Perfect Gaussian Integer Sequences of Arbitrary Length

Soo-Chang Pei* and Kuo-Wei Chang†

National Taiwan University* and Chunghwa Telecom†

Objectives

To construct perfect Gaussian integer sequences of arbitrary length N:

- Perfect sequences are sequences with zero autocorrelation.
- Gaussian integer is a number in the form $a+bi$ where a and b are integer.
- A Perfect Gaussian sequence is a perfect sequence that each value in the sequence is a Gaussian integer.
- Considering the sequence length, there are three cases: N is prime, N is a power of prime p^m or $N = pq$, where p and q are coprime but not necessary prime numbers.

Introduction

Perfect sequences are sequences with zero autocorrelation (ZAC).

$$\sum_{n=0}^{N-1} x^*(n-m)x(n) = C\delta(m)$$

for some constant C.

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).

$$|X(m)| = A$$

for some constant A.

When the sequence length is prime or power of prime, we can use Legendre symbol to construct perfect Gaussian integer sequences. 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.

For composite number, we propose some novel methods to construct perfect Gaussian integer sequences, from the naïve zero padding and convolution, to decomposing N into different groups.

$N = p$ or $N = p^m$ using Legendre sequence and Gauss sum

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

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

A well known result[5] is that

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

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

$$|a|^2 = b^2 + Nc^2 \qquad (1)$$

Then a sequence that

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

is CA, and the DFT of $f(n)$ is ZAC in Gaussian integer.

Example

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

Example

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

$$\{0, 2\sqrt{3}+5i, -2\sqrt{3}+5i, 0, 2\sqrt{3}+5i, -2\sqrt{3}+5i$$
$$0, 2\sqrt{3}+5i, -2\sqrt{3}+5i\}$$

Now second eliminates the remaining zeros.

$$\begin{aligned} f(n) =& \{6+1i, 2\sqrt{3}+5i, -2\sqrt{3}+5i \\ & 1-6i, 2\sqrt{3}+5i, -2\sqrt{3}+5i \\ & 1-6i, 2\sqrt{3}+5i, -2\sqrt{3}+5i\} \\ F(k) =& \{8+19i, 5+7i, 5+7i, 8-44i, 5+7i, 5+7i \\ & 8-8i, 5+7i, 5+7i\} \end{aligned}$$

$N = pq$ where p and q are coprime

Simple zero padding method:

1) Take a ZAC from p and q.

2) 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.

Using the idea of prime-factor algorithm:

Recall that DFT of size $N = N_1N_2$ can be done by taking DFT of size N_1 and N_2 seperately[14]. To construct perfect sequence, just

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

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

2) For each group, use LS or GLS to ensure CA

3) Take DFT

Example

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

$$\begin{bmatrix} f(0) & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & f(5) & f(10) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} +$$

$$\begin{bmatrix} 0 & 0 & 0 \\ f(3) & 0 & 0 \\ f(6) & 0 & 0 \\ f(9) & 0 & 0 \\ f(12) & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 0 & f(8) & f(13) \\ 0 & f(11) & f(1) \\ 0 & f(14) & f(4) \\ 0 & f(2) & f(7) \end{bmatrix}$$

One possible outcome is by

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

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

which is CA, and its Fourier transform

$$\begin{bmatrix} 6+43i & 6+4i & 6+16i \\ 21+13i & 21-41i & 21+31i \\ -9+13i & -9+19i & -9-29i \\ -9+13i & -9+19i & -9-29i \\ 21+13i & 21-41i & 21+31i \end{bmatrix}$$

is a perfect Gaussian integer sequence.

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.

References

[1] Viterbi, A. J., CDMA. Addison Wesley, 1995

[2] Carni, E., and Spalvieri, A. *IEEE Transactions on Wireless Communications*, 2005

[3] Shah, S. F. A., and Tewfik, A. H,*14th IEEE International Conference on Electronics Circuits and Systems*, 2007

[4] Benedetto, J.J., Konstantinidis, I. and Rangaswamy, M. *IEEE Signal Processing Magazine 26* , 2009.

[5] G. H. Hardy and E. M. Wright ,*Oxford University Press*,

[6] Hu, Wei-Wen and Wang, Sen-Hung and Li, Chih-Peng, *ICC*, 2011

[7] B. C. Berndt , R. J. Evans and K. S. Williams ,*A Wiley-Interscience publication*,1998

[8] Yang Yang, Xiaohu Tang, Zhengchun Zhou, *IEEE Signal Processing Letters* , 2012

[9] Soo-Chang Pei and Kuo-Wei Chang, *APSIPA*, 2013

[10] Xiuwen MA, Qiaoyan WEN, Jie ZHANG and Huijuan ZUO,'*IEICE*, Vol.E96-A, No.11, pp.2290-2293

[11] L. G. Hua, *Introduction to Number Theory*, 1997

[12] M. R. Schroeder,*Number Theory in Science and Communications*, 1997 :Springer-Verlag

[13] Pei, Soo-chang and Chia-Chang Wen and Jian-Jiun Ding, *IEEE Transactions on Circuits and Systems*, 2008

[14] Good, I. J., *Journal of the Royal Statistical Society*

Contact Information

- Email: pei@cc.ee.ntu.edu.tw
- Email: muslim@cht.com.tw

國立臺灣大學 National Taiwan University

中華電信研究院 Chunghwa Telecom Laboratories