Almost perfect sequences with $\theta = 2$

By

KA HIN LEUNG, SAN LING, SIU LUN MA and KIAN BOON TAY

Abstract. Almost perfect sequences with $\theta = 2$ are studied in this paper. Recently Arasu, Ma and Voss [1] studied such sequences and they could only obtain sequences having periods 8, 12 and 28. In this paper, we prove that no other almost perfect sequences exist for the case $\theta = 2$.

1. Introduction. Let $S = (s_i)$ be a periodic ± 1 sequence of period n , i.e. $s_i = s_{i+n}$ and $s_i = 1$ or -1 for $i = 0, 1, 2, \dots$. The *autocorrelation coefficients* are defined by

$$C_\tau(S) = \sum_{i=0}^{n-1} s_i s_{i+\tau}$$

for $\tau = 0, 1, 2, \dots$. If $\tau \not\equiv 0 \pmod{n}$, then $C_\tau(S)$ is called an *out-of-phase* autocorrelation coefficient. Sequences which have small out-of-phase autocorrelation coefficients are known to have important engineering applications, see [4] and [8]. Thus it is natural to ask if there exist sequences of zero out-of-phase autocorrelation coefficients – such a sequence is called a *perfect sequence*. Up to now, the only known perfect sequence is of period 4: $+ - - + - - + - - \dots$. For recent progress on perfect sequences, see [10].

Conjecture 1. *No perfect sequence exists with period greater than 4.*

Since a perfect sequence is essentially the same as a cyclic Hadamard-Paley difference set and a circulant Hadamard matrix (see [2]), Conjecture 1 is also well-known among people working on difference sets and Hadamard matrices. The conjecture is tantalizing and has led to many false proofs (see [5] and [7]). For the current status of the conjecture, refer to [6].

Getting a perfect sequence of longer period is a very difficult, if not impossible task. Wolfman [11] has introduced the notion of almost perfect sequences: a periodic ± 1 sequence of period n is said to be *almost perfect* if $C_\tau = 0$ for $1 \leq \tau \leq n - 1$ with exactly one exception. The good news is that there exists an infinite family of almost perfect sequences. However, Bradley and Pott [3] have shown that an almost perfect sequence is equivalent to an $(n/2, 2, (n - 2\theta)/2, \theta(\theta - 1), (n - 4\theta)/4)$ -divisible difference set (see Section 2), where $(n - 2\theta)/2$ is the number of $+$ entries in a generating cycle (without loss of generality, we can also assume the number of $+$ is less than the number of $-$). The new family constructed belongs to the case when $\theta = 1$ and is a well-known series of divisible difference sets.

Recently, Arasu, Ma and Voss [1] studied the case when $\theta = 2$ and could only obtain sequences of periods 8, 12 and 28. This paper follows the work of Arasu, Ma and Voss. We prove that no other almost perfect sequences exist for the case $\theta = 2$.

2. Divisible difference sets. Let G be a finite group of order mm' and N a normal subgroup of G of order m' . A subset D of G is said to be an $(m, m', k, \lambda_1, \lambda_2)$ *divisible difference set* if $|D| = k$ and the list of “differences” $(g_1 g_2^{-1} \mid g_1, g_2 \in D)$ contains each element in $N \setminus \{1\}$ exactly λ_1 times and each element in $G \setminus N$ exactly λ_2 times. For details on divisible difference sets, see Pott [9]. Using the notation of group rings, a subset D of G is an $(m, m', k, \lambda_1, \lambda_2)$ divisible difference set if and only if

$$DD^{(-1)} = (k - \lambda_1) + (\lambda_1 - \lambda_2)N + \lambda_2 G$$

where we identify a subset A of G with the element $\sum_{h \in A} h$ of $\mathbb{Z}[G]$ and write $A^{(t)} = \{h^t \mid h \in A\}$ for any integer t . By applying characters of G to the group ring equation, we have the following well-known result.

Theorem 2. *Let G be a cyclic group of order mm' and let N be the subgroup of G of order m' . A subset D of G is an $(m, m', k, \lambda_1, \lambda_2)$ divisible difference set if and only if for every character χ of G ,*

$$\chi(D)\overline{\chi(D)} = \begin{cases} k - \lambda_1 & \text{if } \chi \text{ is nonprincipal on } N \\ k^2 - mm'\lambda_2 & \text{if } \chi \text{ is principal on } N \text{ but nonprincipal on } G \\ k^2 & \text{if } \chi \text{ is principal on } G. \end{cases}$$

Let us return to almost perfect sequences. The next theorem has been mentioned in Section 1.

Theorem 3. (Bradley and Pott [3]). *Let $G = \langle \gamma \rangle$ be a cyclic group of order n . A $\pm$ periodic sequence $S = (s_i)$ of period n is almost perfect if and only if $D = \{\gamma^i \mid 0 \leq i < n \text{ and } s_i = +1\}$ is an*

$$\left(\frac{n}{2}, 2, \frac{n-2\theta}{2}, \theta(\theta-1), \frac{n-4\theta}{4} \right)$$

divisible difference set of G relative to $N = \{1, \gamma^{n/2}\}$, where $(n-2\theta)/2$ is the number of + entries in a generating cycle. (Note that n must be divisible by 4.)

The case $\theta = 1$ corresponds to the so-called affine difference sets, see [3] and [9], and they exist whenever $(n-2)/2$ is an odd prime power. The case $\theta = 2$ turns out to have only a few examples, namely, $n = 8, 12$ and 28 . No other example exists for $n < 348$ (see [1]).

3. The main result. We prove that an almost perfect sequence with $\theta = 2$ exists precisely when the period of the sequence is 8, 12 or 28. By Theorem 3, we only need to show that no $(n/2, 2, (n-4)/2, 2, (n-8)/4)$ divisible difference set exists in a cyclic group if $n \neq 8, 12, 28$. Let G be a cyclic group of order n , N a subgroup of G of order 2, and D an $(n/2, 2, (n-4)/2, 2, (n-8)/4)$ divisible difference set in G relative to N . By Theorem 2, for

every nonprincipal character χ of G ,

$$\chi(D)\overline{\chi(D)} = \begin{cases} (n-8)/2 & \text{if } \chi \text{ is nonprincipal on } N \\ 4 & \text{if } \chi \text{ is principal on } N. \end{cases}$$

The following lemma summarizes the results in [1].

Lemma 4. *Suppose $n > 8$ and $n \not\equiv 28$. Then $n = 4w$ where w is odd. Furthermore, if K is a subgroup of G of order w , α is an element of G of order 4, and $M = K \cup \alpha K$, then $D = \{1, \alpha^2\} \cup X \cup \alpha^2[M \setminus (X \cup A)]$ where $A = \{1, \alpha, g, \alpha g\}$, for some $g \in K$, and $X \subset M \setminus A$.*

Theorem 5. *Let n be as in Theorem 3. If $n > 8$ and $n \not\equiv 28$, then $n = 12$.*

Proof. By Lemma 4, we can write D as

$$D = \langle \alpha^2 \rangle + X + \alpha^2(M - X - A),$$

where $M = K \cup \alpha K$ and $X = X_1 \cup \alpha X_2$ with $X_1, X_2 \subseteq K - \{1, g\}$. The difference set D can then be rewritten as

$$(1) \quad D = \langle \alpha^2 \rangle + (X_1 + \alpha X_2) + \alpha^2((K - X_1 - \{1, g\}) + \alpha(K - X_2 - \{1, g\})).$$

Let χ be a character of G such that χ is not principal on K and $\chi(\alpha) \in \{\pm i\}$. Applying χ to (1), we obtain

$$\chi(D) = \chi(2X_1 + 1 + g) \pm i\chi(2X_2 + 1 + g).$$

Set $\lambda = \chi(2X_1 + 1 + g)$ and $\mu = \chi(2X_2 + 1 + g)$, so $\lambda, \mu \in \mathbb{Q}(\zeta_w)$. Since $\chi(D)\overline{\chi(D)} = (n-8)/2$, it follows that

$$(2) \quad \frac{n-8}{2} = (\lambda \pm i\mu)(\bar{\lambda} \mp i\bar{\mu}) = (\lambda\bar{\lambda} + \mu\bar{\mu}) \pm (\mu\bar{\lambda} - \lambda\bar{\mu})i.$$

Since $\mathbb{Q}(\zeta_w)$ and $\mathbb{Q}(i)$ are linearly disjoint extensions of $\mathbb{Q}$, (2) implies that $\mu\bar{\lambda} - \lambda\bar{\mu} = 0$ and so $\lambda\bar{\lambda} + \mu\bar{\mu} = (n-8)/2$. These in turn can be rewritten in the following form:

$$(3) \quad \chi\left((2X_1 + 1 + g)(2X_1 + 1 + g)^{(-1)} + (2X_2 + 1 + g)(2X_2 + 1 + g)^{(-1)}\right) = \frac{n-8}{2}$$

and

$$(4) \quad \chi\left((2X_1 + 1 + g)(2X_2 + 1 + g)^{(-1)} - (2X_1 + 1 + g)^{(-1)}(2X_2 + 1 + g)\right) = 0.$$

As we allow χ to run through characters of G that are nonprincipal on K and such that $\chi(\alpha) = \pm i$, upon application of the Fourier Inversion Formula, we obtain from (3) and (4)

$$(5) \quad \begin{aligned} & 4X_1X_1^{(-1)} + 2X_1(1 + g^{-1}) + 2X_1^{(-1)}(1 + g) + 4X_2X_2^{(-1)} + 2X_2(1 + g^{-1}) \\ & + 2X_2^{(-1)}(1 + g) + 4 + 2(g + g^{-1}) = \beta K + \frac{n-8}{2} \end{aligned}$$

and

$$(6) \quad \begin{aligned} & 4X_1X_2^{(-1)} + 2X_1(1 + g^{-1}) + 2X_2^{(-1)}(1 + g) - 4X_1^{(-1)}X_2 - 2X_2(1 + g^{-1}) \\ & - 2X_1^{(-1)}(1 + g) = \beta' K, \end{aligned}$$

where β, β' are integers.

It follows from (5) and (6) that

$$(\beta + \beta')K = 4 \left(X_1 X_1^{(-1)} + X_2 X_2^{(-1)} + X_1 X_2^{(-1)} - X_1^{(-1)} X_2 + X_1(1 + g^{-1}) \right. \\ \left. + X_2^{(-1)}(1 + g) + 2 - \frac{n-4}{8} \right) + 2(1 + g + g^{-1}).$$

This implies that $K = \{1, g, g^{-1}\}$, i.e., $w = 3$ and hence $n = 12$.

References

- [1] K. T. ARASU, S. L. MA and N. J. VOSS, On a class of almost perfect sequences. *J. Algebra* **192**, 47–56 (1997).
- [2] L. D. BAUMERT, *Cyclic Difference Sets*. Berlin-Heidelberg-New York 1971.
- [3] S. P. BRADLEY and A. POTT, Existence and non-existence of almost perfect autocorrelation sequences. *IEEE Trans. Inform. Theory* **41**, 301–304 (1995).
- [4] S. W. GOLOMB, *Shift Register Sequences* (revised edition). Aegean Park, Laguna Hills (California), 1982.
- [5] D. JUNGnickEL, Difference sets. In: *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, eds., 241–324. New York 1992.
- [6] D. JUNGnickEL and B. SCHMIDT, Recent results on difference sets. Preprint.
- [7] C. LIN and W. D. WALLIS, On the circulant Hadamard matrix conjecture. In: *Coding Theory, Design Theory, Group Theory*, D. Jungnickel and S. A. Vanstone, eds., 213–217, 1993.
- [8] F. J. MACWILLIAMS and N. J. A. SLOANE, Pseudo-random sequences and arrays. *Proc. IEEE* **64**, 1715–1729 (1976).
- [9] A. POTT, *Finite Geometry and Character Theory*. Berlin-Heidelberg-New York 1995.
- [10] B. SCHMIDT, Circulant Hadamard matrices: overcoming non-self-conjugacy. Preprint.
- [11] J. WOLFMAN, Almost perfect autocorrelation sequences. *IEEE Trans. Inform. Theory* **38**, 1412–1418 (1992).

Anschrift der Autoren:

K. H. Leung, S. Ling, S. L. Ma, K. B. Tay
 Department of Mathematics
 National University of Singapore
 10 Kent Ridge Crescent
 Singapore 119260
 Singapore