Perfect Gaussian Integer Sequences of Arbitrary Length

Soo-Chang Pei, Life Fellow, IEEE, and Kuo-Wei Chang

Abstract—In this work, we describe some methods to generate zero autocorrelation Gauss integer sequences of arbitrary length. These methods can be combined with each other so that more choices can be made.

Index Terms—Gauss integer sequence, zero autocorrelation.

I. INTRODUCTION

R ESENTLY the study of zero autocorrelation (ZAC) sequences, or perfect sequences, has become very popular, because those sequences play important roles in modern communication system such as CDMA [1], [2] and OFDM [3]. In particular, due to arithmetic convenience, sequences with integer value or Gaussian integer value, which in the form of a+bi where $a, b \in \mathbb{N}$, have been discussed many times [6], [8]–[10]. However, these methods all have some constraints. Hu's method can only be applied when the period length N is even [6], Yang's method can only be applied when the length is odd prime [8], and in [10], the length can only be pq when p and q are twin primes. Although in [9], any arbitrary length of integer-valued ZAC sequences can be achieved, these sequences form a finite abelian group thus only a few number of sequences can be obtained.

When considering whether a sequence if ZAC or not, a smart way is to calculate its discrete Fourier transform (DFT). Benedetto [4] has proven that a sequence is ZAC if and only if its DFT is constant amplitude (CA). This property also gives us a guide to construct ZAC, by calulating in frequency domain and setting all values to be CA, then transform back to time domain to accomplish ZAC. In [9] Ramanujan's sum is introduced to ensure that the result ZAC sequence is integer-valued. We will extand that work to Gaussian integer.

Legendre symbol or sequence(LS)[11], [12] has a strong connection to quadratic Gauss sum, which is also a summation of complex roots of unity, like Ramanujan's sum. The absolute value of Gauss sum is \sqrt{N} [7], [11], which is not always an integer, so we must add some terms. This method can compensate Yang's because that method has only 3 different values.

Manuscript received September 24, 2014; revised December 02, 2014; accepted December 02, 2014. Date of publication December 18, 2014; date of current version December 24, 2014. This work was supported by the Ministry of Science and Technology, Taiwan under Contract MOST 103-2221-E-002-102. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Peter K. Willett.

S.-C. Pei is with the Graduate Institute of Communication Engineering, National Taiwan University, Taipei 10617, Taiwan (e-mail: pei@cc.ee.ntu.edu.tw).

K.-W. Chang is with the Graduate Institute of Communication Engineering, National Taiwan University, Taipei 10617, Taiwan, and also with Chunghwa Telecom Laboratories, Taoyuan County 32601, Taiwan (e-mail: d00942009@ntu.edu.tw; muslim@cht.com.tw).

Digital Object Identifier 10.1109/LSP.2014.2381642

In [8], Yang has invited reader to attack the problem when N is an odd composite number. We accept the challenge and propose some methods to construct perfect Gaussian integer sequences, from the naïve zero padding and convolution, to decomposing N into different groups. A Concrete example is given as N = 15. Note that although N = 15 is a product of twin prime, our method is simpler and can generate more sequences than [10].

This paper is organized as follows. In Section II some new methods for prime length to get more sequences will be introduced. Combination of short prime length sequences into a larger, composite length will be revealed in Section III. Finally the conclusion is made in Section IV.

II. NOVEL METHODS FOR PRIME N

Although this problem has been solved, as Yang's method can generate infinite number of ZAC sequences in gaussian integer, the limitations of that approach are

- 1) The outcome has only 3 different values
- 2) The degree of freedom is only 2.

In this section we proposed two ways to compensate Yang's method. Both of them use the property of Legendre Sequences, but the later can only be applied to 4k + 1 prime.

A. Using Legendre Sequence and Gauss Sum When N is Prime

Recall that when N is prime, Legendre symbol is defined as

$$\left(\frac{n}{N}\right) = \begin{cases} 1, & if \ \exists x, x^2 \equiv n(mod \ N) \\ 0, & n \equiv 0(mod \ N) \\ -1, & otherwise. \end{cases}$$

And the Gauss sum is defined as

$$G(k) = \sum_{n=0}^{N-1} \left(\frac{n}{N}\right) e^{-2\pi i k n/N}$$

A well known result [5] is that

$$G(k) = \begin{cases} \left(\frac{k}{N}\right)\sqrt{N}, & N \equiv 1 \pmod{4} \\ -\left(\frac{k}{N}\right)i\sqrt{N}, & N \equiv 3 \pmod{4} \end{cases}$$

In other words, the Fourier transform of Legendre Sequences is almost CA, with the only exception on k = 0, the first point. The amplitude is \sqrt{N} thus our goal is to find a Gaussian integer a and some integers b, and c such that

$$|a|^2 = b^2 + Nc^2 \tag{1}$$

Then a sequence that

$$f(n) = \begin{cases} a, & n = 0\\ \left(\frac{n}{N}\right)\sqrt{Nc} + bi, & n \neq 0 \end{cases}$$
(2)

is CA, and the DFT of f(n) is ZAC in Gaussian integer. Before we prove this let's see some tiny examples of N = 3 and N = 5

See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Example II.1: For N = 3, the most trivial value we can choose is a = 2, b = 1, and c = 1. Thus

$$f(n) = \left\{2, 1i + \sqrt{3}, 1i - \sqrt{3}\right\}$$

$$F(k) = DFT\left\{f(n)\right\} = \left\{2 + 2i, 2 - 4i, 2 + 2i\right\}$$

As we can see, f(n) is CA and F(k) is with Gaussian integer value. This example shows us a does not necessary to be complex.

Example II.2: N = 3. Let's try a non-trivial value c = 2, b = 5, a = 6 + 1i

$$f(n) = \left\{ 6 + 1i, 5i + 2\sqrt{3}, 5i - 2\sqrt{3} \right\}$$
$$F(k) = \left\{ 6 + 11i, 6 - 10i, 6 + 2i \right\}$$

From this example we can get a very different result from the previous one. Note that *a* has three alternatives 6 - 1i, 1 + 6i, and 1 - 6i. They all give us different ZAC sequences.

Example II.3: N = 5, c = 1, b = 0, a = 2 + 1i

$$f(n) = \left\{2 + 1i, \sqrt{5}, -\sqrt{5}, -\sqrt{5}, \sqrt{5}\right\}$$

$$F(k) = \left\{2 + 1i, 7 + 1i, -3 + 1i, -3 + 1i, 7 + 1i\right\}$$

There are various way to construct infinite triples (a, b, c) satisfied (1). Let $a = a_r + ia_i$, where a_r, a_i are integers. If we choose c = 0, clearly the (1) will reduce to $a_r^2 + a_i^2 = b^2$, and it has infinite solutions. If N is odd, we can choose any odd c and any even a_r . Now (1) becomes

$$a_r^2 + a_i^2 = b^2 + Nc^2$$

 $\Rightarrow a_i^2 - b^2 = Nc^2 - a_r^2$

Since N and c are odd and a_r is even, $Nc^2 - a_r^2$ must be odd. Let $Nc^2 - a_r^2 = 2k + 1$, then we can use $a_i = k + 1$ and b = k. Similarly for any even c and odd a_r , we can find proper a_i and b by the same trick.

We complete this subsection by proving the claim that F(k) is ZAC with Gaussian integer value.

Proof: Since f(n) is CA by definition, thus F(k) is ZAC by [4]. To prove they are all Gaussian integer, we actually give F(k) a closed form. If $N \equiv 1 \pmod{4}$

$$F(k) = \begin{cases} a + (N-1)bi, & k = 0\\ a + \left(\frac{k}{N}\right)Nc - bi, & k \neq 0 \end{cases}$$

If $N \equiv 3 \pmod{4}$

$$F(k) = egin{cases} a+(N-1)bi, & k=0\ a-\left(rac{k}{N}
ight)Nci-bi, & k
eq 0 \end{cases}$$

Either case the F(k) is in Gaussian integer value since a is Gaussian integer and b, c are integers.

B. Using GLS when N is 4k + 1 prime

When N is 4k + 1 prime, there is another way to increase the degree of freedom by using Generalized Legendre Sequences (GLS)[11]–[13]. GLS are originally applied to construct the eigenvectors of discrete Fourier transform (DFT) and generate a complete N-dimensional orthogonal basis [13], because they have the property that their Fourier transform is their conjugate multiply a constant whose absolute value is \sqrt{N} . All the values except the first one of GLS lies on unit circle, and when N = 4k + 1 we can choose the ones which only contains $\{1, i, -1, -i\}$, in order to bound the sequences in gaussian integer. The detail steps is described as follows:

- Choose a GLS x where the first value is 0 and the rest only contain {1, i, -1, -i}.
- 2) Take DFT of x. Now we have a sequence y that the first value is still 0, but the absolute value of rest all equal to \sqrt{N} .
- 3) The first value of y can then be chosen by a Gaussian integer a + bi satisfying $a^2 + b^2 = N$, which always exists by Fermat's theorem. Now the sequence is constant amplitude.
- 4) The DFT of y is a ZAC with Gaussian integer.

It is easy to prove this sequence is really in Gaussian integer. Define

$$\delta(n) = \begin{cases} 1 & n = 0 \\ 0 & n \neq 0 \end{cases}$$

The sequence is actually

 $DFT \{ DFT \{ x(n) \} + (a+bi)\delta(n) \} = Nx(N-n) + a + bi$

where N, a, b, and all value in x are with Gaussian integer, so will be the sequence.

As a concrete example, assume N = 13 and we choose a GLS x

$$x = \{0, 1, -i, 1, -1, -i, -i, i, i, 1, -1, i, -1\}$$

And we choose a + bi = 3 + 2i since $3^2 + 2^2 = 13$. Thus the ZAC sequence is

$$\begin{split} Nx(N-n) + a + bi &= 13 \\ \times &\{0, -1, i, -1, 1, i, i, -i, -i, -1, 1, -i, 1\} + 3 + 2i \\ &= \{3 + 2i, -10 + 2i, 3 + 15i, -10 + 2i, \\ &16 + 2i, 3 + 15i, 3 + 15i, 3 - 11i, 3 - 11i, -10 + 2i, \\ &16 + 2i, 3 - 11i, 16 + 2i\} \end{split}$$

This idea of this method can be extended by multiplying an integer or a Gaussian integer in step 2, and then we can have more choices in step 3. Let the length $N = a^2 + b^2$, then we can find an integer or a Gaussian integer s, satisfying $|s| = \sqrt{c^2 + d^2}$ with some integer c and d, and multiply this number to the GLS. The choices in step 3 can be doubled because

$$(a^{2}+b^{2})(c^{2}+d^{2}) = (ad+bc)^{2} + (ac-bd)^{2} = (ad-bc)^{2} + (ac+bd)^{2}$$

Thus by multiply different c + di we can get different ZAC sequences. This gives us infinite choices.

For instance, if N = 13, originally we can only choose $a + bi = \{3 + 2i, 3 - 2i, 2 + 3i, 2 - 3i\}$. When we multiply the GLS by $s = 5 = \sqrt{3^2 + 4^2}$, then in step 3 we have to find a + bi such that $a^2 + b^2 = 25 \times 13 = 325$, so the choices we have now are:

$$\{15+10i, 15-10i, 10+15i, 10-15i\}$$

which are the original ones multiplyed by 5, and

$$\{17+6i, 17-6i, 6+17i, 6-17i\}$$

since $17^2 + 6^2$ is also 325. Similarly, when we multiply the GLS by s = 2+i, we have to find a+bi such that $a^2+b^2 = 5 \times 13 = 65$, so the choices we have now are:

$$\{4+7i, 4-7i, 7-4i, 7+4i, 8-i, 8+i, 1+8i, 1-8i\}$$

where four of them are the original ones multiplyed by 2 + i.

$$\{4+7i, 8-i, 1+8i, 7-4i\} = (2+i) \\ \times \{3+2i, 3-2i, 2+3i, 2-3i\}$$

In summary, when N is a prime, LS can help us construct many interesting ZAC sequences in Gaussian integer. If N is a 4k + 1 prime, then we can further use GLS to construct more.

III. GENERATING INFINITE SEQUENCES FOR ARBITRARY LENGTH

In [9] a method for generating integer ZAC in arbitrary length N is proposed, but the drawback of that method is it can only generate a few number of sequences. On the other hand, in Section II we proposed methods using LS or GLS to obtain infinite number of sequences, but it can only applied to prime length. In this section we will introduce some methods to combine the sequences. Thus we can take the advantages of both sides, and get infinite number of sequences in arbitrary length.

A. Zero Padding and Convolution

First consider we factorize N to be pq, where gcd(p,q) = 1. We will take $N = p^n$ in next subsection. The simplest way to construct ZAC is by following these steps.

- 1) Take a ZAC from p and q.
- Interpolate q 1 and p 1 zeros to these signals to get two signals of length N.
- 3) Convolution these two signals, then we get a ZAC.
- Before we prove the claim, let see an example first.

Example III.1: Let p = 3 and q = 5, reuse the examples in our previous section. Take

 $F_3(k) = \{6 + 11i, 6 - 10i, 6 + 2i\}$

$$F_5(k) = \{2 + 1i, 7 + 1i, -3 + 1i, -3 + 1i, 7 + 1i\}$$

And by Step2 we get

$$egin{aligned} F_{3,15}(k) &= \{6+11i,0,0,0,0,6-10i,0,0,0,0,6\ &+2i,0,0,0,0\}\ &F_{5,15}(k) &= \{2+1i,0,0,7+1i,0,0,-3+1i,0,0,-4\} \end{aligned}$$

$$egin{aligned} &\mathcal{A}_{5,15}(k) = \{2+1i, 0, 0, 7+1i, 0, 0, -3+1i, 0, 0, -3+1i0, 0, 7\ &+1i, 0, 0\} \end{aligned}$$

And finally we circular convolution these two signals and get

$$F_{15}(k) = \{1 + 28i, -20 + 0i, 52 - 64i, 31 + 83i, -20 + 0i \\ 22 - 14i, -29 - 27i, 40 + 20i, 52 - 64i, -29 - 27i \\ 10 + 10i, -8 + 36i, 31 + 83i, 40 + 20i, -8 + 36i\}$$

which is ZAC with Gaussian integer.

The proof is very easy. It is based three trivial facts.

1) After zero padding, the new signal is still ZAC.

- 2) Convolution of two signals with Gaussian integer is still a signal with Gaussian integer.
- 3) If f_1 and f_2 is ZAC, then $f_1 * f_2$ is also. For details see [9]. The zero padding method can also be used to generate 2 Gaussian integer ZAC signals such that their cross-correlation has many zeros, as in this example, F_{15} and $F_{5,15}$. Recall that the cross-correlation of two signal f_a and f_b can be defined as

$$conj(f_a(-n))*f_b(n)$$

So the cross-correlation of F_{15} and $F_{5,15}$ is

$$\begin{aligned} &conj(F_{5,15}(-n))*F_{15} = conj(F_{5,15}(-n))*(F_{5,15}*F_{3,15}) \\ &= K\delta(n)*F_{3,15} = KF_{3,15} \end{aligned}$$

The last equation is due to the ZAC property of $F_{5,15}$. Thus the cross-correlation of these two signals will be $F_{3,15}$, which has 12 zeros.

B. Duplicate LS when $N = p^l$

When gcd(p,q) > 1, the zero padding method fails to generating "full" ZAC sequences. In other words, those ZAC sequences will have many zeros in them. In this section we will fix this problem by revisiting LS. We assume $N = p^l$ in this subsection because when $N = p_1^{l_1} p_2^{l_2} \dots$, we can use zero padding method and devide $N = N_1 N_2 \dots$, where $N_1 = p_1^{l_1}, N_2 = p_2^{l_2}$, etc. Since in [6] the even case has been solved, we assume p > 2.

Recall that in the theory of DFT, the signal duplicated m times will transform into a zero padding spectrum multiplied by m. For example,

$$f_a(n) = \{2, 1, 1\}, f_b(n) = \{2, 1, 1, 2, 1, 1, 2, 1, 1\}$$

$$F_a(k) = \{4, 1, 1\}, F_b(k) = \{12, 0, 0, 3, 0, 0, 3, 0, 0\}$$

As we can see the F_b is actually the zero padding version of F_a multiplied by 3.

Now we describe our method as follows.

- 1) Let d(n) be the LS duplicate p^{l-1} times.
- 2) Find *a*, *b*, and *c* satifying (1).

3) Then

$$f^{(l)}(n) = \begin{cases} d(n)\sqrt{N}c + bi, & gcd(n,N) = 1\\ f^{(l-1)}(n/p), & otherwise. \end{cases}$$

is CA, and the DFT of f(n) is ZAC in Gaussian integer. Note that this is a recursive definition while $f^{(1)}$ is the same as (2). The proof is similar to the N = p case so it is omitted here. To illustrate the idea, let's see an example.

Example III.2: Let $N=3^2$, and c=2, b=5, a=6+1i, since d(n) is

$$d(n) = \{0, 1, -1, 0, 1, -1, 0, 1, -1\}$$

The first iteration gives us

ł

$$egin{aligned} 0, 2\sqrt{3}+5i, -2\sqrt{3}+5i, 0, 2\sqrt{3}+5i, -2\sqrt{3}+5i, 0, \ &2\sqrt{3}+5i, -2\sqrt{3}+5i \} \end{aligned}$$

Now second (final) iteration eliminates the remaining zeros.

$$f(n) = \{6 + 1i, 2\sqrt{3} + 5i, -2\sqrt{3} + 5i \\ 2\sqrt{3} + 5i, 2\sqrt{3} + 5i, -2\sqrt{3} + 5i \\ -2\sqrt{3} + 5i, 2\sqrt{3} + 5i, -2\sqrt{3} + 5i\}$$

$$F(k) = \{6 + 41i, 6 - 10i, 6 + 2i, 6 - 22i, 6 - 10i, 6 + 2i \\ 6 + 14i, 6 - 10i, 6 + 2i\}$$

As this example points out, these steps are just eliminating zeros. So in this sense we have many degrees of freedom. For instance, we can change the sign of b in second iteration, or use 6 + 1i, 1 - 6i, 1 - 6i to fill up the three zeros

$$f(n) = \{6 + 1i, 2\sqrt{3} + 5i, -2\sqrt{3} + 5i 1 - 6i, 2\sqrt{3} + 5i, -2\sqrt{3} + 5i 1 - 6i, 2\sqrt{3} + 5i, -2\sqrt{3} + 5i \}$$

$$F(k) = \{8 + 19i, 5 + 7i, 5 + 7i, 8 - 44i, 5 + 7i, 5 + 7i 8 - 8i, 5 + 7i, 5 + 7i \}$$

One final words on dulpicated LS is that they are actually a special case of GLS.

This paper previously published in IEEE Signal Processing Letters

C. Factorize N and Prime-Factor Algorithm

The methods of zero padding and duplicated LS are very simple and might be useful enough for many applications, but theoretically more things can be done. Recall that DFT of size $N = N_1N_2$ can be done by taking DFT of size N_1 and N_2 seperately [14], if $gcd(N_1, N_2) = 1$, this property opens a door for us to divide the signal into several groups, and make sure the following ZAC condition holds

1) They are CA.

2) Each of them will transform to Gaussian integer.

For example, if N = 6 we rewrite our one dimension signal $f(n), n = 0, 1, 2, \dots, 5$ into

$$\begin{bmatrix} f(0) & f(3) \\ f(2) & f(5) \\ f(4) & f(1) \end{bmatrix}$$
(3)

The original 6-point DFT is equivalent to perform a 3-point DFT to each column and then 2-point DFT to each row. We do not worry about 2-point DFT since it transforms Gaussian integer into Gaussian integer, so if we ensure the outcome of 3-point DFT is Gaussian integer, then the result will be also. The zero padding method is actually a special case that makes (3) a rank 1 matrix, since the method is equivalent to the outer product of two CA signals. As we have discussed in Section II, LS can also be used to satisfy the condition, we will show an example later.

In general, when given an arbitrary length N, the procedures to generate ZAC sequence in Gaussian integer are

1) Divide $n = 0, 1, 2, \ldots, N - 1$ into groups S_d , where

$$S_d = \{n | gcd(n, N) = d\}$$

2) For each group, use LS or GLS to ensure ZAC condition holds

3) Take DFT

We now take an N = 15 for example, step by step

Example III.3: The factors of 15 is 1,3,5,15. *So we divide our signal into* 4 *groups*

$\Gamma f(0)$	0	ך 0		٢0	f(5)	f(10) ך	
0	0	0		0	0	0	
0	0	0	+	0	0	0	+
0	0	0		0	0	0	
L O	0	0		Lo	0	0]	
Γ 0	0	ך 0		٢O	0	0	٦
f(3)	0	0		0	f(8)	f(13)
f(6)	0	0	+	0	f(11)	f(1)	
f(9)	0	0		0	f(14)	f(4)	
$\lfloor f(12) \rfloor$	0	0		LO	f(2)	f(7)	

We consider the last term first. There are totally 4 GLS *can be applied, namely*

	Γ0	0 0	1	Γ0	0	0 7	
	0	$1 \ 1$		0	1	-1	
	0	$1 \ 1$,	0	1	-1	,
	0	$1 \ 1$		0	1	-1	
	Lo	$1 \ 1$]	LO	1	-1	
Γ0	0	0 -		0	0	0	٦
0	1	1		0	1	-1	
0	-1	-1	,	0	$^{-1}$	1	
0	-1	-1		0	-1	1	
Lo	1	1 _		LO	1	$^{-1}$]

One can notice that they are actually outer product of LS (or all one, which is GLS) of length 5 and 3. If we take DFT now, the first will have integer gain, as it is Ramanujan's Sum. The second will have $a\sqrt{3}i$ gain, the third will have $\sqrt{5}$, and the last will have $\sqrt{15}i$

Here is the critical point. In theory our choices for f(1) *may be in the form of*

$$a_1 + b_1i + c_1\sqrt{3} + d_1\sqrt{3}i + e_1\sqrt{5} + g_1\sqrt{5}i + h_1\sqrt{15} + k_1\sqrt{15}i$$

but we shall remeber that we are constructing CA, so

$$|f(1)| = |f(0)| = |f(3)| = |f(5)|$$

where f(0) should be in the form of a + bi, f(3) should be in the form of

$$a_3 + b_3i + e_3\sqrt{5} + g_3\sqrt{5}i$$

, and f(5) should be in the form of

$$a_5 + b_5i + c_5\sqrt{3} + d_5\sqrt{3}i$$

In practice we can use outer product instead of finding integers to satisfy constraints all of the above. But here we are giving an example to demonstrate that the solution exists and is not that hard to find. Since

$$61 = 6^2 + 5^2 = 1 + 2^2 \times 15 = 7^2 + 2^2 \times 3 = 4^2 + 3^2 \times 5$$

One possible outcome is

$\begin{bmatrix} 6+5i \end{bmatrix}$	$7i + 2\sqrt{3}$	$7i-2\sqrt{3}$
$4i+3\sqrt{5}$	$1i + 2\sqrt{15}$	$1i - 2\sqrt{15}$
$4i - 3\sqrt{5}$	$1i - 2\sqrt{15}$	$1i + 2\sqrt{15}$
$4i - 3\sqrt{5}$	$1i - 2\sqrt{15}$	$1i + 2\sqrt{15}$
$4i + 3\sqrt{5}$	$1i + 2\sqrt{15}$	$1i - 2\sqrt{15}$

which is CA, and its Fourier transform

6+43i	6+4i	6 + 16i 7
21 + 13i	21 - 41i	21 + 31i
-9 + 13i	-9+19i	-9-29i
-9 + 13i	-9+19i	-9 - 29i
21 + 13i	21 - 41i	21 + 31i

is in Gaussian integer. And this is not a rank 1 matrix.

IV. CONCLUSION

We propose several methods to generate zero autocorrelation sequences in Gaussian integer. If the sequence length is prime number, we can use Legendre symbol and provide more degree of freedom than Yang's method. If the sequence is composite, we develop a general method to construct ZAC sequences. Zero padding is one of the special cases of this method, and it is very easy to implement.

This paper previously published in IEEE Signal Processing Letters

REFERENCES

- [1] A. J. Viterbi, *Principles of spread spectrum communication*. Reading, MA, USA: Addison Wesley, 1995, CDMA.
- [2] E. Carni and A. Spalvieri, "Synchronous CDMA based on the cyclical translations of a CAZAC sequence," *IEEE Trans. Wireless Commun.*, 2005.
- [3] S. F. A. Shah and A. H. Tewfik, "Perfectly balanced binary sequences with optimal autocorrelation," in 14th IEEE Int. Conf. Electronics Circuits and Systems, 2007.
- [4] J. J. Benedetto, I. Konstantinidis, and M. Rangaswamy, "Phase-coded waveforms and their design," *IEEE Signal Process. Mag.*, vol. 26, pp. 22–31, 2009.
- [5] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th Ed. ed. Oxford, U.K.: Oxford University Press, ch. XVI.
- [6] H. Wei-Wen, W. Sen-Hung, and L. Chih-Peng, "Gaussian integer sequences with ideal periodic autocorrelation functions," in 2011 IEEE Int. Conf. Communications ICC, pp. 1–5.
- [7] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*. New York, NY, USA: Wiley-Interscience, 1998.

- [8] Y. Yang, X. Tang, and Z. Zhou, "Perfect gaussian integer sequences of odd prime length," *IEEE Signal Process. Lett.*, vol. 19, no. 10, pp. 615–618, Oct. 2012.
- [9] S.-C. Pei and K.-W. Chang, "On integer-valued zero autocorrelation sequences," in Signal and Information Processing Association Annu. Summit and Conf. (APSIPA), 2013, Oct.-Nov. 29-1, 2013, pp. 1–4.
- [10] X. Ma, Q. Wen, J. Zhang, and H. Zuo, "New perfect gaussian integer sequences of period pq," *IEICE Trans. Fund. Electron., Commun. Comput. Sci.*, vol. E96-A, no. 11, pp. 2290–2293.
- [11] L. G. Hua, *Introduction to Number Theory*. Berlin, Germany: Springer-Verlag, 1997.
- [12] M. R. Schroeder, Number Theory in Science and Communications. Berlin, Germany: Springer-Verlag, 1997.
- [13] S.-c. Pei, C.-C. Wen, and J.-J. Ding, "Closed-form orthogonal DFT eigenvectors generated by complete generalized legendre sequence," *IEEE Trans. Circuits Syst. 1*, vol. 55, no. 11, pp. 3469–3479, 2008.
- [14] I. J. Good, "The interaction algorithm and practical fourier analysis," J. Roy. Statist. Soc. B, vol. 20, no. 2, pp. 361–372.