periodic correlations are required in many applications, particularly in pulse compression radar and in wireless communications [1]–[6]. Such sequences can be designed via the minimization of a number of criteria that express, in different ways, the distance between the actual and the desired periodic correlations. In order to describe these criteria, let us assume that r_0 is fixed (i.e., $r_0 = \text{constant}$; for example, in the case of unimodular sequences mentioned above, we have $r_0 = N$ when $|x_n| = 1$). Also, let $\mathbf{X}$ denote the following $N \times N$ right circulant matrix:

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 & \cdots & x_{N-1} & x_N \\ x_N & x_1 & \cdots & x_{N-2} & x_{N-1} \\ \vdots & & & & \vdots \\ x_2 & x_3 & \cdots & x_N & x_1 \end{bmatrix}. \quad (3)$$

Making use of $\mathbf{X}$ we can write the $N \times N$ correlation matrix of the sequence in the following form:

$$\begin{bmatrix} r_0 & r_1^* & \cdots & r_{N-1}^* \\ r_1 & r_0 & \cdots & r_{N-2}^* \\ \vdots & \ddots & \ddots & \vdots \\ r_{N-1} & \cdots & r_1 & r_0 \end{bmatrix} = \mathbf{X}\mathbf{X}^* \quad (4)$$

(this fact is well known; for completeness and for readers' convenience, we include a simple proof of (4) in Appendix A).

With (4) in mind we can think of designing the desired sequence $\{x_n\}$ with impulse-like periodic correlations via the minimization of the following criterion:

$$C_1 = \|\mathbf{X}\mathbf{X}^* - r_0\mathbf{I}\|^2 \quad (5)$$

where $\|\cdot\|$ denotes the Frobenius matrix norm (as well as the Euclidean vector norm). It follows readily from (4) that

$$C_1 = \sum_{\substack{k=-(N-1)\\ k\neq 0}}^{N-1} (N-|k|)|r_k|^2 = 2\sum_{k=1}^{N-1}(N-k)|r_k|^2. \quad (6)$$

Seemingly the above form of C_1 suggests that the larger correlation lags are less emphasized in this criterion than the smaller correlation lags (for example, the weight of $|r_1|^2$ in (6) is $N-1$, whereas that of $|r_{N-1}|^2$ is equal to 1).

The above observation leads to a second, potentially more natural criterion, in which all correlation lags (that are to be minimized) are equally weighted:

$$C_2 = N\sum_{k=1}^{N-1}|r_k|^2 \quad (7)$$

(the factor N in (7) will make the comparison with (5) neater).

Criteria similar to C_1 and C_2 have been used to design unimodular sequences with impulse-like *aperiodic* correlations in [3] (see also [1] and the many references both in [1] and in [3]). The sequences obtained by minimizing C_1 and respectively C_2 turned out, as expected, to have rather different correlation properties. On the other hand, in the periodic case the two criteria are, quite unexpectedly, identical under general conditions, as shown in the next section. A corollary of this result is that the periodic correlations $\{r_k\}$ of an arbitrary sequence $\{x_n\}$ must satisfy the following striking (and possibly novel) identity:

$$N\sum_{k=1}^{N-1}|r_k|^2 = 2\sum_{k=1}^{N-1}(N-k)|r_k|^2 \tag{8}$$

(see (6) and (7)). In the next section we also prove the equivalence between two other design criteria, called C_3 and C_4, which are related to, but at the same time simpler than, C_1 and C_2. This equivalence was, once again, unexpected at least in view of the fact that C_3 and C_4 lead to rather different results in the aperiodic correlation case, see [3].

We should remark on the fact that in the no-constraint case, the sequence $\{x_n\}$ can be easily selected to make both C_1 and C_2 (as well as C_3 and C_4, see the next section) equal to zero. In fact the same is true in the unimodular case, and even in the polyphase case (provided that the number of different phases allowed is large enough), see, e.g., [6] and the references therein. In all these cases, the criteria are equal to one another at the minimizing (also called "perfect") sequences. However, in the next section we prove that $C_1 = C_2$ (and similarly for C_3 and C_4) at *any* sequence $\{x_n\}$, which is a much stronger result.

II. Main Results

First we prove that the criteria C_1 and C_2 are identical.

A. C_1 and C_2

Let $\mathbf{F}$ denote the $N \times N$ (inverse) FFT matrix, whose (k,p)-element is given by

$$[F]_{kp} = \frac{1}{\sqrt{N}}e^{j2\pi/Nkp}, \quad k,p = 1,\ldots,N \tag{9}$$

and let

$$X_p = \sum_{n=1}^{N} x_n e^{-j2\pi/Npn}, \quad p = 1,\ldots,N \tag{10}$$

be the finite Fourier transform of the sequence $\{x_n\}$. Then it is well known that:

$$\mathbf{X} = \mathbf{F}^*\mathbf{D}\mathbf{F} \tag{11}$$

where

$$\mathbf{D} = \begin{bmatrix} X_1 & & 0 \\ & \ddots & \\ 0 & & X_N \end{bmatrix} \tag{12}$$

(once again, for completeness' sake and for readers' convenience we provide a simple proof of (11) in Appendix B).

Using (11) and the fact that $\mathbf{F}$ is unitary (i.e., $\mathbf{F}^*\mathbf{F} = \mathbf{I}$) we can rewrite C_1 as:

$$\begin{aligned} C_1 &= \|\mathbf{X}\mathbf{X}^* - r_0\mathbf{I}\|^2 = \|\mathbf{D}\mathbf{D}^* - r_0\mathbf{I}\|^2 \\ &= \sum_{p=1}^{N}(|X_p|^2 - r_0)^2. \end{aligned} \tag{13}$$

Regarding C_2, from (4) and (11) it follows that

$$\mathbf{F}\begin{bmatrix} r_0 & r_1^* & \cdots & r_{N-1}^* \\ r_1 & r_0 & \cdots & r_{N-1}^* \\ \vdots & \ddots & \ddots & \vdots \\ r_{N-1} & \cdots & r_1 & r_0 \end{bmatrix} = \mathbf{F}\mathbf{X}\mathbf{X}^* = \mathbf{D}\mathbf{D}^*\mathbf{F} \tag{14}$$

and consequently that

$$\mathbf{F}\begin{bmatrix} r_0 \\ r_1 \\ \vdots \\ r_{N-1} \end{bmatrix} = \frac{1}{\sqrt{N}}\begin{bmatrix} |X_1|^2 e^{j2\pi/N} \\ \vdots \\ |X_N|^2 e^{j2\pi/NN} \end{bmatrix}. \tag{15}$$

From (15) we obtain the following expression for C_2:

$$\begin{aligned} C_2 &= N\sum_{k=1}^{N-1}|r_k|^2 = N\left(\left\|\mathbf{F}\begin{bmatrix} r_0 \\ \vdots \\ r_{N-1}\end{bmatrix}\right\|^2 - r_0^2\right) \\ &= \sum_{p=1}^{N}(|X_p|^4 - r_0^2). \end{aligned} \tag{16}$$

Comparing (13) and (16) we see that $C_1 = C_2$ if and only if

$$-2r_0\sum_{p=1}^{N}|X_p|^2 + Nr_0^2 = -Nr_0^2 \tag{17}$$

or, equivalently,

$$r_0 = \frac{1}{N}\sum_{p=1}^{N}|X_p|^2. \tag{18}$$

However (18) is nothing but a Parseval-type equality that follows easily from the fact that

$$\mathbf{F}^*\begin{bmatrix} x_1 \\ \vdots \\ x_N \end{bmatrix} = \frac{1}{\sqrt{N}}\begin{bmatrix} X_1 \\ \vdots \\ X_N \end{bmatrix}. \tag{19}$$

With this observation, the proof of the identity

$$C_1 = C_2 \tag{20}$$

is concluded.

The criterion C_1 is a quartic function of the sequence elements. The following criterion is related to C_1, as explained shortly, but it is a simpler quadratic function of the unknown variables:

$$C_3 = \|\mathbf{X} - \sqrt{r_0}\mathbf{U}\|^2 \tag{21}$$

where $\mathbf{U}$ is an $N \times N$ unitary matrix: $\mathbf{U}^*\mathbf{U} = \mathbf{U}\mathbf{U}^* = \mathbf{I}$. The criterion C_3 is related to C_1 in the sense that C_1 takes on a small value if C_3 does so, and vice versa; in particular, $C_1 = 0$ if and only if $C_3 = 0$. Consequently, an alternative way of designing the sequence is to minimize C_3 (with respect to both $\{x_n\}$ and $\mathbf{U}$) instead of minimizing C_1.

Regarding C_2, a similar argument to the above one leads to the following related but simpler criterion [see (13) and (20)]:

$$C_4 = \sum_{p=1}^{N} |X_p - \sqrt{r_0} e^{j\psi_p}|^2 \tag{22}$$

where $\{\psi_p\}$ are auxiliary variables (similar to the $\mathbf{U}$ in (21)).

The equality of C_1 and C_2 does not necessarily imply the equivalence of C_3 and C_4. However, once again somewhat unexpectedly, C_3 and C_4 can be shown to be equivalent, as explained next.

B. C_3 and C_4

Making use of (11) we can rewrite C_3 as follows:

$$C_3 = \|\mathbf{D} - \sqrt{r_0}\mathbf{V}\|^2 \tag{23}$$

where $\mathbf{V} = \mathbf{F}\mathbf{U}\mathbf{F}^*$ is an $N \times N$ auxiliary unitary matrix. Because $\mathbf{D}$ is diagonal we can expect that the minimizing unitary matrix $\mathbf{V}$ is also diagonal. To show that this is indeed the case, note that the matrices made from the right and left singular vectors of $\mathbf{D}$ are diagonal with unit-modulus elements on the main diagonal. Then it follows from a result proved in [5] (see also the references there) that the minimizing matrix $\mathbf{V}$ must have the form:

$$\mathbf{V} = \begin{bmatrix} e^{j\psi_1} & & 0 \\ & \ddots & \\ 0 & & e^{j\psi_N} \end{bmatrix}. \tag{24}$$

Inserting (24) into (23) we obtain the criterion C_4 after a simple calculation, a fact that we informally can state as follows:

$$\min_{\{V_{kp}(k \neq p)\}} C_3 = C_4. \tag{25}$$

With this observation the proof of the equivalence between C_3 and C_4 is concluded.

III. Discussion and a Numerical Example

In the heavily constrained case of binary sequences or of polyphase sequences with a small phase set, perfect sequences (for which $C_1 = C_2 = C_3 = C_4 = 0$) are rare occurrences [6]. For such cases, minimizing C_1 or C_2 may be the only way available for designing an optimal sequence. Alternatively, we can design a quasi-optimal sequence by minimizing the related but simpler criteria C_3 or C_4 (note that the sequence minimizing C_3 or C_4 is not necessarily the same as the sequence that minimizes C_1 or C_2). We recommend using C_4 for such a design task due to the computational convenience of this criterion. Indeed, the evaluation of C_4 can be efficiently done by means of the FFT. Furthermore, C_4 can be conveniently minimized using a cyclic algorithm called PeCAN (**Pe**riodic-correlation **C**yclic **A**lgorithm-**N**ew) that was introduced in [4] (see below for an outline). If the performance achieved by C_4 and PeCAN is not deemed to be satisfactory, then the direct minimization of C_1 or C_2 (which is harder) may be advised.

In the mildly constrained case of polyphase sequences with large phase sets or of unimodular sequences, on the other hand, perfect sequences exist for any length N (see, e.g., [6]). Furthermore, there are systematic analytical ways (including closed-form expressions) for constructing such perfect sequences. However, even in this situation, designing a perfect sequence by minimizing one of the above criteria (all of which can be made equal to zero in such a case) is of considerable interest for radar and for wireless communications in hostile environments (such as covert underwater communications, see, e.g., [4] and the references therein). Indeed, in such applications it is important not only to use a perfect sequence to mitigate the multipath interferences, but also to employ one that is hard to guess by the adversary. Perfect sequences given by closed-form expressions or constructed in some other analytical ways are typically easy to guess because they depend on a relatively small number of parameters (such as the sequence's length, possible sign changes or phase shifts etc.). On the other hand, perfect sequences generated by minimizing the above criteria depend on the initial sequence used to start the search, and are nearly uncorrelated to one another when obtained using random initializations; and a random initial sequence depends on too many unknowns (between 2^N in the binary case, and infinity in the unimodular case) to allow an exact guessing (even when the sequence's length and the generating algorithm are known). Similarly to what we said in the previous paragraph, we recommend using C_4 for sequence design in this case as well: indeed C_4 can be efficiently minimized by the PeCAN algorithm, whereas no similarly efficient algorithm is available for minimizing the other criteria.

To illustrate the above claim, we consider the design of a unimodular sequence (with $|x_n| = 1$) of length $N = 256$. We will use C_4 in (22) and the PeCAN algorithm for this purpose. Here is a brief review of PeCAN (see [3] and [4] for more details; note that this algorithm can be used with values of N up to 10^6).

1) Use N independent and uniformly distributed phases in the interval $[0, 2\pi]$ to randomly generate an initial unimodular sequence $\{x_n\}_{n=1}^N$.
2) For given $\{x_n\}$, compute the FFT of $\{x_n\}$, i.e., $\{X_p\}_{p=1}^N$, and minimize C_4 with respect to $\{\psi_p\}_{p=1}^N$. The minimizing $\{\psi_p\}$ are simply given by
$$\psi_p = \arg(X_p), \quad p = 1, \ldots, N. \tag{26}$$
3) For given $\{\psi_p\}$, compute the IFFT of $\{e^{j\psi_p}\}$, let us say $\{z_n\}$, and minimize C_4 with respect to $\{x_n\}$ (subject to $|x_n| = 1$). Similarly to (26), the minimizing $\{x_n\}$ are easy to compute:
$$x_n = e^{j \arg(z_n)}, \quad n = 1, \ldots, N. \tag{27}$$
4) Iterate Steps 2 and 3 until a practical convergence criterion is satisfied.

(We should note that design algorithms similar to PeCAN have been proposed before in the literature, see e.g., [1], [2] and references therein; however, these algorithms have been motivated on only heuristic grounds, without any clear connection to the minimization of C_4, and in fact they fall short of being minimization algorithms for C_4).

We have run PeCAN with $N = 256$ and 200 different random initializations. Out of the obtained 200 unimodular sequences,

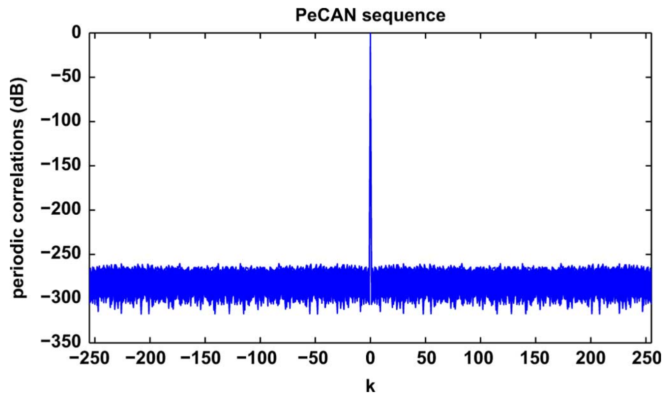

Fig. 1. Superimposed normalized periodic correlations (see (28)) of 100 perfect sequences (of length $N = 256$) generated using PeCAN with random initialization.

the 100 sequences with the lowest integrated sidelobe level, $\sum_{k=1}^{N-1} |r_k|^2$, were kept. The normalized periodic correlations (in dB) of these 100 sequences, viz.

$$20 \log_{10} \frac{|r_k|}{N} \quad (k = -255, \dots, 255) \tag{28}$$

are shown in Fig. 1, in a superimposed manner. The values of the correlation sidelobes (corresponding to lags $k \neq 0$) in this figure are lower than -260 dB (i.e., 10^{-13}), which can actually be considered as zero in practice. We have also computed the normalized periodic cross-correlations of these 100 perfect sequences associated with Fig. 1:

$$\frac{1}{N} \sum_{n=1}^{N} x_n^{(m_1)} x_{n+k(\text{mod} N)}^{(m_2)*} \quad k = 0, \dots, 255 \quad \text{and}$$
$$m_1, m_2 = 1, \dots, 100 \quad (m_1 \neq m_2) \tag{29}$$

where $\{x_n^{(m_1)}\}_{n=1}^{N}$ denotes the $m_1{}^{\text{th}}$ perfect sequence. The absolute values of (29), for the shown k, m_1 and m_2, turned out to lie in the interval $[4.83 \times 10^{-5}, 0.24]$ (with a mean value equal to 0.055), which means that the perfect sequences obtained using PeCAN with random initialization can be considered to be nearly uncorrelated to one another. Note that the corresponding interval for the initial sequences was $[2.77 \times 10^{-5}, 0.25]$ (with a mean value of 0.055), from which we can infer that the PeCAN algorithm lowers the auto-correlation sidelobes of the initial random sequences to almost zero without increasing the cross-correlations among them.

Appendix A

Proof of (4): Let $\mathbf{J}$ denote the $N \times N$ shift matrix:

$$\mathbf{J} = \begin{bmatrix} \mathbf{0} & \mathbf{I} \\ 1 & \mathbf{0} \end{bmatrix}. \tag{30}$$

Then, we have that

$$\mathbf{J}^T \begin{bmatrix} x_1 \\ \vdots \\ x_{N-1} \\ x_N \end{bmatrix} = \begin{bmatrix} x_N \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} \tag{31}$$

(the superscript ^{T} denotes the matrix transpose) and, by induction, that the k^{th} row of $\mathbf{X}$ is $\mathbf{x}^T \mathbf{J}^k$ ($\mathbf{x} = [x_1 \ \cdots \ x_N]^T$) and therefore that

$$[\mathbf{X}\mathbf{X}^*]_{kp} = \mathbf{x}^T \mathbf{J}^k (\mathbf{x}^T \mathbf{J}^p)^* = \mathbf{x}^T \mathbf{J}^k (\mathbf{J}^*)^p (\mathbf{x}^T)^*. \tag{32}$$

Let $k \geq p$. Because $r_k = \mathbf{x}^T \mathbf{J}^k (\mathbf{x}^T)^*$ and $\mathbf{J}^k (\mathbf{J}^*)^p = \mathbf{J}^{k-p}$ (as $\mathbf{J}\mathbf{J}^* = \mathbf{I}$), it follows that

$$[\mathbf{X}\mathbf{X}^*]_{kp} = \mathbf{x}^T \mathbf{J}^{k-p} (\mathbf{x}^T)^* = r_{k-p} \tag{33}$$

which proves (4).

Appendix B
Proof of (11)

Let

$$\begin{aligned} \mathbf{a}_p &= \text{the } p^{\text{th}} \text{ column of } \mathbf{F}^* \\ &= \left[e^{-j2\pi/Np} \ \cdots \ e^{-j2\pi/NNp} \right]^T. \end{aligned} \tag{34}$$

Then we have the following equivalences (see also the proof of (4)):

$$\begin{aligned} (11) &\iff \mathbf{X}\mathbf{F}^* = \mathbf{F}^*\mathbf{D} \iff \mathbf{X}\mathbf{a}_p = \mathbf{a}_p X_p \\ &\iff \mathbf{x}^T \mathbf{J}^k \mathbf{a}_p = e^{-j2\pi/Nkp} X_p \ (p, k = 1, \dots, N). \end{aligned} \tag{35}$$

The last equality is obviously true for $k = N$; so let us assume that $k = 1, \dots, N-1$. To show that (35) holds in the latter case as well, observe that

$$\begin{aligned} &e^{-j2\pi/Nkp} X_p \\ &= \sum_{s=1}^{N} x_s e^{-j2\pi/Np(s+k)} \quad (k = 1, \dots, N-1) \\ &= \mathbf{x}^T \begin{bmatrix} e^{-j2\pi/Np(k+1)} \\ \vdots \\ e^{-j2\pi/NpN} \\ e^{-j2\pi/Np(N+1)} \\ \vdots \\ e^{-j2\pi/Np(N+k)} \end{bmatrix} = \mathbf{x}^T \begin{bmatrix} e^{-j2\pi/Np(k+1)} \\ \vdots \\ e^{-j2\pi/NpN} \\ e^{-j2\pi/Np} \\ \vdots \\ e^{-j2\pi/Npk} \end{bmatrix} \\ &= \mathbf{x}^T \mathbf{J}^k \mathbf{a}_p \end{aligned} \tag{36}$$

which proves (35), and therefore (11).

References

[1] N. Levanon and E. Mozeson, *Radar Signals*. New York: Wiley, 2004.

[2] A. Freedman, N. Levanon, and S. Gabbay, "Perfect periodic correlation sequences," *Signal Process.*, vol. 41, no. 2, pp. 165–174, 1995.

[3] P. Stoica, H. He, and J. Li, "New algorithms for designing unimodular sequences with good correlation properties," *IEEE Trans. Signal Process.*, vol. 57, pp. 1415–1425, Apr. 2009.

[4] J. Ling, H. He, P. Stoica, J. Li, and W. Roberts, "Covert underwater acoustic communications: Transceiver structures, waveform designs and associated performances," *IEEE Trans. Signal Process.* [Online]. Available: http://plaza.ufl.edu/haohe/papers/CovertComm.pdf, submitted for publication

[5] P. Stoica, J. Li, and X. Zhu, "Waveform synthesis for diversity-based transmit beampattern design," *IEEE Trans. Signal Process.*, vol. 56, pp. 2593–2598, Jun. 2008.

[6] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inform. Theory*, vol. 50, pp. 559–565, Mar. 2004.