Proceedings of the International MultiConference of Engineers and Computer Scientists 2016 Vol II,
IMECS 2016, March 16 - 18, 2016, Hong Kong

Perfect Gaussian Integer Sequences From Binary Idempotents

Chi-Yen Hung, Ping-Song Li, Chong-Dao Lee*

Abstract–**Gaussian integers are the complex numbers whose real and imaginary parts are both integers. Recently, Gaussian integer sequences with ideal autocorrelation, called the *perfect Gaussian integer sequences*, have been extensively used in code-division multiple-access and orthogonal frequency-division multiplexing (OFDM) systems. In this paper, binary idempotent is utilized to generate a set of integers and can be employed as the positions for a given Gaussian integer. The obtained perfect sequences are over two Gaussian integers and have high sequence energy. As the sequence length is large, their energy efficiency is close to 1 such that these sequences can be used to peak-to-average power ratio reduction in OFDM systems.**

Keywords: autocorrelation, Gaussian integers, idempotent, sequences

1 Introduction

Gaussian integers are the complex numbers whose real and imaginary parts are both integers. The complex sequence $\mathcal{S} = \{s(t)\}_{t=0}^{N-1}$ of length N, where $s(t) = u(t) + v(t)j$ for $u(t), v(t) \in \mathbb{Z}$, and $j = \sqrt{-1}$, is said to be a *perfect Gaussian integer sequence* if

$$R_{\mathcal{S}}(\tau) = \sum_{t=0}^{N-1} s(t)\overline{s(t+\tau)} \qquad (1)$$

is nonzero for $\tau = 0$ and is zero for any $1 \leq \tau \leq N-1$, where $\overline{a}$ denotes the conjugate of the complex number a. As described in [1], in order to reduce the peak-to-average power ratio (PAPR) in orthogonal frequency division multiplexing (OFDM) systems, Li *et al.* used the perfect sequences over Gaussian integers in the selected mapping schemes. To construct more sequences needed in communication systems, the perfect Gaussian integer sequences of arbitrary even lengths was proposed in [2] that uses six base sequences. At the same time, Yang *et al.* [3] constructed the perfect Gaussian integer sequences of prime length $N = p$ from the cyclotomic classes of orders 2 and 4 over the finite field $\mathbb{F}_p$. A generalization of the paper [3] was to construct the perfect Gaussian integer sequences of twin-primes length $p(p+2)$ using the Whiteman's generalized cyclotomy of order 2 over $\mathbb{Z}_{p(p+2)}$, see Ma *et al.* [4]. Different perfect Gaussian integer sequences of even lengths can be found in [5] that the interleaving method is employed. The perfect Gaussian integer sequences of arbitrary lengths have been investigated in [6] and [7]. For a class of odd length $2^m - 1$, where $m \geq 3$, it was shown in [8] that the trace representations over finite fields provided another approach to generate perfect Gaussian integer sequences.

In 1979, MacWilliams [9] presented a table of primitive binary idempotents of odd length N between 7 and 511. One of applications for idempotents is to construct cyclic codes, which are a class of error-correcting codes. To the best of the authors' knowledge, the present study is the first work that idempotents can be used to construct the perfect Gaussian integer sequences of some odd lengths. Some perfect Gaussian integer sequences of odd period are proposed in this paper. These sequences over Gaussian integers have the significant advantage of the energy efficiency with value close to 1. Due to the high energy efficiency, such sequences can be applied to the PAPR reduction in OFDM systems [10].

The organization of this paper is as follows: Section 2 provides the important properties and listed examples of idempotents. Section 3 constructs the perfect Gaussian integer sequences of some odd periods and gives the illustrated examples. Section 4 investigates the energy efficient of the obtained sequences. Finally, Section 5 summarizes this letter.

2 Idempotent

Let $\mathbb{F}_2 = \{0, 1\}$. Let N be a positive integer. A binary polynomial $e(x) = e_0 + e_1 x + \cdots + e_{N-1}x^{N-1}$, $e_i \in \mathbb{F}_2, 0 \leq i < N$, is called *idempotent* if $e^2(x) \equiv e(x)$.

Example 1 *Let $N = 7$. The idempotent $e(x)$ of length 7 can be the following four polynomials: $e_1(x) = 1 + x + x^2 + x^4$, $e_2(x) = x + x^2 + x^4$, $e_3(x) = 1 + x^3 + x^5 + x^6$, and $e_4(x) = x^3 + x^5 + x^6$.*

It is easily seen that a binary sequence 1110100 can express the coefficients of the polynomial $e_1(x)$ in Example

*C.-Y. Hung, P.-S. Li, and C.-D. Lee are Department of Communication Engineering, I-Shou University, Taiwan, R.O.C. Tel/Fax: 886-7-6577711/6578930 Emails: zxcasd84520@yahoo.com.tw, leo850406@yahoo.com.tw, chongdao@isu.edu.tw

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table 1: Idempotents for $7 \leq N \leq 511$

N	hexadecimal
7	e8
15	7ac8
31	85763e680
63	6885a52783731d7e
71	81164729716b1d977e
79	930b409e755186fd2f360
103	96380e9115bd964257768fe3960
127	921816c50769e137446b3997a9571f7e0
143	04314a07749d113e3b2583e756531bed5bde
199	92195692276883181d7e3d85d45e438147e73ee91bb69567b60
255	69c29059d90427d792971125196ab62f980dd23f0753586343c73dc99b795dfe
271	920d15b642339a3861580a1fc6dd5e913d437685449c07afe579e3a633bd92574fb60
359	8106142d13300cf7530e1b4541e4ef2a625b40bd539b71263542fd25b9ab08d87d5d278f3510cff3374bd79f7e
463	973e1bb806ce9e810138b5ac96f8850740565b948e33c9b1d779abd59176542a6114726c338ed62595fd1f5ee09 6ca52e37f7e868c9fe22783160
511	96793ad60adda26955c8a3a6c8192d876332e185891fdc6df48446820de3d52f6d4e0f09f8128533949317ebe2 a039f3ba31c4356579805d45a7bd0fb3735dfe0

1. Further, this binary sequence can be shown as the hexadecimal representation $e8$ listed in Table 1. As a result, Table 1 lists the hexadecimal representations for idempotents of some odd lengths N, where $7 \leq N \leq 511$, which can be used to generate the perfect Gaussian integer sequences. To end this section, the properties of binary idempotents are given in the following:

Property 1 *Let $A(x) = 1 + x + \cdots + x^{N-1}$ be all-one polynomial of degree $N-1$. The idempotents of odd length N in Table 1 have two properties:*
1. $e_i(x) = e_{i+1}(x) + 1$ for $i = 1, 3$.
2. $e_j(x) + e_{5-j}(x) = A(x)$ for $j = 1, 2$.

3 Proposed Gaussian Integer Sequences

To describe the construction method for the perfect Gaussian integer sequences, some definitions are first introduced.

Now, denote $B_N = \{b(t)\}_{t=0}^{N-1}$, where $b(t)$ is either 0 or 1, by a binary sequence of length N which is obtained from the idempotent of length N. Let G_1 and G_2 be two Gaussian integers.

An observation of Table 1 indicates that the length N can be divided into three cases: $N = 2^{2k+1} - 1$, $N = 2^{2k} - 1$, and $N = 4 \times (19 + 2 \times \sum_{i=1}^{k}(2i - 3)) + 3$. Below, three theorems are given.

Theorem 1 *A perfect Gaussian integer sequence of odd length $N = 2^{2k+1} - 1$ over two Gaussian integers $G_1 = 2^{k-1} + (2^{k-1} + 1)j$ and $G_2 = -2^{k-1} - 2^{k-1}j$ can be constructed by*

$$s(t) = \begin{cases} G_1, & \text{for } b(t) = 1 \\ G_2, & \text{for } b(t) = 0 \end{cases} \tag{2}$$

for $k \geq 1$, $0 \leq t < N$, and $b(t) \in B_N$.

Proof: This proof is due to the fact that binary sequence B_N is the characteristic sequence of the $(N, (N-1)/2, (N-3)/4)$ cyclic difference set (see [8]).

Example 2 *Consider $k = 2$ and $N = 2^{2k+1} - 1 = 31$. It follows from Theorem 1 that combining two Gaussian integers $G_1 = 2 + 3j$ and $G_2 = -2 - 2j$ and $B_{31} = 1000010101110110001111100110100$ yields the perfect Gaussian integer sequence*

$$\begin{aligned}\mathcal{S} = (&\underbrace{2+3j}_{0}, -2-2j, -2-2j, -2-2j, -2-2j, \underbrace{2+3j}_{5}, \\ &-2-2j, \underbrace{2+3j}_{7}, -2-2j, \underbrace{2+3j}_{9}, \underbrace{2+3j}_{10}, \underbrace{2+3j}_{11}, \\ &-2-2j, \underbrace{2+3j}_{13}, \underbrace{2+3j}_{14}, -2-2j, -2-2j, -2-2j, \\ &\underbrace{2+3j}_{18}, \underbrace{2+3j}_{19}, \underbrace{2+3j}_{20}, \underbrace{2+3j}_{21}, \underbrace{2+3j}_{22}, -2-2j, \\ &-2-2j, \underbrace{2+3j}_{25}, \underbrace{2+3j}_{26}, -2-2j, \underbrace{2+3j}_{28}, -2-2j, \\ &-2-2j).\end{aligned}$$

Theorem 2 *A perfect Gaussian integer sequence of odd length $N = 2^{2k} - 1$ over two Gaussian integers $G_1 = -2^{k-1} - 2^{k-1}j$ and $G_2 = (2^{k-1} - 1) + (2^{k-1} + 1)j$ can be constructed by (2) for any positive integer k.*

Proof: The proof of this theorem is analogous to the proof of Theorem 1.

Example 3 *Let $k = 2$ and $N = 2^{2k} - 1 = 15$. There exist two Gaussian integers $G_1 = -2-2j$, $G_2 = 1+3j$ and the sequence $B_{15} = 011110101100100$ such that the perfect Gaussian integer sequence of length 15 is determined from Theorem 2 as*

$$\begin{aligned}\mathcal{S} = (1+3j, &\underbrace{-2-2j}_{1}, \underbrace{-2-2j}_{2}, \underbrace{-2-2j}_{3}, \underbrace{-2-2j}_{4},\\ &1+3j, \underbrace{-2-2j}_{6}, 1+3j, \underbrace{-2-2j}_{8}, \underbrace{-2-2j}_{9},\\ &1+3j, 1+3j, \underbrace{-2-2j}_{12}, 1+3j, 1+3j).\end{aligned}$$

Theorem 3 *A perfect Gaussian integer sequence of odd length $N = 4 \times (19 + 2 \times \sum_{i=1}^{k}(2i-3)) + 3$ over two Gaussian integers $G_1 = (-2-k) + (-4+k)j$ and $G_2 = (1+k) + (4-k)j$ can be constructed by (2) for $1 \le k \le 8$.*

Proof: This proof is similar to that of Theorem 1.

Example 4 *Consider $k = 1$ and $N = 4 \times 17 + 3 = 71$. For $G_1 = -3-3j$, $G_2 = 2+3j$, and $B_{71} = 10000001 00010110010001110010100101110001011010110001110110 0101110111111$, in Theorem 3, there is a sequence*

$$\begin{aligned}\mathcal{S} = (&\underbrace{-3-3j}_{0}, 2+3j, 2+3j, 2+3j, 2+3j, 2+3j, 2+3j,\\ &\underbrace{-3-3j}_{7}, 2+3j, 2+3j, 2+3j, \underbrace{-3-3j}_{11}, 2+3j,\\ &\underbrace{-3-3j}_{13}, \underbrace{-3-3j}_{14}, 2+3j, 2+3j, \underbrace{-3-3j}_{17}, 2+3j,\\ &2+3j, 2+3j, \underbrace{-3-3j}_{21}, \underbrace{-3-3j}_{22}, \underbrace{-3-3j}_{23}, 2+3j,\\ &2+3j, \underbrace{-3-3j}_{26}, 2+3j, \underbrace{-3-3j}_{28}, 2+3j, 2+3j,\\ &\underbrace{-3-3j}_{31}, 2+3j, \underbrace{-3-3j}_{33}, \underbrace{-3-3j}_{34}, \underbrace{-3-3j}_{35}, 2+3j,\\ &2+3j, 2+3j, \underbrace{-3-3j}_{39}, 2+3j, \underbrace{-3-3j}_{41}, \underbrace{-3-3j}_{42},\\ &2+3j, \underbrace{-3-3j}_{44}, 2+3j, \underbrace{-3-3j}_{46}, \underbrace{-3-3j}_{47}, 2+3j,\\ &2+3j, 2+3j, \underbrace{-3-3j}_{51}, \underbrace{-3-3j}_{52}, \underbrace{-3-3j}_{53}, 2+3j,\\ &\underbrace{-3-3j}_{55}, \underbrace{-3-3j}_{56}, 2+3j, 2+3j, \underbrace{-3-3j}_{59}, 2+3j,\\ &\underbrace{-3-3j}_{61}, \underbrace{-3-3j}_{62}, \underbrace{-3-3j}_{63}, 2+3j, \underbrace{-3-3j}_{65},\\ &\underbrace{-3-3j}_{66}, \underbrace{-3-3j}_{67}, \underbrace{-3-3j}_{68}, \underbrace{-3-3j}_{69}, \underbrace{-3-3j}_{70}).\end{aligned}$$

4 Energy Efficiency

As has been reported in [8], the energy efficiency $\eta_{\mathcal{Z}}$ of the time-discrete sequence $\mathcal{Z} = \{z(t)\}_{t=0}^{N-1}$ of length N is denoted to be

$$\eta_{\mathcal{Z}} = \frac{E_{\mathcal{Z}}}{\max_{0 \le t < N} |z(t)|^2}, \tag{3}$$

where $E_{\mathcal{Z}} = (1/N) \times \sum_{t=0}^{N-1} |z(t)|^2$ is the average energy of a sequence $\mathcal{Z}$.

For the perfect Gaussian integer sequences derived from three theorems in the foregoing section, their energy efficiency is discussed below:

Corollary 1 *Let $\mathcal{S}$ be the perfect sequence of length $N = 2^{2k+1} - 1$ with two Gaussian integers $G_1 = 2^{k-1} + (2^{k-1} + 1)j$ and $G_2 = -2^{k-1} - 2^{k-1}j$. If the numbers of G_1 and G_2 appeared in the sequence $\mathcal{S}$ are 2^{2k} and $2^{2k} - 1$, respectively, then its energy efficiency $\eta_{\mathcal{S}}$ is exactly*

$$\eta_{\mathcal{S}} = \frac{2 \times 2^{4k} + 2 \times 2^{3k} + 2^{2k}}{(2^{2k} + 2^{k+1} + 2)(2 \times 2^{2k} - 1)} \tag{4}$$

and is approximately 1 as $k \to \infty$.

Proof: A substitution of $N = 2^{2k+1} - 1$, $|G_1|^2 = 2^{2k-1} + 2^k + 1$, and $|G_2|^2 = 2^{2k-1}$ into (3) yields (4). Furthermore, (4) becomes

$$\eta_{\mathcal{S}} = 1 - \frac{2^{3k+1} + 2^{2k+1} - 2^{k+1} - 2}{2^{4k+1} + 2^{3k+2} + 2^{2k+2} - 2^{2k} - 2^{k+1} - 2}.$$

It is easy to see that the highest power $4k+1$ of 2 in the denominator is larger than the power $3k+1$ of 2 in the numerator. If $k \to \infty$, or equivalently, $N \to \infty$, then $\eta_{\mathcal{S}} \to 1$. The proof of this corollary is complete.

Corollary 2 *Let $\mathcal{S}$ be the perfect Gaussian integer sequence of length $N = 2^{2k} - 1$. If the numbers of $G_1 = -2^{k-1} - 2^{k-1}j$ and $G_2 = (2^{k-1} - 1) + (2^{k-1} + 1)j$ appeared in the sequence $\mathcal{S}$ are 2^{2k-1} and $2^{2k-1} - 1$, respectively, then its energy efficiency $\eta_{\mathcal{S}}$ is exactly*

$$\eta_{\mathcal{S}} = \frac{2^{4k} + 2^{2k} - 2^2}{(2^{2k} + 2^2)(2^{2k} - 1)} \tag{5}$$

and is approximately 1 as $k \to \infty$.

Proof: Substituting $N = 2^{2k} - 1$, $|G_1|^2 = 2^{2k-1}$, and $|G_2|^2 = 2^{2k-1} + 2$ into (3) yields (5), which can also be expressed as

$$\eta_{\mathcal{S}} = 1 - \frac{2^{2k+2} - 2^{2k+1}}{2^{4k} + 2^{2k+2} - 2^{2k} - 2^2}.$$

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

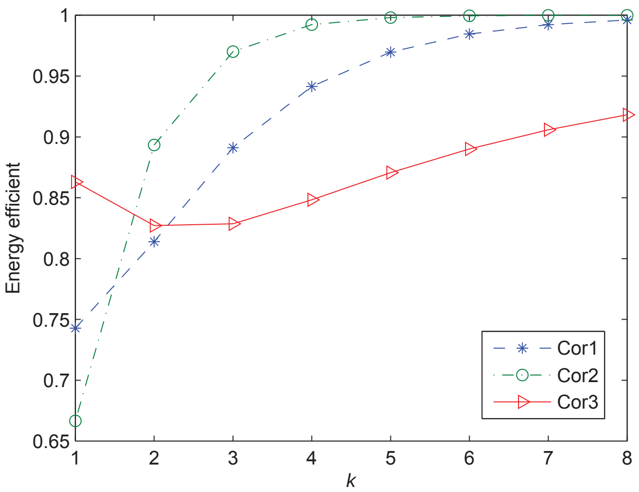

Figure 1: Energy efficiency of the proposed sequences $\mathcal{S}$.

Clearly, the highest power $4k$ of 2 in the denominator is larger than the power $2k + 2$ of 2 in the numerator. If $k \to \infty$, then $\eta_{\mathcal{S}} \to 1$, which completes the proof of this corollary.

Corollary 3 *Let $\mathcal{S}$ be the perfect sequence of length $N = 4 \times (19 + 2 \times \sum_{i=1}^{k}(2i - 3)) + 3$ with two Gaussian integers $G_1 = (-2 - k) + (-4 + k)j$ and $G_2 = (1 + k) + (4 - k)j$, where $1 \leq k \leq 8$. If the numbers of G_1 and G_2 appeared in the sequence $\mathcal{S}$ are $(N + 1)/2$ and $(N - 1)/2$, respectively, then its energy efficiency $\eta_{\mathcal{S}}$ is exactly*

$$\eta_{\mathcal{S}} = \frac{4Nk^2 - 10Nk + 37N + 2k + 3}{4N(k^2 - 2k + 10)}. \tag{6}$$

Proof: Since $|G_1|^2 = (-2 - k)^2 + (-4 + k)^2$ and $|G_2|^2 = (1 + k)^2 + (4 - k)^2$, it is easy to check that $|G_1|^2 > |G_2|^2$ for $k = 1, \ldots, 8$. As a consequence, the energy efficiency in (3) has the form

$$\begin{aligned} \eta_{\mathcal{S}} &= \frac{\frac{(N+1)}{2} \times |G_1|^2 + \frac{(N-1)}{2} \times |G_2|^2}{N \times |G_1|^2} \\ &= \frac{4Nk^2 - 10Nk + 37N + 2k + 3}{4N(k^2 - 2k + 10)}. \end{aligned} \tag{7}$$

Figure 1 plots the energy efficiency $\eta_{\mathcal{S}}$ in (5), (6), and (7) for $1 \leq k \leq 8$. An observation in this figure reveals that the perfect Gaussian integer sequences $\mathcal{S}$ constructed from Theorems 1 and 2 have high energy efficiency with value close to 1 when k is large. It is also shown that, for $\mathcal{S}$ described in Theorem 3, their energy efficiency $\eta_{\mathcal{S}}$ is between 0.80 and 0.95.

5 Conclusions and Future Work

This paper has presented the perfect Gaussian integer sequences which can be constructed from binary idempotents. These sequences are over two Gaussian integers and have the high energy efficiency. In the future work, it is of interest to investigate the sequences over more than two Gaussian integers.

Acknowledgment

The work was supported by Ministry of Science and Technology, Taiwan, under Grant MOST104-2221-E-214-009.

References

[1] Li, C.-P., Wang, S.-H., Wang, C.-L., "Novel Low-Complexity SLM Schemes for PAPR Reduction in OFDM Systems," *IEEE Trans on Signal Processing*, V58, N5, pp. 2916-2921, 5/10

[2] Hu, W.-W., Wang, S.-H., Li, C.-P., "Gaussian Integer Sequences With Ideal Periodic Autocorrelation Functions," *IEEE Trans on Signal Processing*, V60, N11, pp. 6074-6079, 11/12

[3] Yang, Y., Tang, X., Zhou, Z., "Perfect Gaussian Integer Sequences of Odd Prime Length," *IEEE Signal Processing Letters*, V19, N10, pp. 615-618, 10/12

[4] Ma, X., Wen, Q., Zhang, J., Zuo, H., "New Perfect Gaussian Integer Sequences of Period pq," *IEICE Trans Fundamentals of Electronics, Communications & Computer Sciences*, VE96-A, N11, pp. 2290-2293, 11/13

[5] Peng X., Xu, C., "New Constructions of Perfect Gaussian Integer Sequences of Even Length," *IEEE Communications Letters*, V18, N9, pp. 1547-1550, 9/14

[6] Chang, H.H., Li, C.P., Lee, C.D., Wang, S.H., Wu, T.C., "Perfect Gaussian Integer Sequences of Arbitrary Composite Length," *IEEE Trans on Information Theory*, V61, N7, pp. 4107-4115, 7/15

[7] Pei S.C., Chang, K.W., "Perfect Gaussian Integer Sequences of Arbitrary Length," *IEEE Signal Processing Letters*, V22, N8, pp. 1040-1044, 8/15

[8] Lee, C.D., Huang, Y.P., Chang, Y., Chang, H.H., "Perfect Gaussian Integer Sequences of Odd Period $2^m - 1$," *IEEE Signal Processing Letters*, V22, N7, pp. 881-885, 7/15

[9] MacWilliams, F.J., "A Table of Primitive Binary Idempotents of Odd Length n, $7 \leq n \leq 511$," *IEEE Trans on Information Theory*, VIT-25, N1, pp. 118-121, 1/79

[10] Wang, S.H., Li, C.P., Lee, K.C., Su, H.J., "A New Low-Complexity Precoded OFDM System With Reduced PAPR," *IEEE Trans on Signal Processing*, V63, N6, pp. 1366-1376, 6/15

ISBN: 978-988-14047-6-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)