Almost perfect autocorrelation sequences with small number of pauses for applications in magnetic resonance

Tekin, Eda; Gnilke, Oliver Wilhelm; Özbudak, Ferruh; Blümich, Bernhard; Greferath, Marcus

Published in:
Cryptography and Communications

DOI (link to publication from Publisher):
10.1007/s12095-023-00659-x

Publication date:
2024

Document Version
Early version, also known as pre-print

Almost Perfect Autocorrelation Sequences With Small Number of Pauses for Applications in Magnetic Resonance

Eda Tekin[1], Oliver Wilhelm Gnilke[2], Ferruh Özbudak[3*], Bernhard Blümich[4] and Marcus Greferath[5]

[1]Department of Business Administration, Karabük University, Karabük, Turkey.
[2]Department of Mathematical Sciences, Aalborg University, Aalborg, Denmark.
[3*]Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey.
[4]Institut für Technische und Makromolekulare Chemie, RWTH Aachen University, Aachen, Germany.
[5]School of Mathematics and Statistics, University College Dublin, Dublin, Ireland.

*Corresponding author(s). E-mail(s): ozbudak@metu.edu.tr;
Contributing authors: tedatekin@gmail.com; owg@math.aau.dk;
bluemich@itmc.rwth-aachen.de; marcus.greferath@ucd.ie;

Abstract

It is well known that it is a challenge to find complex-valued sequences with perfect autocorrelation over small alphabets. In this work we present a construction that provides sequences with perfect cyclic autocorrelation over different alphabets using the value zero only once or twice in their period. The constructions provide a big variety of periods also at moderate lengths and the corresponding sequences may be considered to be of 'almost' constant amplitude. These sequences have applications in NMR spectroscopy with low excitation power.

Keywords: Sequences, Autocorrelation, NMR spectroscopy, Low excitation power

1 Introduction

Sequences with perfect (cyclic) auto-correlation behavior have been a subject of interest for a long time [1–4]. They enjoy applications in radar, communication, analysis, imaging and magnetic resonance [1, 5–8]. These sequences are all constant amplitude, i.e., each symbol in the alphabet has norm 1. This often makes their technical realization more involved and expensive.

There are applications of sequences with constant amplitude to nuclear magnetic resonance spectroscopy (NMR) [5, 6, 9–12], magnetic resonance imaging [11, 12], electron paramagnetic resonance [7, 8], and nuclear quadrupole resonance [13, 14]. Sequences that have been explored so far are maximum length binary sequences (MLBS) [9–13, 15, 16], which are also known under the term m-sequences, and perfect Frank sequences [5–8]. While the alphabet of an MLBS has only two values, its auto-correlation function suffers from a constant offset. The lengthy alphabet of Frank sequences, on the other hand, is difficult to realize technically. On the positive side, evidence has shown that excitation with constant amplitude sequences requires orders of magnitude less peak excitation power than conventional single-pulse excitation [6] and bears promise for larger excitation bandwidths [6, 11–14].

In this work we propose to loosen the requirement of constant amplitude by allowing for pauses in the sequence, i.e., we add 0 to the alphabet. This enables us to construct sequences over binary and quaternary alphabets with the added pause. We will strive for as few as possible pauses in our sequences to maximize the energy transfer, i. e., to minimize the peak excitation power.

It is well known that it has been a challenge to obtain new sequences with perfect autocorrelation over the alphabets $A = \{\pm 1, \pm i\}$ and $B = \{\pm 1\}$. For application purposes we construct some sequences with some twists in the purpose. Namely our aim in this paper is to construct new sequences with perfect or almost perfect autocorrelation over the alphabets $A \cup \{0\}$ and $B \cup \{0\}$ and having flexible (and moderate) periods with the property that such a sequence should take the value 0 only a few times over its period.

Through the paper, q is an odd prime power, $\mathbb{F}_q$ is the finite field with q elements, $n \geq 2$ is an integer, $\mathbb{F}_{q^n}$ is the degree n extension of $\mathbb{F}_q$ and $M = {}^{(q^n-1)}/_{(q-1)}$.

It has been a challenge to obtain new sequences with perfect autocorrelation over the alphabets A and B. Ryser's conjecture [17] states that there are no circulant Hadamard matrices of order $n > 4$. No perfect autocorrelation sequences of length $n > 4$ and $n > 16$ are known over the alphabets A and B, respectively [18]. Furthermore, binary almost perfect autocorrelation sequences of order $n \leq 452$ do exist if and only if $n/2 - 1$ is a prime power[19]. Thus, these sequences exist only in very specific lengths.

2 Organisation of the Paper

The paper is organised as follows. In Definition 2, we construct a sequence s_1 over the alphabet $A \cup \{0\}$. In Theorem 1 we show that when $q \equiv 1 \mod 4$

and $n \equiv 2 \mod 4$, s_1 has perfect autocorrelation over its period M; and when $q \equiv 3 \mod 4$ and n is even, s_1 has almost perfect autocorrelation over its period $2M$. Furthermore if $q \equiv 1 \mod 4$ and $n = 2$, then s_1 takes the value 0 only 1 time over its period $q + 1$. Note that this holds for any q with $q \equiv 1 \mod 4$. Similarly if $q \equiv 3 \mod 4$ and $n = 2$, then s_1 takes the value 0 only 2 times over its period $2(q + 1)$. Again this holds for any q with $q \equiv 3 \mod 4$.

In Definition 3, we construct a sequence s_2 over the alphabet $B \cup \{0\}$. In Theorem 2 we show that when q is an odd prime power and $n \geq 2$ is an even integer, s_2 has almost perfect autocorrelation over its period $2M$. Also if $n = 2$, s_2 takes the value 0 only 2 times over its period $2(q + 1)$. Note that as in the case of the sequences s_1 above, we obtain sequences s_2 for infinitely many different values of q having different periods and taking the value 0 only 2 times over their periods.

Moreover the possible periods of the sequences s_1 and s_2 are very flexible and quite dense including moderate sizes. We refer to Section 2 for some concrete examples.

The results obtained in Theorem 1 and Theorem 2 have very good properties for application purposes. Our methods allow us to construct further sequences as in Theorem 3. However the properties of the sequences in Theorem 3 are not as good as the ones in Theorem 1 and Theorem 2 for application puposes. In Remark 2, we compare the results of Theorem 1 and Theorem 2 with some other parameters given in Theorem 3.

3 Related Work

In [20], Popovic constructed a sequence s over the alphabet $A \cup \{0\}$ with perfect autocorrelation when $q \equiv 1 \mod 4$ and $n \equiv 1 \mod 4$. In Remark 3 and Remark 4, we also compare our sequences with this sequence of Popovic. We show that this sequence of Popovic takes the value 0 too many times over its period. Moreover the possible values of the periods in the sequence of Popovic are very sparse with huge jumps. Hence our sequences s_1 and s_2 are more suitable for the applications puposes of this paper. In particular when $n = 2$, the number of 0 values in our sequences is independent from q, which is either 1 or 2. On the other hand, Popovic obtains perfect autocorrelation sequences with alphabet $A \cup \{0\}$ only when $q \equiv 1 \mod 4$ and $n \equiv 1 \mod 4$. The number of 0 values in the periods in a sequences of Popovic is $(q^{n-1} - 1)/(q - 1)$, which always depends on q (and n). Moreover this number grows exponentially as n increases. The smallest n in the sequences of Popovic is 5. Even for $n = 5$, the number of 0 values in Popovic's sequences is $q^3 + q^2 + q + 1$. Then the smallest value of q in Popovic's sequences is $q = 5$, which gives a sequences having $q^3 + q^2 + q + 1 = 156$ number of 0 values over its period of length 781. Moreover the possible period lengths are very sparse with huge gaps in Popovic's sequences. The next shortest length with $q = 5$ is when $n = 9$. It gives a sequences of period 488281 and 97656 symbols of its values in a period is 0. For further information, please see Remark 4.

In [21], Lee constructed a sequence s over the alphabet $A \cup \{0\}$ with perfect autocorrelation. When $n = 2$, the necessary restrictions of Lee requires that $p \equiv 1 \mod 4$ where p is a prime number. In Remark 5, we also compare our sequences with this sequence of Lee and give the number of 0 values of our sequences (either 0 or 1). Even though our sequences intersects with Lee for some parameters (e.g. $p = 29$ and $n = 2$), we obtain different sequences than in [21]. For application purposes it is important that our sequences have only a few number of zero values.

4 Preliminaries

Definition 1 For a complex valued sequence $u = (u(0), u(1), ..., u(N-1))$, where N is the period of the sequence, the periodic autocorrelation function is defined as

$$C_u(\tau) = \sum_{t=0}^{N-1} u(t+\tau)\overline{u(t)}.$$

Here, τ represents the phase shift of the sequence. If $C_u(\tau) = 0$ for all $\tau \neq 0 \mod N$ then the sequence has perfect autocorrelation. When $\tau = 0$, then for all sequences $u = u(0), u(1), ..., u(N-1)$, we have maximum auto-correlation.

Let q be a prime power, $n \geq 2$ and $\mathbb{F}_q$ be the finite field with q elements. Tr denotes the trace function from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ which is defined as

$$\mathrm{Tr}(x) = x + x^q + x^{q^2} + ... + x^{q^{(n-1)}}$$

and Norm denotes the norm function from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ which is defined as

$$\mathrm{Norm}(x) = x^{\frac{q^n-1}{q-1}}.$$

5 Our Sequences s_1 and s_2

In this chapter, we introduce a complex sequence s_1 in Definition 2 and give its periodic autocorrelation in Theorem 1. Next, we introduce a binary sequence s_2 in Definition 3 and give its periodic autocorrelation in Theorem 2.

Definition 2 Let q be an odd prime power, $n \geq 2$, $< w >= \mathbb{F}_{q^n}^*$, $c \in \mathbb{F}_{q^n}^*$ and $i = \sqrt{-1}$. Let Tr be the trace map from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$. Let S be the set of non-zero squares of $\mathbb{F}_q$, N be set of the non-squares of $\mathbb{F}_q$. For $t \geq 0$, let $s_1(t)$ be the sequence defined as

$$s_1(t) = \begin{cases} i^t, & \text{if } \mathrm{Tr}(cw^t) \in S^*, \\ -(i)^t, & \text{if } \mathrm{Tr}(cw^t) \in N, \\ 0, & \text{if } \mathrm{Tr}(cw^t) = 0. \end{cases} \quad (1)$$

Theorem 1 *Let q be an odd prime power, $n \geq 2$, $M = \frac{q^n-1}{q-1}$ and s_1 be the sequence given in Definition 2.*

- ***Case*** $q \equiv 1 \mod 4$ ***and*** $n \equiv 2 \mod 4$***:*** *In this case* s_1 *is periodic with period* M*. Using this period, for* $0 \leq \tau \leq M-1$*, the periodic autocorrelation of* s_1 *is*

$$C_{s_1}(\tau) = \begin{cases} q^{n-1}, & \text{if } \tau = 0, \\ 0, & \text{otherwise.} \end{cases}$$

  Note that s_1 *has alphabet* $\{0, \pm 1, \pm i\}$*. Furthermore if* $n = 2$*, then for any odd prime power* q *with* $q \equiv 1 \mod 4$*,* s_1 *takes the value* 0 *exactly* 1 *time over its period* M*.*
- ***Case*** $q \equiv 3 \mod 4$ ***and*** $n \equiv 0 \mod 2$***:*** *In this case* s_1 *is periodic with period* $2M$*. Using this period, for* $0 \leq \tau \leq 2M-1$*, the periodic autocorrelation of* s_1 *is*

$$C_{s_1}(\tau) = \begin{cases} 2q^{n-1}, & \text{if } \tau = 0, \\ -2q^{n-1}, & \text{if } \tau = M, \\ 0, & \text{otherwise.} \end{cases}$$

  Note that s_1 *has alphabet* $\{0, \pm 1, \pm i\}$*. Furthermore if* $n = 2$*, then for any odd prime power* q *with* $q \equiv 3 \mod 4$*,* s_1 *takes the value* 0 *exactly* 2 *times over its period* $2M$*.*

Definition 3 Let q be an odd prime power, $n \geq 2$, $< w >= \mathbb{F}_{q^n}^*$ and $c \in \mathbb{F}_{q^n}^*$. Let Tr be the trace map from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$. Let S be the set of non-zero squares of $\mathbb{F}_q$, N be the set of non-squares of $\mathbb{F}_q$. For $t \geq 0$, let $s_2(t)$ be the sequence defined as

$$s_2(t) = \begin{cases} (-1)^t, & \text{if } \mathrm{Tr}(cw^t) \in S^*, \\ -(-1)^t, & \text{if } \mathrm{Tr}(cw^t) \in N, \\ 0, & \text{if } \mathrm{Tr}(cw^t) = 0. \end{cases} \tag{2}$$

Theorem 2 *Let* q *be an odd prime power,* $n \geq 2$*,* $M = \frac{q^n-1}{q-1}$ *and* s_2 *be the sequence given in Definition 3.*

- ***Case*** $q \equiv 1 \mod 2$ ***and*** $n \equiv 0 \mod 2$***:*** *In this case* s_2 *is periodic with period* $2M$*. Using this period, for* $0 \leq \tau \leq 2M-1$*, the periodic autocorrelation of* s_2 *is*

$$C_{s_2}(\tau) = \begin{cases} 2q^{n-1}, & \text{if } \tau = 0, \\ -2q^{n-1}, & \text{if } \tau = M, \\ 0, & \text{otherwise.} \end{cases}$$

  Note that s_2 *has alphabet* $\{0, \pm 1\}$*. Furthermore if* $n = 2$*, then for any odd prime power* q*,* s_2 *takes the value* 0 *exactly* 2 *times over its period* $2M$*.*

Remark 1 Using our methods, it is possible to obtain the periodic autocorrelation of s_1 and s_2, and the number of times s_1 and s_2 take the value 0 over its period for

other q and n values. However, the cases given in Theorem 1 and Theorem 2 seem to be the most interesting for our applications.

For the sake of completeness, we give the periodic autocorrelations of s_1 and s_2 for other cases that we also obtained in the next theorem. We skip the proof of Theorem 3 since it is very similar to Theorem 1 and Theorem 2.

Theorem 3 *Let q be an odd prime power, $n \geq 2$ and $M = \frac{q^n-1}{q-1}$. Let s_1 and s_2 be the sequences given in Definition 2 and Definition 3.*

- ***Case*** $q \equiv 1 \mod 2$ ***and*** $n \equiv 1 \mod 2$***:*** *In this case s_2 is periodic with period M. Using this period, for $0 \leq \tau \leq M-1$, the periodic autocorrelation of s_2 is*

$$C_{s_2}(\tau) = \begin{cases} q^{n-1}, & \text{if } \tau = 0, \\ 0, & \text{otherwise.} \end{cases}$$

- ***Case*** $q \equiv 1 \mod 4$ ***and*** $n \equiv 0 \mod 4$***:*** *In this case s_1 is periodic with period $2M$. Using this period, for $0 \leq \tau \leq 2M-1$, the periodic autocorrelation of s_1 is*

$$C_{s_1}(\tau) = \begin{cases} 2q^{n-1}, & \text{if } \tau = 0, \\ -2q^{n-1}, & \text{if } \tau = M, \\ 0, & \text{otherwise.} \end{cases}$$

- ***Case*** $q \equiv 1 \mod 4$ ***and*** $n \equiv 1 \mod 4$***:*** *In this case s_1 is periodic with period $4M$. Using this period, for $0 \leq \tau \leq 4M-1$, the periodic autocorrelation of s_1 is*

$$C_{s_1}(\tau) = \begin{cases} 4q^{n-1}, & \text{if } \tau = 0, \\ -4iq^{n-1}, & \text{if } \tau = M, \\ -4q^{n-1}, & \text{if } \tau = 2M, \\ 4iq^{n-1}, & \text{if } \tau = 3M, \\ 0, & \text{otherwise.} \end{cases}$$

- ***Case*** $q \equiv 1 \mod 4$ ***and*** $n \equiv 3 \mod 4$***:*** *In this case s_1 is periodic with period $4M$. Using this period, for $0 \leq \tau \leq 4M-1$, the periodic autocorrelation of s_1 is*

$$C_{s_1}(\tau) = \begin{cases} 4q^{n-1}, & \text{if } \tau = 0, \\ 4iq^{n-1}, & \text{if } \tau = M, \\ -4q^{n-1}, & \text{if } \tau = 2M, \\ -4iq^{n-1}, & \text{if } \tau = 3M, \\ 0, & \text{otherwise.} \end{cases}$$

Remark 2 Here, we list the smallest number of 0 values that a sequence takes over its period for the cases given in Theorem 3.

- Let $q \equiv 1 \mod 2$ and $n \equiv 1 \mod 2$. If $n = 3$, then s_2 takes the value 0 exactly $(q+1)$ times over its period M.
- Let $q \equiv 1 \mod 4$ and $n \equiv 0 \mod 4$. If $n = 4$, then s_1 takes the value 0 exactly $2(q^2+q+1)$ times over its period $2M$.
- Let $q \equiv 1 \mod 4$ and $n \equiv 1 \mod 4$. If $n = 5$, then s_1 takes the value 0 exactly $4(q^3+q^2+q+1)$ times over its period $4M$.
- Let $q \equiv 1 \mod 4$ and $n \equiv 3 \mod 4$. If $n = 3$, then s_1 takes the value 0 exactly $4(q+1)$ times over its period $4M$.

Note that using Theorem 1 and Theorem 2, new sequences with only 1 or 2 zero values can be obtained over a given period. However, under given conditions on q and n given in Theorem 3, the number of 0 values of s_1 and s_2 depends on q. As n increases, the smallest number of 0 values of s_1 and s_2 also increase exponentially.

In [20], Popovic introduced some sequences with perfect autocorrelation. Note that when $q \equiv 1 \mod 4$ and $n \equiv 1 \mod 4$, the alphabet of Popovic's sequence is $\{\pm 1, \pm i\} \cup \{0\}$. In the following remarks, we compare the smallest possible number of 0 values in a sequence in our construction and Popovic's construction.

Remark 3 We first give the smallest number of zero values in a sequence given in Definition 2 and Definition 3. As a result of Theorem 1, we obtain the following. If $q \equiv 1 \mod 4$ and $n = 2$, then s_1 has perfect autocorrelation and takes the value 0 only 1 time over its period $q+1$. If $q \equiv 3 \mod 4$ and $n = 2$, then s_1 has almost perfect autocorrelation and takes the value 0 only 2 times over its period $2(q+1)$. This indicates that s_1 takes the values $\{\pm 1, \pm i\}$ remaining q or $2q$ times over their periods $q+1$ and $2(q+1)$ respectively.

Similarly, as a result of Theorem 2, we obtain the following. If $q \equiv 1 \mod 2$ and $n = 2$, then s_2 has almost perfect autocorrelation and takes the value 0 exactly 2 times over its period $2(q+1)$. This indicates that s_2 takes the values $\{\pm 1\}$ remaining $2q$ times over its period $2(q+1)$.

Furthermore, since we can choose n as small as required, the lengths of sequences can be chosen very small. Hence, we can construct new sequences for various parameters with flexible lengths. For further information please see Section 6.

Remark 4 In Popovic's construction [20], a complex valued sequence s with perfect autocorrelation is obtained when $q \equiv 1 \mod 4$ and $n \equiv 1 \mod 4$. As a special case if $n = 5$, then a sequence takes the value 0 exactly

$$1 + q + q^2 + q^3$$

times over its period $M = 1 + q + q^2 + q^3 + q^4$. For example if $q = 5$ and $n = 5$, then s takes the value 0 exactly 156 times and the values $\{\pm 1, \pm i\}$ remaining 625 times over its period $M = 781$. if $q = 9$ and $n = 5$, then s takes the value 0 exactly 820 times and the values $\{\pm 1, \pm i\}$ remaining 6561 times over its period $M = 7381$. As a

result, the number of 0's in our construction is much smaller when compared to the sequences given in [20].

To obtain a complex valued sequence, since $q \equiv 1 \mod 4$ and $n \equiv 1 \mod 4$ must be satisfied, using Popovic's construction we can not obtain new sequences with short lengths. Two closest lengths are 781 and 7381 given above. As a result, if Popovic's construction is used, it can not be obtained various sequences between two lengths.

Remark 5 In [21], Lee constructed sequences over the alphabet $A \cup \{0\}$ with perfect autocorrelation when p is a prime number. In that construction, Lee introduced 2 methods using different intermediate mappings. When $n = 2$, Lee obtained sequences using his first method only for $p \equiv 1 \mod 4$ (ex. $p = 5, 13, 17, 29, \cdots$).

Our main aim is to construct sequences with good autocorrelation properties which has small number of 0 values in their periods. We use different mathematical techniques constructing our sequences. Thus, we obtain different sequences than the sequences constructed in [21]. In our construction q is either a prime or a prime power and we obtain sequences with small number of 0 values for both $q \equiv 1 \mod 4$ and $q \equiv 3 \mod 4$. When $n = 2$, we obtain sequences s_1 with corresponding lengths and number of 0 values (only 1 or 2) as given in the table below.

q	3	5	7	9	11	13	17	19	23	25	27	29
period of s_1	8	6	16	10	24	14	18	40	48	26	56	30
#0 values	2	1	2	1	2	1	1	2	2	1	2	1

As a result, Lee [21] constructed perfect sequences when p is a prime number. Our sequences intersects with the construction of [21] for some values of q and n (for example when $q = 29$ and $n = 2$). However, using different mathematical techniques we obtain different sequences than Lee's [21] for either when q is a prime number or a prime power. Furthemore, our sequences with good autocorrelation properties have a few 0 values (only 1 or 2) and this is important for application purposes.

6 Numerical Examples

In this Section, we give some numerical examples of sequences introduced in Theorem 1 and Theorem 2 for small q and n values using MAGMA program.

Example 1 Let $n = 2$ and $q \equiv 1 \mod 4$. Using Theorem 1, s_1 takes the value 0 only 1 time and takes $\{\pm 1, \pm i\}$ remaining q times over its period $M = q + 1$. In the following table, we give a list of sequences for some $q \equiv 1 \mod 4$.

q	s_1
5	$(0, 1, i, -1, i, 1)$
9	$(0, -1, i, -1, -i, 1, -i, -1, i, -1)$
13	$(0, -1, -i, 1, i, -1, i, -1, i, -1, i, 1, -i, -1)$
17	$(0, -1, -i, 1, -i, -1, -i, 1, i, 1, i, 1, -i, -1, -i, 1, -i, -1)$
25	$(0, -1, i, 1, i, -1, i, -1, -i, -1, i, 1, -i,$ $1, -i, 1, i, -1, -i, -1, i, -1, i, 1, i, -1)$
29	$(0, -1, -i, 1, -i, 1, i, 1, i, 1, -i, -1, i, 1, i,$ $-1, i, 1, i, -1, -i, 1, i, 1, i, 1, -i, 1, -i, -1)$
37	$(0, 1, i, 1, -i, 1, -i, -1, -i, -1, -i, 1, i, -1, -i, 1, -i, -1, i,$ $-1, i, -1, -i, 1, -i, -1, i, 1, -i, -1, -i, -1, -i, 1, -i, 1, i, 1)$
41	$(0, 1, -i, 1, -i, 1, i, 1, i, -1, -i, 1, -i, -1, i, -1, -i, -1, i, 1, -i,$ $1, -i, 1, i, -1, -i, -1, i, -1, -i, 1, -i, -1, i, 1, i, 1, -i, 1, -i, 1)$
125	$(0, -1, -i, -1, i, -1, -i, 1, -i, 1, -i, 1, i, -1, i, -1, -i, -1, -i, 1, i,$ $1, -i, 1, -i, -1, i, 1, i, 1, -i, 1, i, -1, i, 1, -i, -1, i, -1, -i, -1, -i,$ $-1, i, 1, -i, -1, i, 1, -i, -1, -i, -1, -i, 1, i, -1, i, -1, i, -1, i, -1,$ $i, -1, i, -1, i, -1, i, 1, -i, -1, -i, -1, -i, 1, i, -1, -i, 1, i, -1, -i,$ $-1, -i, -1, i, -1, -i, 1, i, -1, i, 1, -i, 1, i, 1, i, -1, -i, 1, -i, 1, i, 1,$ $-i, -1, -i, -1, i, -1, i, 1, -i, 1, -i, 1, -i, -1, i, -1, -i, -1)$

Example 2 Let $n = 2$ and $q \equiv 3 \mod 4$. Using Theorem 1, s_1 takes the value 0 only 2 times and takes $\{\pm 1, \pm i\}$ remaining $2q$ times over its period $M = 2(q + 1)$. In the following table, we give a list of sequences for some $q \equiv 3 \mod 4$.

q	s_1
3	$(0, -i, 1, -i, 0, i, -1, i)$
7	$(0, -i, 1, -i, -1, -i, 1, -i, 0, i, -1, i, 1, i, -1, i)$
19	$(0, i, -1, i, 1, -i, -1, -i, 1, -i, 1, -i, 1, -i, -1, -i, 1, i, -1, i,$ $0, -i, 1, -i, -1, i, 1, i, -1, i, -1, i, -1, i, 1, i, -1, -i, 1, -i)$
23	$(0, i, -1, i, -1, i, 1, -i, -1, i, -1, -i, -1, -i, -1, i, -1, -i, 1, i, -1, i, -1,$ $i, 0, -i, 1, -i, 1, -i, -1, i, 1, -i, 1, i, 1, i, 1, -i, 1, i, -1, -i, 1, -i, 1, -i)$
59	$(0, i, -1, i, -1, -i, -1, -i, -1, -i, -1, i, 1, -i, -1, -i, -1, i,$ $-1, -i, 1, i, -1, i, 1, i, -1, -i, -1, -i, 1, -i, -1, -i, -1, i, 1,$ $i, -1, i, 1, -i, -1, i, -1, -i, -1, -i, 1, i, -1, -i, -1, -i, -1,$ $-i, -1, i, -1, i, 0, -i, 1, -i, 1, i, 1, i, 1, i, 1, -i, -1, i, 1, i, 1, -i,$ $1, i, -1, -i, 1, -i, -1, -i, 1, i, 1, i, -1, i, 1, i, 1, -i, -1, -i, 1,$ $-i, -1, i, 1, -i, 1, i, 1, i, -1, -i, 1, i, 1, i, 1, i, 1, -i, 1, -i)$

Example 3 Let q be an odd prime power, $n = 2$ be an even integer. Using Theorem 2, s_2 takes the value 0 only 2 times and takes $\{\pm 1\}$ remaining $2q$ times over its period $M = 2(q + 1)$. In the following table, we give a list of sequences for some $q \equiv 1 \mod 2$.

q	s_2
3	$(0, -1, 1, 1, 0, 1, -1, -1)$
5	$(0, 1, -1, 1, 1, 1, 0, -1, 1, -1, -1, -1)$
7	$(0, 1, -1, -1, -1, 1, -1, -1, 0, -1, 1, 1, 1, -1, 1, 1)$
9	$(0, 1, 1, -1, 1, -1, -1, -1, -1, 1, 0, -1, -1, 1, -1, 1, 1, 1, 1, -1)$
19	$(0, 1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1,$ $-1, -1, 0, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, 1, 1)$

Over a period M, if $n = 3$ a sequence has $q + 1$ zeros, if $n = 4$ a sequence has $q^2 + q + 1$ zeros, if $n = 5$ a sequence has $q^3 + q^2 + q + 1$ zeros, if $n = 6$ a sequence has $q^4 + q^3 + q^2 + q + 1$ zeros and so on. As n increases the number of zeros in a sequence over a given period also increase exponentially. Thus, we skip numerical examples for $n \geq 3$.

7 Proof of Theorems

Lemma 4 *Let $A \subseteq \mathbb{C}$ be a nonempty subset. Let $N \geq 1$, $u = (u(t) \in A : t \geq 0)$ be a sequence such that N is a period of u. For $0 \leq \tau \leq N - 1$, let $C_u(\tau)$ be the $N-$periodic autocorrelation of u given by*

$$C_u(\tau) = \sum_{t=0}^{N-1} u(t+\tau)\overline{u(t)}.$$

Assume further that there exist integers M and $a \geq 2$ such that $N = aM$ where M is also a period of u. For $t \geq 0$, let $v(t) = u(t)$ and put $v = (v(t) \in A : t \geq 0)$ be the same sequence considered with period M. For $0 \leq \tau \leq M - 1$, let $C_v(\tau)$ be the $M-$periodic autocorrelation of v given by

$$C_v(\tau) = \sum_{t=0}^{M-1} v(t+\tau)\overline{v(t)}.$$

For $0 \leq \tau \leq N - 1$, we have

$$C_u(\tau) = aC_v(\tau).$$

In particular, for $0 \leq \tau \leq M - 1$ and $1 \leq j \leq a - 1$, we have

$$C_u(\tau) = C_u(jM + \tau).$$

For completeness, we present a proof of the following simple Lemma that gives the number of 0 values of a sequence s_1 or s_2 over a period.

Lemma 5 *The number of 0 values in a sequence s_1 or s_2 over a given period $M = {}^{(q^n-1)}/_{(q-1)}$ is*

$$T = \frac{q^{n-1} - 1}{q - 1}.$$

Proof The number of 0's in a sequence s_1 or s_2 for $0 \leq t < q^n - 1$ is

$$| \{0 \leq t < q^n - 1 : \mathrm{Tr}(cw^t) = 0\} | = q^{n-1} - 1.$$

When M is a period, $\mathrm{Tr}(cw^{t+M}) = w^M \mathrm{Tr}(cw^t)$ and

$$| \{0 \leq t < M : \mathrm{Tr}(cw^t) = 0\} | = | \{0 \leq t < M : \mathrm{Tr}(cw^{t+M}) = 0\} | .$$

As a result, over a period $M = {}^{(q^n-1)}/_{(q-1)}$, the number of 0's in a sequence is

$$T = \frac{q^{n-1} - 1}{q - 1}.$$

□

For completeness, we present a proof of the following simple Lemma.

Lemma 6 *Let* $M = \frac{q^n-1}{q-1}$, s_1 *and* s_2 *be the sequences given in Definition 2 and Definition 3. Then the following conditions are satisfied.*

- *If* $q \equiv 3 \mod 4$ *and* $n \equiv 0 \mod 2$, *then* $2M = 2(\frac{q^n-1}{q-1})$ *is a period of* s_1.
- *If* $q \equiv 1 \mod 4$ *and* $n \equiv 0 \mod 4$, *then* $2M = 2(\frac{q^n-1}{q-1})$ *is a period of* s_1.
- *If* $q \equiv 1 \mod 4$ *and* $n \equiv 2 \mod 4$, *then* $M = \frac{q^n-1}{q-1}$ *is a period of* s_1.
- *If* $q \equiv 1 \mod 4$ *and* $n \equiv 1 \mod 2$, *then* $4M = 4(\frac{q^n-1}{q-1})$ *is a period of* s_1.
- *If* $q \equiv 1 \mod 2$ *and* $n \equiv 0 \mod 2$, *then* $2M = 2(\frac{q^n-1}{q-1})$ *is a period of* s_2.
- *If* $q \equiv 1 \mod 2$ *and* $n \equiv 1 \mod 2$, *then* $M = \frac{q^n-1}{q-1}$ *is a period of* s_2.

Proof Let $q \equiv 3 \mod 4$. To show that the sequence s_1 is periodic with a period $2M$, we need to show that $s_1(t) = s_1(t + 2M)$ for all $t \geq 0$.

- First let $\mathrm{Tr}(cw^t) = 0$, then $s_1(t) = 0$. $s_1(t + 2M) = 0$ since
$$\mathrm{Tr}(cw^{t+2M}) = w^{2M}\mathrm{Tr}(cw^t) = 0.$$
- Now let $\mathrm{Tr}(cw^t) \in S^*$, then $s_1(t) = i^t$. Since $w^{2M} \in S^*$,
$$\mathrm{Tr}(cw^{t+2M}) = w^{2M}\mathrm{Tr}(cw^t) \in S^*$$
and $s_1(t + 2M) = (i)^{t+2M} = (i)^{2M}s_1(t)$. Then $s_1(t + 2M) = s_1(t)$ if and only if $n \equiv 0 \mod 2$ since $M = \frac{q^n-1}{q-1} = 1 + q + \cdots + q^{n-1} \equiv n \mod 2$.
- Finally let $\mathrm{Tr}(cw^t) \in N$, then $s_1(t) = -(i)^t$. Then
$$\mathrm{Tr}(cw^{t+2M}) = w^{2M}\mathrm{Tr}(cw^t) \in N$$
and $s_1(t + 2M) = -(i)^{t+2M} = (i)^{2M}s_1(t)$. Similarly $s_1(t + 2M) = s_1(t)$ if and only if $n \equiv 0 \mod 2$.

The proofs of the remaining cases are similar. □

For $t \geq 0$, let $s_1(t) \in \{0, \pm 1, \pm i\} \subseteq \mathbb{C}$ be the element defined as

$$s_1(t) = \begin{cases} i^t, & \text{if } \mathrm{Tr}(cw^t) \in S^*, \\ -(i)^t, & \text{if } \mathrm{Tr}(cw^t) \in N, \\ 0, & \text{if } \mathrm{Tr}(cw^t) = 0. \end{cases} \tag{3}$$

Let $s_1 = (s_1(t) : t \geq 0)$ be the sequence defined using Equation (3). It is clear that $q^n - 1$ is a period of s_1. Note that the $(q^n - 1)-$periodic autocorrelation

of s_1 is given by

$$C_{s_1}(\tau) = \sum_{t=0}^{q^n-2} s_1(t+\tau)\overline{s_1(t)}. \tag{4}$$

For $t \geq 0$, let $s_2(t) \in \{0, \pm 1\}$ be the element defined as

$$s_2(t) = \begin{cases} (-1)^t, & \text{if } \mathrm{Tr}(cw^t) \in S^*, \\ -(-1)^t, & \text{if } \mathrm{Tr}(cw^t) \in N, \\ 0, & \text{if } \mathrm{Tr}(cw^t) = 0. \end{cases} \tag{5}$$

Let $s_2 = (s_2(t) : t \geq 0)$ be the sequence defined using Equation (3). It is clear that $q^n - 1$ is a period of s_2. Note that the $(q^n - 1)-$periodic autocorrelation of s_2 is given by

$$C_{s_2}(\tau) = \sum_{t=0}^{q^n-2} s_2(t+\tau)\overline{s_2(t)}. \tag{6}$$

In Lemma 7, we assume that $0 \leq \tau < q^n - 1$ without loss of generality.

Lemma 7 *For $0 \leq \tau < q^n - 1$, we have*

$$C_{s_1}(\tau) = \begin{cases} (i)^\tau (q-1)q^{n-1}, & \text{if } \tau \equiv 0 \mod 2(\frac{q^n-1}{q-1}), \\ -(i)^\tau (q-1)q^{n-1}, & \text{if } \tau \equiv \frac{q^n-1}{q-1} \mod 2(\frac{q^n-1}{q-1}), \\ 0, & \text{otherwise,} \end{cases}$$

and

$$C_{s_2}(\tau) = \begin{cases} (-1)^\tau (q-1)q^{n-1}, & \text{if } \tau \equiv 0 \mod 2(\frac{q^n-1}{q-1}), \\ -(-1)^\tau (q-1)q^{n-1}, & \text{if } \tau \equiv \frac{q^n-1}{q-1} \mod 2(\frac{q^n-1}{q-1}), \\ 0, & \text{otherwise.} \end{cases}$$

Proof Let $S_1(\tau)$, $S_2(\tau)$, $S_3(\tau)$ and $S_4(\tau)$ be the subsets of $\mathbb{F}_{q^n}^*$ defined as

$$\begin{aligned} S_1(\tau) &= \{x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}(cw^\tau x) \in S^* \text{ and } \mathrm{Tr}(cx) \in S^*\}, \\ S_2(\tau) &= \{x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}(cw^\tau x) \in S^* \text{ and } \mathrm{Tr}(cx) \in N\}, \\ S_3(\tau) &= \{x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}(cw^\tau x) \in N \text{ and } \mathrm{Tr}(cx) \in S^*\}, \\ S_4(\tau) &= \{x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}(cw^\tau x) \in N \text{ and } \mathrm{Tr}(cx) \in N\}. \end{aligned}$$

Then it follows from equations (3) and (4) that

$$C_{s_1}(\tau) = \sum_{x \in S_1(\tau)} (i)^\tau - \sum_{x \in S_2(\tau)} (i)^\tau - \sum_{x \in S_3(\tau)} (i)^\tau + \sum_{x \in S_4(\tau)} (i)^\tau. \tag{7}$$

It follows from equations (5) and (6) that

$$C_{s_1}(\tau) = \sum_{x \in S_1(\tau)} (-1)^\tau - \sum_{x \in S_2(\tau)} (-1)^\tau - \sum_{x \in S_3(\tau)} (-1)^\tau + \sum_{x \in S_4(\tau)} (-1)^\tau. \tag{8}$$

The proof follows immediately using Equation (7) for s_1 and Equation (8) for s_2 provided we show that

$$\mid S_1(\tau) \mid = \mid S_4(\tau) \mid = \begin{cases} (\frac{q-1}{2})q^{n-1}, & \text{if } \tau \equiv 0 \mod 2(\frac{q^n-1}{q-1}), \\ 0, & \text{if } \tau \equiv \frac{q^n-1}{q-1} \mod 2(\frac{q^n-1}{q-1}), \\ (\frac{q-1}{2})^2 q^{n-2}, & \text{otherwise,} \end{cases}$$

and

$$\mid S_2(\tau) \mid = \mid S_3(\tau) \mid = \begin{cases} 0, & \text{if } \tau \equiv 0 \mod 2(\frac{q^n-1}{q-1}), \\ (\frac{q-1}{2})q^{n-1}, & \text{if } \tau \equiv \frac{q^n-1}{q-1} \mod 2(\frac{q^n-1}{q-1}), \\ (\frac{q-1}{2})^2 q^{n-2}, & \text{otherwise.} \end{cases}$$

In the rest of the proof, we determine these cardinalities. Let L, L_1 and L_2 be $\mathbb{F}_q-$linear maps defined as

$$\begin{aligned} L : \mathbb{F}_{q^n} &\to \mathbb{F}_q \times \mathbb{F}_q \\ x &\mapsto (\mathrm{Tr}(cw^\tau x), \mathrm{Tr}(cx)), \end{aligned} \tag{9}$$

$$\begin{aligned} L_1 : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}(cw^\tau x), \end{aligned} \tag{10}$$

$$\begin{aligned} L_2 : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ x &\mapsto \mathrm{Tr}(x). \end{aligned} \tag{11}$$

If $w^\tau \notin \mathbb{F}_q$, then $\ker(L_1) \neq \ker(L_2)$ and hence,

$$\dim_{\mathbb{F}_q}(\ker(L)) = n-2 \text{ and } L \text{ is surjective.}$$

If $w^\tau \in \mathbb{F}_q$, then $\ker(L_1) = \ker(L_2)$ and hence,

$$\dim(\ker(L)) = n-1 \text{ and } \mathrm{Im}(L) = \{(w^\tau y, y) : y \in \mathbb{F}_q\}.$$

Moreover $w^\tau \in \mathbb{F}_q$ if and only if $\tau \equiv 0 \mod \frac{q^n-1}{q-1}$. Furthermore, we have

- $\tau \not\equiv 0 \mod \frac{q^n-1}{q-1} \Rightarrow w^\tau \notin \mathbb{F}_q$,
- $\tau \equiv \frac{q^n-1}{q-1} \mod 2\left(\frac{q^n-1}{q-1}\right) \Rightarrow w^\tau \in N$,
- $\tau \equiv 0 \mod 2\left(\frac{q^n-1}{q-1}\right) \Rightarrow w^\tau \in S^*$.

Assume first that $\tau \not\equiv 0 \mod \frac{q^n-1}{q-1}$. Then L is surjective, $\dim_{\mathbb{F}_q}(\ker(L)) = n-2$ and hence

$$\mid S_1(\tau) \mid = \mid S_2(\tau) \mid = \mid S_3(\tau) \mid = \mid S_4(\tau) \mid = q^{n-2}\left(\frac{q-1}{2}\right)\left(\frac{q-1}{2}\right).$$

Next assume that $\tau \equiv 0 \mod 2\left(\frac{q^n-1}{q-1}\right)$. Then $\dim_{\mathbb{F}_q}(\ker(L)) = n-1$ and hence

$$\mid S_1(\tau) \mid = q^{n-1} \mid \{(w^\tau y, y) : y \in S^*\} \mid = q^{n-1}\left(\frac{q-1}{2}\right).$$

Similarly $\mid S_4(\tau) \mid = q^{n-1}\left(\frac{q-1}{2}\right)$. Moreover, $\mid S_2(\tau) \mid = \mid S_3(\tau) \mid = 0$ as there is no $(y_1, y_2) \in \mathrm{Im}(L)$ with $y_1 \neq 0, y_2 \neq 0$ and $y_1/y_2 \in N$.

Finally assume that $\tau \equiv \frac{q^n-1}{q-1} \mod 2\left(\frac{q^n-1}{q-1}\right)$. Then $\dim_{\mathbb{F}_q}(\ker(L)) = n-1$ and hence

$$| S_2(\tau) | = q^{n-1} | \{(w^\tau y, y) : y \in S^*\} | = q^{n-1}\left(\frac{q-1}{2}\right).$$

Similarly $| S_3(\tau) | = q^{n-1}\left(\frac{q-1}{2}\right)$. Moreover, $| S_1(\tau) | = | S_4(\tau) | = 0$ as there is no $(y_1, y_2) \in \mathrm{Im}(L)$ with $y_1 \neq 0, y_2 \neq 0$ and $y_1/y_2 \in S^*$. This completes the proof. □

Using the fact that q is odd, we compute i^τ in Lemma 7 explicitly for all cases in the following Corollary.

Corollary 1 For $0 \leq \tau < q^n - 1$,

- If $\tau \equiv 0 \mod 4\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_1}(\tau) = (q-1)q^{n-1}.$$

- If $\tau \equiv 2\left(\frac{q^n-1}{q-1}\right) \mod 4\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_1}(\tau) = \begin{cases} (q-1)q^{n-1}, & \text{if } n \text{ is even,} \\ -(q-1)q^{n-1}, & \text{if } n \text{ is odd.} \end{cases}$$

- If $\tau \equiv \frac{q^n-1}{q-1} \mod 4\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_1}(\tau) = \begin{cases} -(q-1)q^{n-1}, & \text{if } [n \equiv 0 \mod 4 \text{ and } q \equiv 1 \mod 4] \text{ or} \\ & [n \text{ is even and } q \equiv 3 \mod 4], \\ -i(q-1)q^{n-1}, & \text{if } [n \equiv 1 \mod 4 \text{ and } q \equiv 1 \mod 4] \text{ or} \\ & [n \text{ is odd and } q \equiv 3 \mod 4], \\ (q-1)q^{n-1}, & \text{if } [n \equiv 2 \mod 4 \text{ and } q \equiv 1 \mod 4], \\ i(q-1)q^{n-1}, & \text{if } [n \equiv 3 \mod 4 \text{ and } q \equiv 1 \mod 4]. \end{cases}$$

- If $\tau \equiv 3\left(\frac{q^n-1}{q-1}\right) \mod 4\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_1}(\tau) = \begin{cases} -(q-1)q^{n-1}, & \text{if } [n \equiv 0 \mod 4 \text{ and } q \equiv 1 \mod 4] \text{ or} \\ & [n \text{ is even and } q \equiv 3 \mod 4], \\ i(q-1)q^{n-1}, & \text{if } [n \equiv 1 \mod 4 \text{ and } q \equiv 1 \mod 4] \text{ or} \\ & [n \text{ is odd and } q \equiv 3 \mod 4], \\ (q-1)q^{n-1}, & \text{if } [n \equiv 2 \mod 4 \text{ and } q \equiv 1 \mod 4], \\ -i(q-1)q^{n-1}, & \text{if } [n \equiv 3 \mod 4 \text{ and } q \equiv 1 \mod 4]. \end{cases}$$

- If $\tau \not\equiv 0 \mod 4\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_1}(\tau) = 0.$$

Proof First we consider the case $\tau \equiv 3\left(\frac{q^n-1}{q-1}\right) \mod 4\left(\frac{q^n-1}{q-1}\right)$, $n \equiv 1 \mod 4$ and $q \equiv 1 \mod 4$. Using Lemma 7, we have

$$C_{s_1}(\tau) = -(i)^{\tau}(q-1)q^{n-1}. \tag{12}$$

As $\tau \equiv 3\left(\frac{q^n-1}{q-1}\right) \mod 4\left(\frac{q^n-1}{q-1}\right)$, we obtain

$$(i)^{\tau} = (-i)^{\frac{q^n-1}{q-1}}. \tag{13}$$

Note that $q \equiv 1 \mod 4$ and hence

$$\frac{q^n-1}{q-1} = 1 + q + \cdots + q^{n-1} \equiv 1 + 1 + \cdots + 1 \equiv n \equiv 1 \mod 4. \tag{14}$$

Combining equations (12), (13) and (14) we obtain

$$C_{s_1}(\tau) = -(-i)^1(q-1)q^{n-1} = i(q-1)q^{n-1}.$$

Secondly we consider the case $\tau \equiv 3\left(\frac{q^n-1}{q-1}\right) \mod 4\left(\frac{q^n-1}{q-1}\right)$, n is odd and $q \equiv 3 \mod 4$. As $q \equiv 3 \mod 4$ we have

$$\frac{q^n-1}{q-1} = 1 + 3 + 1 + 3 \cdots \mod 4 \equiv \begin{cases} 0 \mod 4, & \text{if } n \text{ is even,} \\ 1 \mod 4, & \text{if } n \text{ is odd.} \end{cases} \tag{15}$$

Since n is odd, using equations (12), (13) and (15) we obtain

$$C_{s_1}(\tau) = -(-i)^1(q-1)q^{n-1} = i(q-1)q^{n-1}.$$

The proofs of the remaining cases are similar. □

Corollary 2 Let s_1 be the sequence given in Definition 2. When q is an odd prime power and $n \geq 2$, the results for the periodic autocorrelation $C_{s_1}(\tau)$ given in Theorem 1 and Theorem 3 follows immediately using Lemma 4, Lemma 7 and Corollary 1. For example, when $q \equiv 1 \mod 4$ and $n \equiv 2 \mod 4$, using Lemma 7 and Corollary 1, the periodic autocorrelation of s_1 for $0 \leq \tau < q^n - 1$ is

$$C_{s_1}(\tau) = \begin{cases} (q-1)q^{n-1}, & \text{if } \tau \equiv 0 \mod 2\left(\frac{q^n-1}{q-1}\right), \\ 0, & \text{otherwise.} \end{cases}$$

Also s_1 is periodic with period $M = {}^{(q^n-1)}/_{(q-1)}$. Using this period and Lemma 4, the periodic autocorrelation of s_1 for $0 \leq \tau \leq M - 1$ is

$$C_{s_1}(\tau) = \begin{cases} q^{n-1}, & \text{if } \tau = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Other results for the periodic autocorrelation $C_{s_1}(\tau)$ given in Theorem 1 and Theorem 3 are obtained similarly.

Corollary 3 For $0 \leq \tau < q^n - 1$,

- If $\tau \equiv 0 \mod 2\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_2}(\tau) = (q-1)q^{n-1}.$$

- If $\tau \equiv \frac{q^n-1}{q-1} \mod 2\left(\frac{q^n-1}{q-1}\right)$, then

$$C_{s_1}(\tau) = \begin{cases} -(q-1)q^{n-1}, & \text{if } n \text{ is even,} \\ (q-1)q^{n-1}, & \text{if } n \text{ is odd.} \end{cases}$$

We skip the proof of Corollary 3, since it is very similar to the proof of Corollary 1.

Corollary 4 Let s_2 be the sequence given in Definition 3. When q is an odd prime power and $n \geq 2$, the results for the periodic autocorrelation $C_{s_2}(\tau)$ given in Theorem 2 and Theorem 3 follows immediately using Lemma 4, Lemma 7 and Corollary 3.

8 Conclusion

In this paper we present sequences with perfect and almost perfect cyclic autocorrelation over the alphabets $\{1, -1, 0\}$ and $\{1, i, -1, -i, 0\}$ using the value zero only once or twice in their period. The constructions provide a big variety of periods also at moderate lengths and the corresponding sequences can be considered 'almost' constant amplitude.

9 Appendix

In Appendix, we give the periodicity and correlation properties of the sequence given below, introduced by Popovic in [20].

Definition 4 Let $q \equiv 1 \mod 4$ be a prime power and H be the subgroup of $\mathbb{F}_q^*$ with $\mathsf{H} = \frac{q-1}{2}$. Let $n \geq 2$, $\mathbb{F}_q^* =< \beta >$ and $\mathbb{F}_{q^n}^* =< w >$. For $t \geq 0$ if $\mathrm{Tr}(w^t) \neq 0$, then let $j(t)$ be the integer such that $0 \leq j(t) < q-1$ and

$$\beta^{j(t)} = \frac{\mathrm{Tr}(w^t)}{\mathrm{Norm}(w^t)}.$$

Then the sequence given by Popovic is defined as

$$s(t) = \begin{cases} 1, & \text{if } j(t) \equiv 0 \mod 4, \\ i, & \text{if } j(t) \equiv 1 \mod 4, \\ -1, & \text{if } j(t) \equiv 2 \mod 4, \\ -i, & \text{if } j(t) \equiv 3 \mod 4, \\ 0, & \text{if } \mathrm{Tr}((w^t)) = 0. \end{cases} \tag{16}$$

Lemma 8 *If* $n \equiv 1 \mod 4$, *then* $N = \frac{q^n-1}{q-1}$ *is a period of* s. *For* $0 \leq \tau < \frac{q^n-1}{q-1}$ *the periodic autocorrelation of* s *is*

$$C_s(\tau) = \begin{cases} q^{n-1}, & \text{if } \tau = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Proof Since $w^N \in \mathbb{F}_q^*$, without loss of generality $w^N = \beta$. To show that N is a period, we need to show $s(t+N) = s(t)$ for $t \geq 0$. Note that

$$\beta^{j(t+N)} = \frac{\mathrm{Tr}(w^{t+N})}{\mathrm{Norm}(w^{t+N})} = \frac{\beta \mathrm{Tr}(w^t)}{\beta^n \mathrm{Norm}(w^t)} = \frac{1}{\beta^{n-1}} \beta^{j(t)}.$$

Since $n \equiv 1 \mod 4$, that is $n-1 \equiv 0 \mod 4$, we obtain $\beta^{j(t+N)} \equiv \beta^{j(t)} \mod 4$. Thus if $n \equiv 1 \mod 4$, $s(t+N) = s(t)$ and $N = \frac{q^n-1}{q-1}$ is a period.

Let $\tau = 0$, then

$$C_s(\tau) = \sum_{t=0}^{N-1} s(t)\overline{s(t)} = \frac{q^n-1}{q-1} - \frac{q^{n-1}-1}{q-1} = q^{n-1}.$$

It remains to prove that if $0 < \tau < \frac{q^n-1}{q-1}$, then $C_s(\tau) = 0$. Consider $v = (s(t) : t \geq 0)$ be the sequence defined by using Equation 16. It is clear that $q^n - 1$ is a period of v. We need to prove that if $w^\tau \notin \mathbb{F}_q$, or equivalently $\tau \not\equiv 0 \mod \frac{q^n-1}{q-1}$, then $C_v(\tau) = 0$. The $(q^n-1)-$periodic autocorrelation is

$$\begin{aligned} C_v(\tau) &= \sum_{t=0}^{q^n-2} v(t+\tau)\overline{v(t)} \\ &= \mid A_{00}(\tau) \mid -i \mid A_{01}(\tau) \mid - \mid A_{02}(\tau) \mid +i \mid A_{03}(\tau) \mid \\ &+ i \mid A_{10}(\tau) \mid + \mid A_{11}(\tau) \mid -i \mid A_{12}(\tau) \mid - \mid A_{13}(\tau) \mid \\ &- \mid A_{20}(\tau) \mid +i \mid A_{21}(\tau) \mid + \mid A_{22}(\tau) \mid -i \mid A_{23}(\tau) \mid \\ &- i \mid A_{30}(\tau) \mid - \mid A_{31}(\tau) \mid +i \mid A_{32}(\tau) \mid + \mid A_{33}(\tau) \mid . \end{aligned}$$

Here for $0 \leq l_1, l_2 \leq 3$,

$$\begin{aligned} A_{l_1 l_2}(\tau) = \{x \in \mathbb{F}_{q^n}^* : &\mathrm{Tr}(w^\tau x) \neq 0, \ \mathrm{Tr}(x) \neq 0, \\ &\frac{\mathrm{Tr}(w^\tau x)}{\mathrm{Norm}(w^\tau x)} \in \beta^{l_1} H \text{ and } \frac{\mathrm{Tr}(x)}{\mathrm{Norm}(x)} \in \beta^{l_2} H\}. \end{aligned}$$

For $0 \leq l \leq 3$, let $\oplus$ denote addition modulo 4. Put

$$T_0(\tau) = \sum_{l=0}^{3} A_{l,l}(\tau),$$

$$T_1(\tau) = \sum_{l=0}^{3} A_{l,l\oplus 1}(\tau),$$

$$T_2(\tau) = \sum_{l=0}^{3} A_{l,l\oplus 2}(\tau),$$

$$T_3(\tau) = \sum_{l=0}^{3} A_{l,l\oplus 3}(\tau).$$

Then for $0 \leq l \leq 3$,

$$T_l(\tau) = \left\{ x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}(w^\tau x) \neq 0,\ \mathrm{Tr}(x) \neq 0,\ \frac{\mathrm{Tr}(w^\tau x)}{\mathrm{Norm}(w^\tau x)} \frac{\mathrm{Norm}(x)}{\mathrm{Tr}(x)} \in \frac{1}{\beta^l} H \right\}.$$

Note that since $\mathrm{Tr}(w^\tau x) \neq 0$ and $\mathrm{Tr}(x) \neq 0$,

$$\frac{\mathrm{Tr}(w^\tau x)}{\mathrm{Norm}(w^\tau x)} \frac{\mathrm{Norm}(x)}{\mathrm{Tr}(x)} = \frac{\mathrm{Tr}(w^\tau x)}{\mathrm{Tr}(x)} \frac{1}{\mathrm{Norm}(w^\tau)},$$

where $\frac{1}{\mathrm{Norm}(w^\tau)}$ is a constant.

Recall that if $w^\tau \notin \mathbb{F}_q$, then the $\mathbb{F}_q-$linear map L given by Equation (9) is surjective and $\dim_{\mathbb{F}_q}(\ker(L)) = n-2$. Fix $0 \leq l \leq 3$ and consider

$$\begin{aligned} T_l(\tau) &= \left\{ x \in \mathbb{F}_{q^n}^* : \mathrm{Tr}(w^\tau x) \neq 0,\ \mathrm{Tr}(x) \neq 0,\ \frac{\mathrm{Tr}(w^\tau x)}{\mathrm{Norm}(w^\tau x)} \frac{\mathrm{Norm}(x)}{\mathrm{Tr}(x)} \in \frac{1}{\beta^l} H \right\} \\ &= \bigcup_{h \in H} \bigcup_{a \in \mathbb{F}_q^*} \left\{ x \in \mathbb{F}_{q^n}^* : L(x) = \left(ah \frac{\mathrm{Norm}(w^\tau)}{\beta^l}, a \right) \right\}. \end{aligned}$$

Since L is surjective and $\dim_{\mathbb{F}_q}(\ker(L)) = n-2$, for each fixed $h \in H$ and $a \in \mathbb{F}_q^*$, the number of the elements of the set

$$\left\{ x \in \mathbb{F}_{q^n}^* : L(x) = \left(ah \frac{\mathrm{Norm}(w^\tau)}{\beta^l}, a \right) \right\}$$

is q^{n-2}. Also if $(a_1, h_1) \neq (a_2, h_2)$ with $h_1, h_2 \in H$ and $a_1, a_2 \in \mathbb{F}_q^*$, then

$$\left(a_1 h_1 \frac{\mathrm{Norm}(w^\tau)}{\beta^l}, a_1 \right) \neq \left(a_2 h_2 \frac{\mathrm{Norm}(w^\tau)}{\beta^l}, a_2 \right).$$

Otherwise $a_1 = a_2$ and $h_1 = h_2$. Hence,

$$| T_l(\tau) | = | \mathbb{F}_q^* | \, | H | \, q^{n-2} = \left(\frac{q-1}{2} \right)^2 q^{n-2}.$$

Since $| T_0(\tau) | = | T_1(\tau) | = | T_2(\tau) | = | T_3(\tau) |$, we obtain

$$C_v(\tau) = | T_0(\tau) | - i | T_1(\tau) | - | T_2(\tau) | + i | T_3(\tau) | = 0.$$

Finally, using Lemma 4, when $\tau \neq 0$ we obtain

$$C_s(\tau) = 0.$$

□

References

[1] Wen, Y., Huang, W., Zhang, Z.: Cazac sequence and its application in lte random access, 544–547 (2006). IEEE

[2] Chu, D.: Polyphase codes with good periodic correlation properties (corresp.). IEEE Transactions on Information Theory **18**(4), 531–532 (1972). https://doi.org/10.1109/TIT.1972.1054840

[3] Frank, R., Zadoff, S., Heimiller, R.: Phase shift pulse codes with good periodic correlation properties (corresp.). IEE Transactions on Information Theory **8**(6), 381–382 (1962). https://doi.org/10.1109/TIT.1962.1057786

[4] Heimiller, R.: Phase shift pulse codes with good periodic correlation properties. IRE Transactions on Information Theory **7**(4), 254–257 (1961). https://doi.org/10.1109/TIT.1961.1057655

[5] Blümich, B., Gong, Q., Byrne, E., Greferath, M.: NMR with excitation modulated by Frank sequences. Journal of Magnetic Resonance **199**(1), 18–24 (2009)

[6] Görges, A., Benders, S., Greferath, M., Küppers, M., Adams, M., Blümich, B.: Selective magnetic resonance signal suppression by colored Frank excitation. Journal of Magnetic Resonance **317**(2), 106776 (2020)

[7] Tseitlin, M., Quine, R.W., Eaton, S.S., Eaton, G.R.: Use of polyphase continuous excitation based on the Frank sequence in EPR. Journal of Mag. Resonance **211**(2), 221–227 (2011)

[8] Tseitlin, M., Quine, R.W., Eaton, S.S., Eaton, G.R., Halpern, H.J., Ardenkjaer-Larsen, J.-H.: Use of the Frank sequence in pulsed EPR. Journal of Magnetic Resonance **209**(2), 306–309 (2011)

[9] Kaiser, R.: Application of the Hadamard transform to NMR spectrometry with pseudonoise excitation. Journal of Magnetic Resonance (1969) **15**(1), 44–63 (1974)

[10] Ziessow, D., Blümich, B.: Hadamard-NMR-spektroskopie. Berichte der Bunsengesellschaft für physikalische Chemie **78**(11), 1168–1179 (1974)

[11] Greferath, M., Blümich, B., Griffith, W., Hoatson, G.: Saturation in deuteron Hadamard NMR spectroscopy of solids. Journal of Magnetic Resonance, Series A **102**(1), 73–80 (1993)

[12] Zhang, T., Michal, C.A.: Broadband NMR random window noise excitation. Journal of Magnetic Resonance **297**, 172–179 (2018)

[13] Liao, M.-Y., Zax, D.B.: Analysis of signal-to-noise ratios for noise excitation of quadrupolar nuclear spins in zero field. The Journal of Physical Chemistry **100**(5), 1483–1487 (1996)

[14] Somasundaram, S.D., Jakobsson, A., Rowe, M.D., Smith, J.A., Butt, N.R., Althoefer, K.: Robust detection of stochastic nuclear quadrupole resonance signals. IEEE Transactions on Signal Processing **56**(9), 4221–4229 (2008)

[15] Blumich, B., Jansen, J., Nilgens, H., Blumler, P., Hoatson, G.: Nmr imaging with noise excitation, slice selection. Magn. Reson. Biol. Med **1**, 61–72 (1993)

[16] Pursley, R.H., Kakareka, J., Salem, G., Devasahayam, N., Subramanian, S., Tschudin, R.G., Krishna, M.C., Pohida, T.J.: Stochastic excitation and Hadamard correlation spectroscopy with bandwidth extension in rf ft-epr. Journal of Magnetic Resonance **162**(1), 35–45 (2003)

[17] Ryser, H.J.: Combinatorial Mathematics vol. 14. American Mathematical Soc., U.S.A. (1963)

[18] Arasu, K., De Launey, W., Ma, S.L.: On circulant complex Hadamard matrices. Designs, Codes and Cryptography **25**(2), 123–142 (2002)

[19] Arasu, K., De Launey, W., Ma, S.L.: Existence and nonexistence of almost perfect autocorrelation seq. Designs, Codes and Cryptography **25**(2), 123–142 (2002)

[20] Popovic, B.M.: New class of complex sequences with ideal autocorrelation. In: Proceedings. Electrotechnical Conference Integrating Research, Industry and Education in Energy and Communication Engineering, IEEE, pp. 618–620 (1989)

[21] Lee, C.E.: On a New Class of 5-ary Sequences Exhibiting Ideal Periodic Autocorrelation Properties with Applications to Spr. Spec. Sys. Mississippi State University, U.S.A. (1986)