On Integer-valued Zero Autocorrelation Sequences

Soo-Chang Pei* and Kuo-Wei Chang† ‡
*Department of Electrical Engineering, National Taiwan University, Taipei Taiwan 10617 R.O.C.
Email: pei@cc.ee.ntu.edu.tw, Fax: 886-2-23671909
†Graduate Institute of Communication Engineering, National Taiwan University, Taipei Taiwan 10617 R.O.C.
E-mail:d00942009@ntu.edu.tw
‡Chunghwa Telecom Laboratories, Taoyuan County 32601, Taiwan
E-mail:muslim@cht.com.tw

***Abstract*—A systematic way to construct Integer-valued zero autocorrelation sequences is proposed. This method only uses fundamental theorems of discrete Fourier transform(DFT) and some number theories.**

I. Introduction

Zero autocorrelation(ZAC) sequences have many applications in communication and cryptography. In this work we propose a systematic way to find integer-valued ZAC sequences. By the properties of Fourier transform and Ramanujan's sum, the method is easy to understand and implement.

ZAC sequences have been extensively used in communication engineering, such as synchronization, CDMA [1], [2] and OFDM[3] system. They have also been applied to cryptography for constructing pseudo random sequences. In this paper a special kind of ZAC sequences is considered, that is, integer-valued ZAC, because integer has the following advantages comparing to complex floating point number.

1) Integer requires less memory, for both saving and sending.

2) Arithmetic operations can be done faster and error-free.

3) The system can be implemented on hardware easily.

There are some trivial integer-valued ZAC. The most obvious one is

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}$$

The second one, although less known, is still in simple form

$$\begin{pmatrix} N-2 \\ -2 \\ -2 \\ \vdots \\ -2 \\ -2 \end{pmatrix}$$

This paper is sponsored by Chunghwa Telecom Co., Ltd, Taiwan

where N is the signal length. For example, $N = 5$ and $N = 6$

$$\begin{pmatrix} 3 \\ -2 \\ -2 \\ -2 \\ -2 \end{pmatrix} \text{ and } \begin{pmatrix} 4 \\ -2 \\ -2 \\ -2 \\ -2 \\ -2 \end{pmatrix}$$

When N is a composite number, constructing integer-valued ZAC from its factor by zero-padding is not difficult to think of. Let say $N = 15 = 3 \times 5$, by the examples given above, we can organize signals like

$$(3, 0, 0, -2, 0, 0, -2, 0, 0, -2, 0, 0, -2, 0, 0)$$

or

$$(1, 0, 0, 0, 0, -2, 0, 0, 0, 0, -2, 0, 0, 0, 0)$$

One natural question is, are there any non-trivial integer-valued ZAC? The answer is yes, such as

$$\begin{pmatrix} 2 \\ -1 \\ -1 \\ 2 \\ -1 \\ 5 \end{pmatrix}$$

In this paper we will show how to find these signals systematically. One related research is [5] which generates Gaussian Integer and some real integer ZAC, but the major drawback of that method is the signal length N must be even.

The paper is organized as follows. In section II we will state some definitions, and in section III we will describe two major theorems that help us to construct integer-valued ZAC signals. The algorithm will be presented in section IV. The conclusion is in section V.

II. Preliminaries

Unless specified otherwise the singal is considered as periodic, with period N. The terms "signal" is equivalent to "sequence".

Let $W_N = \exp(2\pi i/N)$, $i = \sqrt{-1}$. If $x(n)$ is the input signal with period N, then $X(k) = \sum_{n=0}^{N-1} x(n) W_N^{-nk}$ is called

the discrete Fourier transform (DFT) of $x(n)$, also represented by $F\{x(n)\}$.

One of the useful lemma of DFT is the circular shift property.

$$X(k+s) = F\left\{W_N^{-ns}x(n)\right\} \tag{1}$$

A signal $x(n)$ is called constant amplitude (CA) if $x^*(n)x(n) = C \quad \forall n$ and for some constant C, where * means complex conjugate.

The autocorrelation of a signal $x(n)$ is defined as $R_{xx}(m) = \sum_{n=0}^{N-1} x^*(n+m)x(n)$. A signal is called zero autocorrelation (ZAC) if its autocorrelation is $B\delta(n)$ for some constant B, where $\delta(n)$ is periodic delta function

$$\delta(n) = \begin{cases} 1, & n \equiv 0(\text{mod } N) \\ \\ 0, & elsewhere \end{cases} \tag{2}$$

A signal is called gcd-delta if $s(n) = \delta(d - gcd(N,n))$ for some constant $d|N$. We express it as $s_{N,d}(n)$. For example,

$$s_{6,2}(n) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, s_{6,6}(n) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Since $gcd(N,0) = N$ we can easily prove that $s_{N,N}(n) = \delta(n)$.

III. Theory

In this section we will discuss two fundamental theorems. The first one is elementary to verify [6]

Theorem III.1. *If a signal $x(n)$ is CA, then $X(k)$,the discrete Fourier transform of $x(n)$, is ZAC. Moreover, if $x^*(n)x(n) = C$, then $R_{XX}(m) = CN^2\delta(m)$*

Proof:

$$\begin{aligned} R_{XX}(m) &= \sum_{k=0}^{N-1} X^*(k+m)X(k) \\ &= \sum_{k=0}^{N-1}\Big(\sum_{n_1=0}^{N-1} x^*(n_1)W_N^{n_1(k+m)}\Big)\Big(\sum_{n_2=0}^{N-1} x(n_2)W_N^{-n_2k}\Big) \\ &= \sum_{n_1=0}^{N-1} W_N^{n_1m}\sum_{n_2=0}^{N-1} x^*(n_1)x(n_2)\sum_{k=0}^{N-1} W_N^{(n_1-n_2)k} \\ &= \sum_{n_1=0}^{N-1} W_N^{n_1m}\sum_{n_2=0}^{N-1} x^*(n_1)x(n_2)N\delta(n_1-n_2) \\ &= N\sum_{n_1=0}^{N-1} W_N^{n_1m}x^*(n_1)x(n_1) \\ &= CN\sum_{n_1=0}^{N-1} W_N^{n_1m} \\ &= CN^2\delta(m) \end{aligned}$$

■

As an example we consider $N = 6$, and

$$x(n) = \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ -1 \\ -1 \end{pmatrix}$$

which is CA. So the $F\{f(n)\}$ is equal to

$$X(k) = \begin{pmatrix} 0 \\ 2-2\sqrt{3}i \\ 0 \\ 2 \\ 0 \\ 2+2\sqrt{3}i \end{pmatrix}$$

which is ZAC.

The second theorem is related to Ramanujan's sum.

Theorem III.2. *The discrete Fourier transform of a gcd-delta signal is integer-valued.*

Proof:

$$\begin{aligned} S_{N,d}(k) &= \sum_{n=0}^{N-1} s_{N,d}(n)W_N^{-nk} \\ &= \sum_{gcd(n,N)=d} W_N^{-nk} \\ &= \sum_{gcd(s,N/d)=1} W_{N/d}^{-sk} \\ &= c_{N/d}(k) \end{aligned}$$

The last term is call Ramanujan's sum. The proof of any Ramanujan's sum is integer can be found in [4]. ■

IV. Constructing Integer ZAC sequence

A. Algorithm

By Theorem III.1 we can construct ZAC sequences but can not guarantee if they were integer-valued. Thus we need Theorem III.2 to help us. The steps are described as follows

Step 1) Given a signal length N, calculate all its factors d.

Step 2) for every d choose a binary number $b_d = 0$ or 1 and a phase shift $W_N^{p_d}$, where p_d is any integer between 0 and $N-1$.

Step 3) Let

$$g(n) = \sum_{d|N}(-1)^{b_d}W_N^{p_dn}s_{N,d}(n)$$

Step 4) Then $G(k) = F\{g(n)\}$ is an integer-valued ZAC squence.

Before we prove this, we provide another example to explain the ideas. Let $N = 6$, so $d = 1, 2, 3, 6$. We can arbitrarily

choose $b_1 = 0, b_2 = 1, b_3 = 1, b_6 = 0$ and $p_1 = 2, p_2 = 1, p_3 = 2, p_6 = 0$. Since

$$s_{6,1}(n) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, s_{6,2}(n) = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$s_{6,3}(n) = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, s_{6,6}(n) = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

therefore in step 3,

$$g(n) = \begin{pmatrix} 1 \\ -W_6^2 \\ -W_6^2 \\ -1 \\ -W_6^4 \\ -W_6^4 \end{pmatrix}$$

And the fourier transform of $g(n)$ is

$$G(k) = \begin{pmatrix} 2 \\ -1 \\ -1 \\ 2 \\ -1 \\ 5 \end{pmatrix}$$

The $G(k)$ is an integer-valued ZAC as seen in the introduction.

From the example above we can notice that $g(n)$ is CA, so by theorem III.1 $G(k)$ is ZAC. We now formally prove this.

Theorem IV.1. *$g(n)$ in step 3 is CA.*

Proof: Let $gcd(N, n) = d'$,

$$\begin{aligned} g(n) &= \sum_{d|N} (-1)^{b_d} W_N^{p_d n} s_{N,d}(n) \\ &= \sum_{d|N} (-1)^{b_d} W_N^{p_d n} \delta(d - gcd(N, n)) \\ &= \sum_{d|N} (-1)^{b_d} W_N^{p_d n} \delta(d - d') \\ &= (-1)^{b_{d'}} W_N^{p_{d'} n} \end{aligned} \tag{3}$$

so $g(n)$ is on unit circle for all n. In other words,

$$g^*(n)g(n) = 1 \,\forall\, n$$

which complete the proof. ∎

The last part is to verify $G(k)$ is integer-valued.

Theorem IV.2. *$G(k)$ in the step 4 is integer-valued.*

Proof: Since Fourier transform is a linear transformation,

$$\begin{aligned} G(k) &= F\{g(n)\} \\ &= \sum_{d|N} (-1)^{b_d} F\{W_N^{p_d n} s_{N,d}(n)\} \end{aligned}$$

and by (1)

$$= \sum_{d|N} (-1)^{b_d} S_{N,d}(k - p_d)$$

Since by theorem III.2 $S_{N,d}(k)$ is integer-valued, and the circular shift of an integer-valued sequence is still integer-valued, thus $G(k)$ is in fact a linear combination of integer-valued sequence with coefficients ± 1. This proves that $G(k)$ is integer-valued. ∎

It is worthy to note that in step 3, if we change $(-1)^{b_d}$ to i^{b_d} and choose b_d in the range of 0 to 3, then the $G(k)$ is a Gaussian-Integer valued ZAC as in [5]

B. Some special cases

We will check two special cases, the first one is

$$\{1, \underbrace{0, ..., 0}_{k_1}, 1, \underbrace{0, ..., 0}_{k_2}, 1, \underbrace{0, ..., 0}_{k_1}, -1, \underbrace{0, ..., 0}_{k_2}\}$$

if N is even and $2k_1 + 2k_2 + 4 = N$. It is trivial that it is an integer-valued ZAC. We claim that this type can be established in step 3. In fact, if we choose all $b_d = 1$ and

$$p_d = \begin{cases} k_1 + 1, & d \equiv 1 (\mathrm{mod}\ 2) \\ 0, & elsewhere \end{cases}$$

The proof is easy so we omit it here. As a tiny example let $N = 6$ and $k_1 = 0$. So

$$g(n) = \begin{pmatrix} 1 \\ W_6 \\ 1 \\ W_6^3 \\ 1 \\ W_6^5 \end{pmatrix}, G(k) = \begin{pmatrix} 3 \\ 3 \\ 0 \\ 3 \\ -3 \\ 0 \end{pmatrix}$$

which is the scaling of $[1, 1, 0, 1, -1, 0]$. This is what we want since $k_1 = 0$ so the first two 1s has no zero between them.

The second special case is zero-padding as seen in the introduction. We want to prove that, if $g(n)$ is the length N signal we choose in step 3, with parameters $[b_d, p_d]$, and build $G(k)$ in step 4, then the length MN zero-padding integer-valued ZAC signal

$$H(k) = \begin{cases} G(\frac{k}{M}), & k \equiv 0 (\mathrm{mod}\ M) \\ 0, & elsewhere \end{cases}$$

can also be built by choose

$$\begin{aligned} p'_d &= M p_{gcd(d,N)} \\ b'_d &= b_{gcd(d,N)} \end{aligned} \tag{4}$$

Proof: By basic Discrete Fourier Transform property, repetition in time domain will cause zero-inserting in frequency domain. So we divide the proof into two parts. First we show that $h(n) = g(n)$ for $1 \leq n \leq N$, and then prove that $h(n+N) = h(n)$.

Part 1. Recall (3)

$$g(n) = (-1)^{b_{d_1}} W_N^{p_{d_1} n}, d_1 = gcd(N, n)$$
$$h(n) = (-1)^{b'_{d_2}} W_{MN}^{p'_{d_2} n}, d_2 = gcd(MN, n)$$

since $h(n)$ is also built in step 3. Rewrite $h(n)$ by (4),

$$\begin{aligned} h(n) &= (-1)^{b'_{d_2}} W_{MN}^{p'_{d_2} n}, d_2 = gcd(MN, n) \\ &= (-1)^{b_{gcd(d_2,N)}} W_{MN}^{M p_{gcd(d_2,N)} n} \\ &= (-1)^{b_{gcd(d_2,N)}} W_N^{p_{gcd(d_2,N)} n} \end{aligned} \quad (5)$$

And note that $gcd(gcd(n, MN), N) = gcd(n, N)$ for $1 \leq n \leq N$, thus

$$\begin{aligned} h(n) &= (-1)^{b_{gcd(d_2,N)}} W_N^{p_{gcd(d_2,N)} n}, d_2 = gcd(MN, n) \\ &= (-1)^{b_{gcd(n,N)}} W_N^{p_{gcd(n,N)} n} \\ &= g(n) \end{aligned}$$

Part 2. By (5)

$$\begin{aligned} h(n+N) &= (-1)^{b_{gcd(d_2,N)}} W_N^{p_{gcd(d_2,N)}(n+N)} \\ &, d_2 = gcd(MN, n+N) \\ &= (-1)^{b_{gcd(d_2,N)}} W_N^{p_{gcd(d_2,N)} n} \end{aligned}$$

But $gcd(gcd(n+N, MN), N) = gcd(n, N) = gcd(gcd(n, MN), N)$, so $h(n+N) = h(n)$ and the proof is completed. ■

C. Discussion in algebraic view

One can notice that the set of signals we construct in step 3 actually forms a finite abelian group $(G, \cdot)$, where $\cdot$ means the pointwise product: $g_1(n) \cdot g_2(n) = g_1(n) g_2(n)$. To prove that this set is a group, we first note that g is determined by the choices of b_d and p_d. Suppose we have two elements g_1 and g_2, with the parameters [b_{1d} ,p_{1d}] and [b_{2d} , p_{2d}] respectively. Then define

$$b_{3d} = b_{1d} + b_{2d} (\text{mod } 2)$$
$$p_{3d} = p_{1d} + p_{2d} (\text{mod } N)$$

this parameters form $g_3 \in G$. We can easily show that $g_1(n) g_2(n) = g_3(n)$, which prove the closure property. The identity in this group is $I(n) = 1$ and the inverse of g_1 is g_2 where

$$b_{2d} = -b_{1d} (\text{mod } 2)$$
$$p_{2d} = -p_{1d} (\text{mod } N)$$

We can extend our discussion in abelian group with $\mathbb{Q}$.

Theorem IV.3. *If $g_1(n), g_2(n)$ are CA, and $F\{g_1(n)\}, F\{g_2(n)\}$ are rational-valued. Then*

1) $g_1(n) g_2(n)$ is CA, and

2) $F\{g_1(n) g_2(n)\}$ is rational-valued.

Proof: Since the pointwise product of two constant amplitude function is still constant amplitude, the first part is trivial.

Second, recall that the Fourier transform property

$$F\{g_1(n) g_2(n)\} = F^{-1}\{g_1(n)\} \odot_N F^{-1}\{g_2(n)\}$$

where $\odot_N$ means N points circular convolution. By assumption $F\{g_1(n)\}, F\{g_2(n)\}$ are rational-valued, and

$$F^{-2}\{x(n)\} = \frac{1}{N} x(-n)$$

so $F^{-1}\{g_1(n)\}, F^{-1}\{g_2(n)\}$ are the reverse order of $F\{g_1(n)\}, F\{g_2(n)\}$ and divided by N, so they are rational-valued, too. Since the circular convolution of two rational-valued signals is still rational-valued, the proof is completed. ■

The theorem immediately tells us:

Corollary IV.4. *The rational-value ZAC signals form a group (G,$\odot_N$).*

In practice we can multiply the least common multiple (LCM) to get rid of rational-value and become integer-value signal.

V. Conclusions

In this paper a systematic approach to construct integer-valued zero autocorrelation signal is proposed. By the cicular shift property and Ramanujan's sum, we can generate a lot of these signals which form a finite abelian group. In addition, zero-padding method can be viewed as our special case.

Acknowledgment

References

[1] Viterbi, A. J., CDMA, *Principles of Spread Spectrum Communication.* Addison Wesley, 1995

[2] Carni, E., and Spalvieri, A. "Synchronous CDMA based on the cyclical translations of a CAZAC sequence", *IEEE Transactions on Wireless Communications*, 2005

[3] Shah, S. F. A., and Tewfik, A. H, "Perfectly balanced binary sequences with optimal autocorrelation", *14th IEEE International Conference on Electronics Circuits and Systems*, 2007

[4] G. H. Hardy and E. M. Wright , "An Introduction to the Theory of Numbers",*Oxford University Press*, fifth edition. Chap. XVI.

[5] Hu, Wei-Wen and Wang, Sen-Hung and Li, Chih-Peng, "Gaussian Integer Sequences with Ideal Periodic Autocorrelation Functions", *2011 IEEE International Conference on Communications ICC*, pp. 1-5

[6] Benedetto, J.J., Konstantinidis, I. and Rangaswamy, M. "Phase-Coded Waveforms and Their Design", *IEEE Signal Processing Magazine 26*, pp. 22-31 , 2009.