Arbitrary Length Reducible and Irreducible Perfect Gaussian Integer Sequences with A Pre-Given Gaussian Integer

Soo-Chang Pei
Dept. of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.
pei@cc.ee.ntu.edu.tw

Kuo-Wei Chang
Telecommunication Laboratories
Chunghwa Telecom
Taoyuang, Taiwan, R.O.C.
muslim@cht.com.tw

***Abstract*—In this paper we will discuss two construction schemes on arbitrary length perfect Gaussian integer sequence (PGIS) with a pre-given constant. The first scheme uses geometric series, which brings reducible PGIS. We will also discuss the irreducible case and find an easy way to obtain PGIS for even length. Moreover, the same concept can be applied for some odd length $N = 3p$ by using Ramanujan's Sum. Concrete examples are provided.**

***Index Terms*—Discrete Fourier transform, perfect Gaussian integer sequences, zero autocorrelation, Ramanujan's Sum**

I. Introduction

A finite sequence $x(n)$ with length N is called perfect or zero autocorrelation (ZAC) if its autocorrelations satisfy

$$R_{xx}(m) = \sum_{n=0}^{N-1} \overline{x(n-m)}x(n) = C\delta(m), \tag{1}$$

for all integer m and some constant C. The notation $\overline{x}$ is the complex conjugate of x, $\delta(n)$ is the delta function such that

$$\delta(n) = \begin{cases} 1 & n = 0 \\ 0 & n \neq 0 \end{cases}, \tag{2}$$

and the index $n \triangleq (n \mod N)$, in every sequence $x(n)$.

In particular, a sequence $x(n)$ is called perfect Gaussian integer sequence (PGIS) if it is perfect and complex integer valued

$$x(n) \in \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\},$$

where $i = \sqrt{-1}$.

There are many kinds of perfect sequences, and their applications can be found in many research topics. In particular, perfect integer or Gaussian integer sequences have been studied a lot [1]–[14] over the years because they have many applications such as code division multiple access (CDMA) [10], equalization, synchronization, channel estimation, cell search and CW radar [11], [15]. A survey of the perfect Gaussian integer sequences can be found in the reference [11]. In addition, in the Chapter 7 of [16], Fanxin Zeng et al. have a complete discussion on perfect sequences and perfect arrays for communications.

Recently a special kind of perfect Gaussian integer sequence is discussed [17]. More precisely, this PGIS is further constrained to contain a pre-given Gaussian integer $c = a + bi$. In [17], some methods for even length are proposed, but non of these methods can be generalized to odd case.

Naïvely, if we can generate a PGIS $x(n)$ which contains a "1", then the desired PGIS can be obtained by multiplying $x(n)$ with c. In other words, $c \cdot x(n)$ is a PGIS with a pre-given Gaussian integer. We call this PGIS *reducible*.

Definition 1. *A Gaussian integer sequence $y(n)$ is* reducible *if there exists a Gaussian integer c and another Gaussian integer sequence $x(n)$ such that*

$$y(n) = c \cdot x(n).$$

Otherwise, it is called irreducible.

In Section III, we will prove that for any sequence length N, there exists a reducible PGIS with any pre-given constant $c = a + bi$. The irreducible PGIS construction, however, is still an open problem. In Section IV, we will discuss how to solve this in some special cases.

II. Preliminary

The discrete Fourier transform (DFT) of $x(n)$ is defined as

$$\hat{x}(m) = \sum_{n=0}^{N-1} x(n) W_N^{nm}, \tag{3}$$

where $n, m \in \{0, 1, 2, ..., N-1\}$, $W_N = e^{\frac{-2\pi i}{N}}$.

We define constant amplitude (CA) as follows.

Definition 2. *A sequence $x(n)$ is constant amplitude (CA) if*

$$|x(n)| = A, \tag{4}$$

for some constant A

A very useful theorem about how CA and ZAC are related states as follows.

Theorem 1. *A sequence x is CA if and only if its DFT $\hat{x}$ is ZAC. Similarly, a sequence x is ZAC if and only if its DFT $\hat{x}$ is CA.*

Proof. See [18]. □

A sequence $s_{N,d}(n)$ is called *gcd-delta* function if

$$s_{N,d}(n) = \delta(d - \gcd(N,n)) = \begin{cases} 1, & \gcd(N,n) = d \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

where $\gcd(a,b)$ is the greatest common divisor of two integers a and b. The DFT of gcd-delta fucntion is called Ramanujan's Sum [19].

$$\hat{s}_{N,d}(m) = \sum_{n=0}^{N-1} s_{N,d}(n) W_N^{nm} = \sum_{\substack{n=1 \\ \gcd(n,N)=d}}^{N} W_N^{nm} \tag{6}$$

It is noted that despite (6) is a complex sum, $\hat{s}_{N,d}(m)$ is always integer.

Example 1.

$$s_{6,2} = [0,0,1,0,1,0]^T,$$
$$\hat{s}_{6,2} = [2,-1,-1,2,-1,-1]^T$$

where T means vector transpose.

III. Arbitrary length reducible PGIS with a pre-given constant

As we have discussed in the introduction, generating reducible PGIS is equivalent to finding a PGIS which contains at least an "1". In other words, we want to find a PGIS $x(n)$ such that

$$x(k) = 1 \tag{7}$$

for some integer k. There are some perfect integer sequences derived from difference set [8], [20]–[25] which have this property. Recall that a (v,k,λ) difference set is a subset D of size k of a group G of order v such that every nonidentity element of G can be expressed as a product $d_1 d_2^{-1}$ of elements of D in exactly λ ways.

For a concrete example, if $N = 7$ then

$$x(n) = [-1,1,1,0,1,0,0]^T \tag{8}$$

is a perfect sequence derived from (7,3,1) difference set. However, this method cannot be applied to arbitrary length since difference sets only exist for some N.

Luckily in [13], a construction method for PGIS from geometric series is proposed, which can be applied to arbitrary N. The first step is choosing a ratio $z, |z| = r \neq 1$ and let

$$y(n) = z^n = [1, z^1, z^2, ..., z^{N-1}]. \tag{9}$$

The DFT of $y(n)$ is

$$\hat{y}(m) = \sum_{n=0}^{N-1} z^n W_N^{nm} \tag{10}$$

$$= \frac{1 - z^N}{1 - zW^m} \tag{11}$$

To make $\hat{y}$ CA, so that y is ZAC, we can use the following theorem.

Theorem 2. *For any complex number $z' = re^{i\theta}$, where $r = |z'| \neq 1$,*

$$\left| \frac{1}{1-z'} - \frac{1}{1-r^2} \right| = \left| \frac{r}{1-r^2} \right| \tag{12}$$

In other words, the magnitude of $\frac{1}{1-z'} - \frac{1}{1-r^2}$ only depends on r and is independent to θ.

Proof. See [13]. □

Applying Theorem 2 to (11) and assume

$$\hat{f}(m) = \hat{y}(m) - \frac{1-z^N}{1-r^2} = (1-z^N)\left(\frac{1}{1-zW^m} - \frac{1}{1-r^2}\right). \tag{13}$$

In other words, let $z' = zW^m$

$$|\hat{f}(m)| = \left|(1-z^N)\left(\frac{1}{1-z'} - \frac{1}{1-r^2}\right)\right| = |1-z^N| \left|\frac{r}{1-r^2}\right|. \tag{14}$$

is CA, which implies the inverse DFT of $\hat{f}(m)$

$$f(n) = \begin{cases} 1 - \frac{1-z^N}{1-r^2}, & n = 0 \\ z^n, & \text{otherwise.} \end{cases} \tag{15}$$

is ZAC.

However, f do not have any "1" in general. Moreover, $f(0)$ is not a Gaussian integer if $|1 - r^2| > 1$. To solve these problems, the final construction step is let $z = 1 + i$. Note that $r = |z| = \sqrt{2}$ and $\frac{1}{1-r^2} = -1$.

$$f(n) = \begin{cases} 1 - \frac{1-z^N}{1-r^2}, & n = 0 \\ z^n, & \text{otherwise} \end{cases} \tag{16}$$

$$= \begin{cases} 2 - z^N, & n = 0 \\ z^n, & \text{otherwise} \end{cases} \tag{17}$$

Therefore, by $2 = (1+i)(1-i) = z(1-i)$

$$x(n) = \frac{f(n)}{z} = \begin{cases} (1-i) - (1+i)^{N-1} & n = 0 \\ (1+i)^{n-1}, & \text{otherwise} \end{cases} \tag{18}$$

is a PGIS. When $n = 1$, $x(1) = 1$.

We summarize the above discussion as the following theorem.

Theorem 3 (Main Result)**.** *For any length N, there exists a PGIS with one "1". In particular,*

$$x(n) = \begin{cases} (1-i) - (1+i)^{N-1}, & n = 0 \\ (1+i)^{n-1}, & \textit{otherwise} \end{cases} \tag{19}$$

is an example, where $x(1) = 1$.

Example 2 (Odd and prime case)**.** *Let $N = 3$,*

$$x(n) = \begin{bmatrix} 1-3i \\ 1 \\ 1+i \end{bmatrix} \tag{20}$$

is a PGIS.

Example 3 (Even and non-prime case)**.** *Let $N = 4$,*

$$x(n) = \begin{bmatrix} 3-3i \\ 1 \\ 1+i \\ (1+i)^2 \end{bmatrix} = \begin{bmatrix} 3-3i \\ 1 \\ 1+i \\ 2i \end{bmatrix} \tag{21}$$

is a PGIS. In fact, the DFT of $x(n)$

$$\hat{x}(m) = [5, -5i, 3-4i, 4-3i]^T \tag{22}$$

which is obviously CA with $A = 5$.

From these examples we can observe that this method can be applied no matter N is even or odd.

Note: We just use the case $z = 1+i$ to prove the existence, but in fact, as long as we can find z such that

$$f(0) = 1 - \frac{1-z^N}{1-r^2} = z(a+bi)$$

is a Gaussian integer multiplied by z, then by (15) we can derive another PGIS with "1".

Example 4. *Let $N = 4$ and $z = 1+2i$. By* (15)*,*

$$f(n) = \begin{cases} 1 - \frac{1-z^N}{1-r^2}, & n = 0 \\ z^n, & \textit{otherwise} \end{cases} \tag{23}$$

$$= [3+6i, 1+2i, -3+4i, -11-2i]\,. \tag{24}$$

We can note that $f(0) = 3(1+2i) = 3z$, therefore,

$$x(n) = \frac{f(n)}{z} = [3, 1, 1+2i, -3+4i] \tag{25}$$

is another PGIS with "1", which is not *derived from theorem 3.*

IV. Irreducible PGIS with pre-given constant

The PGIS derived from Theorem 3 is reducible and has high dynamic range. The largest value with $z = 1+i, |z| = \sqrt{2}$ will be $|z^{N-1}| = 2^{\frac{N-1}{2}}$ while the smallest one is 1. Meanwhile, [17] proposed some algorithms to construct irreducible PGIS, but only suitable for even length. In this section, we will briefly introduce a method to make even length PGIS with pre-given constant, which is slightly different from [17]. Then we will extend it to some odd length. More precisely, the proposed method can applied to $N = 3p$ where $p > 3$ is a prime number.

A. Even length construction

Assume the sequence length $N = 2K$ for some positive integer K. Define two sequences $x_1(n)$ and $x_2(n)$,

$$x_1(n) = \begin{cases} 1, & n \text{ is odd,} \\ 0, & n \text{ is even} \end{cases}, \tag{26}$$

$$x_2(n) = \begin{cases} K-1 & n = 0 \\ -1, & n \neq 0, n \text{ is even,} \\ 0, & n \text{ is odd} \end{cases}. \tag{27}$$

The DFT of x_1 and x_2 are

$$\hat{x}_1(m) = \begin{cases} K, & n = 0 \\ -K, & n = K \\ 0, & \text{otherwise} \end{cases}, \tag{28}$$

$$\hat{x}_2(m) = \begin{cases} 0 & n = 0, K \\ K & \text{otherwise.} \end{cases}. \tag{29}$$

In other words, $|\hat{x}_1|$ and $|\hat{x}_2|$ are binary and complement to each other. Therefore, for any pre-given Gaussian integer c, if we can find another Gaussian integer c', such that $|c'| = |c|$, then

$$x(n) = c \cdot x_1(n) + c' \cdot x_2(n) \tag{30}$$

is a PGIS with c, since $\hat{x}$ is CA. In particular, $|\hat{x}(m)| = K|c|$ for all m.

Example 5. *Let $N = 6$ and $c = 1+2i$, by definition, (Equations* (26) *to* (29)*)*

$$x_1(n) = [0, 1, 0, 1, 0, 1]^T\,, \tag{31}$$

$$x_2(n) = [2, 0, -1, 0, -1, 0]^T\,, \tag{32}$$

and

$$\hat{x}_1(m) = [3, 0, 0, -3, 0, 0]^T\,, \tag{33}$$

$$\hat{x}_2(m) = [0, 3, 3, 0, 3, 3]^T\,. \tag{34}$$

Suppose we choose $c' = 1-2i$, then the final PGIS is

$$x(n) = c \cdot x_1(n) + c' \cdot x_2(n) \tag{35}$$

$$= \begin{bmatrix} 2-4i \\ 1+2i \\ -1+2i \\ 1+2i \\ -1+2i \\ 1+2i \end{bmatrix} \tag{36}$$

It is noted that $x(n)$ is irreducible since $1+2i$ and $-1+2i$ has no common factor.

The amplitude of x from the example above is shown in Figure 2a, and its auto-correlation R_{xx} is demonstrated in Figure 2b. Note that $R_{xx}(m) = 0$ for all $m \neq 0$. In Figure 2c, additional noise has been added $y = x + n$, where n in Gaussian noise with variance equal to 1. The auto-correlation R_{yy} is illustrated in Figure 2d. $R_{yy}(0)$ has at least 7db gain compared to other $m \neq 0$. As result, it shows that ZAC sequence can be applied in synchronization under noise environment.

B. Odd length construction using Ramanujan's Sum when $N = 3p$

From the last section we have learned the tricks to construct an irreducible PGIS with pre-given constant. First we must choose two integer sequences x_1 and x_2 such that

- In time domain, there is an index k such that $x_1(k) = 1$ and $x_2(k) = 0$.

$$
\begin{aligned}
\hat{s}_{15,15}(n) &= [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]^T\,, \\
\hat{s}_{15,1}(n) &= [8,1,1,-2,1,-4,-2,1,1,-2,-4,1,-2,1,1]^T \\
\hat{s}_{15,3}(n) &= [4,-1,-1,-1,-1,4,-1,-1,-1,-1,4,-1,-1,-1,-1]^T \\
\hat{s}_{15,5}(n) &= [2,-1,-1,2,-1,-1,2,-1,-1,2,-1,-1,2,-1,-1]^T
\end{aligned}
$$

Fig. 1: Ramanujan's Sum for $N = 15$, where T means vector transpose .

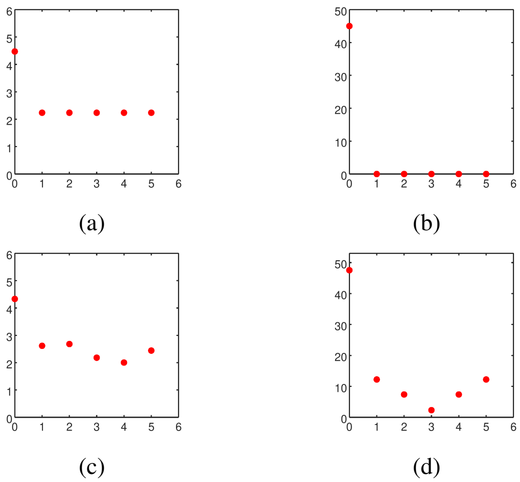

Fig. 2: An experiment of auto-correlation against noise. (a) The absolute value of signal x in eq. (36); (b) the auto-correlation of x, which is perfect; (c) the absolute value of signal x in eq. (36) with additional noise; (d) The auto-correlation of (c).

- In frequency domain, there is a set of integer $\mathbb{S}$ and a constant A such that

$$
\begin{cases}
|\hat{x}_1(m)| = A, |\hat{x}_2(m)| = 0, & \forall s \in \mathbb{S} \\
|\hat{x}_1(m)| = 0, |\hat{x}_2(m)| = A, & \forall s \notin \mathbb{S}
\end{cases}.
$$

Then for any pre-given Gaussian integer c, we can choose another Gaussian integer c' such that $|c'| = |c|$. Note that this c' always exists because we can choose the complex conjugate of c. Finally we can use (30) to construct the desired PGIS.

Now we generalize this concept into $N = 3p, p > 3$, where p is a prime number. There are 4 factors of N, which are $1, 3, p, N$. And we choose

$$x_1(n) = \hat{s}_{N,N}(n) = 1, \forall n \tag{37}$$
$$x_2(n) = -\hat{s}_{N,1}(n) + \hat{s}_{N,3}(n) + \hat{s}_{N,p}(n-1) \tag{38}$$

where $\hat{s}$ is the Ramanujan's Sum defined in (6).

Example 6. *Let $p = 5$ and $N = 15$. The 4 Ramanujan's Sum are given in Figure 1. Therefore, it is easy to have*

$$x_1(1) = 1 \tag{39}$$
$$
\begin{aligned}
x_2(1) &= -\hat{s}_{15,1}(1) + \hat{s}_{15,3}(1) + \hat{s}_{N,5}(0) \\
&= -1 - 1 + 2 = 0
\end{aligned} \tag{40}
$$

which satisfies the above first condition in time domain.

On the other hand, it can be verified that

$$
\begin{cases}
|\hat{x}_1(m)| = 15, |\hat{x}_2(m)| = 0, & m = 0 \\
|\hat{x}_1(m)| = 0, |\hat{x}_2(m)| = 15, & m \neq 0
\end{cases}. \tag{41}
$$

Thus, the above second condition in frequency domain is also satisfied. Let $c = 1 + 2i$ and $c' = 1 - 2i$, the final PGIS using x_1 and x_2 in (37) *and* (38) *is*

$$
x(n) = \begin{cases}
-4 + 12i & n = 0 \\
1 + 2i & n = 1,3,4,6,7,9,12,13 \\
-2 + 8i & n = 2,8,11,14 \\
8 - 12i & n = 5 \\
11 - 18i & n = 10
\end{cases} \tag{42}
$$

$$
\textit{where } x_2(n) = \begin{cases}
-5 & n = 0 \\
0 & n = 1,3,4,6,7,9,12,13 \\
-3 & n = 2,8,11,14 \\
7 & n = 5 \\
10 & n = 10
\end{cases} \tag{43}
$$

The idea behind this construction includes

- Ramanujan's Sum is always integer, so will be x_1 and x_2.
- The DFT of Ramanujan's Sum comes back to gcd-delta function, which guarantee the amplitude of frequency domain will have only 0 or N.
- The shifted $\hat{s}_{N,p}$ in time domain does not change the amplitude in frequency domain.
- In order to satisfy the first condition in time domain and make $x_2(k) = 0$, the shifted $\hat{s}_{N,p}$ must be used since it can provide a "2", which can be canceled as (40) . If $N \neq 3p$, there is no "2" so the same trick cannot be used easily.

V. CONCLUSION

In this paper we prove perfect Gaussian integer sequence (PGIS) with a pre-given constant can be constructed on arbitrary length N. By reviewing the concept of geometric series, the PGIS will contain a "1" when $1 + i$ is chosen as ratio, so reducible PGIS can be obtained . We also discussed the irreducible case and found another easy way to obtain PGIS for even length. Moreover, the same concept can be generalized to odd length $N = 3p$ by using Ramanujan's Sum.

References

[1] N. Y. Yu and G. Gong, "New binary sequences with optimal autocorrelation magnitude," *Information Theory, IEEE Transactions on*, vol. 54, no. 10, pp. 4771–4779, Oct 2008.

[2] W.-W. Hu, S.-H. Wang, and C.-P. Li, "Gaussian integer sequences with ideal periodic autocorrelation functions," *Signal Processing, IEEE Transactions on*, vol. 60, no. 11, pp. 6074–6079, Nov 2012.

[3] Y. Yang, X. Tang, and Z. Zhou, "Perfect gaussian integer sequences of odd prime length," *Signal Processing Letters, IEEE*, vol. 19, no. 10, pp. 615–618, Oct 2012.

[4] M. Xiuwen, W. Qiaoyan, J. Zhang, and Z. Huijuan, "New perfect gaussian integer sequences of period pq," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 96, no. 11, pp. 2290–2293, 2013.

[5] S.-C. Pei and K.-W. Chang, "On integer-valued zero autocorrelation sequences," in *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2013 Asia-Pacific*, Oct 2013, pp. 1–4.

[6] X. Peng and C. Xu, "New constructions of perfect gaussian integer sequences of even length," *Communications Letters, IEEE*, vol. 18, no. 9, pp. 1547–1550, Sept 2014.

[7] H.-H. Chang, C.-P. Li, C.-D. Lee, S.-H. Wang, and T.-C. Wu, "Perfect gaussian integer sequences of arbitrary composite length," *Information Theory, IEEE Transactions on*, vol. 61, no. 7, pp. 4107–4115, July 2015.

[8] C.-D. Lee, Y.-P. Huang, Y. Chang, and H.-H. Chang, "Perfect gaussian integer sequences of odd period $2^m - 1$," *Signal Processing Letters, IEEE*, vol. 22, no. 7, pp. 881–885, July 2015.

[9] S.-C. Pei and K.-W. Chang, "Perfect gaussian integer sequences of arbitrary length," *Signal Processing Letters, IEEE*, vol. 22, no. 8, pp. 1040–1044, Aug 2015.

[10] H.-H. Chang, S.-C. Lin, and C.-D. Lee, "A CDMA scheme based on perfect gaussian integer sequences," *AEU - International Journal of Electronics and Communications*, vol. 75, pp. 70 – 81, 2017.

[11] S. H. Wang, C. P. Li, H. H. Chang, and C. D. Lee, "A systematic method for constructing sparse gaussian integer sequences with ideal periodic autocorrelation functions," *IEEE Transactions on Communications*, vol. 64, no. 1, pp. 365–376, Jan 2016.

[12] K. J. Chang and H. H. Chang, "Perfect gaussian integer sequences of period p^k with degrees equal to or less than $k + 1$," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3723–3733, Sept 2017.

[13] S.-C. Pei and K.-W. Chang, "Arbitrary Length Perfect Integer Sequences Using Geometric Series," in *EUSIPCO*, 2018.

[14] ——, "Arbitrary length perfect integer sequences using all-pass polynomial," *IEEE Signal Processing Letters*, vol. 26, no. 8, pp. 1112–1116, Aug 2019.

[15] S.W.Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*. Cambridge, U.K Cambridge Univ. Press, 205.

[16] S. Yurish, *Advances in Networks, Security and Communications: Reviews, Vol. 2*. Lulu.com, 2020. [Online]. Available: https://books.google.com.tw/books?id=svLCDwAAQBAJ

[17] F. Zeng, X. He, G. Xuan, Z. Zhang, Y. Peng, and L. Yan, "Perfect gaussian integer sequences embedding pre-given gaussian integers," *IEEE Signal Processing Letters*, vol. 26, no. 8, pp. 1122–1126, Aug 2019.

[18] J. Benedetto, I. Konstantinidis, and M. Rangaswamy, "Phase-coded waveforms and their design," *Signal Processing Magazine, IEEE*, vol. 26, no. 1, pp. 22–31, Jan 2009.

[19] S. Ramanujan, "On certain trigonometrical sums and their applications in the theory of numbers," *Trans. Cambridge Philos. Soc*, vol. 22, no. 13, pp. 259–276, 1918.

[20] M. Hall, "A survey of difference sets," *Proceedings of the American Mathematical Society*, vol. 7, no. 6, pp. 975–986, 1956.

[21] J. D. Olsen, R. Scholtz, L. R. Welch *et al.*, "Bent-function sequences," *Information Theory, IEEE Transactions on*, vol. 28, no. 6, pp. 858–864, 1982.

[22] D. Jungnickel, "Difference sets," *Contemporary Design Theory: A Collection of Surveys*, pp. 241–324, 1992.

[23] M. Rupf and J. L. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *Information Theory, IEEE Transactions on*, vol. 40, no. 4, pp. 1261–1266, 1994.

[24] C.-S. Weng and J. Wu, "Perfect difference codes for synchronous fiber-optic CDMA communication systems," *Lightwave Technology, Journal of*, vol. 19, no. 2, pp. 186–194, 2001.

[25] P. Xia, S. Zhou, and G. B. Giannakis, "Achieving the welch bound with difference sets," *Information Theory, IEEE Transactions on*, vol. 51, no. 5, pp. 1900–1907, 2005.